WPROWADZENIE

Dzisiejszy świat jest niebezpiecznym miejscem dla korporacji. Internet umożliwił firmom dostęp do miliardów klientów i innych partnerów biznesowych, ale dał również przestępcom dostęp do setek milionów korporacji i osób fizycznych. Przestępcy mogą atakować witryny internetowe, bazy danych i krytyczne systemy informacyjne bez przekraczania granicy kraju będącego gospodarzem korporacji. Korporacje stały się krytycznie zależne od technologii informatycznych (IT) jako części ich ogólnej przewagi konkurencyjnej. Aby chronić swoją infrastrukturę IT przed różnymi zagrożeniami i późniejszą rentownością, korporacje muszą mieć kompleksowe zasady bezpieczeństwa IT, ugruntowane procedury, wzmocnione aplikacje i bezpieczny sprzęt.

Podstawowa terminologia dotycząca bezpieczeństwa

Środowisko zagrożenia

Jeśli firmy mają być w stanie się bronić, potrzebują zrozumienia środowiska zagrożeń - to znaczy typów napastników i ataków, z którymi borykają się firmy. „Zrozumieć środowisko zagrożenia" to fantazyjny sposób powiedzenia „Poznaj swojego wroga". Jeśli nie wiesz, jak możesz zostać zaatakowany, nie możesz planować obrony. Ta część skupi się prawie wyłącznie na środowisku zagrożeń.

Środowisko zagrożeń składa się z typów napastników i ataków, z którymi mierzą się firmy

CELE BEZPIECZEŃSTWA

Korporacje i podgrupy w korporacjach mają cele bezpieczeństwa - warunki, które chcą osiągnąć pracownicy ochrony. Trzy wspólne podstawowe cele określane są łącznie jako CIA. To nie jest Centralna Agencja Wywiadowcza. CIA oznacza raczej poufność (confidentiality), integralność (integrity) i dostępność (availability)

* Poufność - Poufność oznacza, że ludzie nie mogą czytać poufnych informacji, ani gdy znajdują się one na komputerze, ani gdy podróżują przez sieć.

* Integralność-integralność oznacza, że osoby atakujące nie mogą zmieniać ani niszczyć informacji, ani gdy znajdują się one na komputerze, ani gdy podróżują przez sieć. Lub przynajmniej, jeśli informacja zostanie zmieniona lub zniszczona, odbiorca może wykryć zmianę lub przywrócić zniszczone dane.

* Dostępność-Dostępność oznacza, że nie uniemożliwia się tego osobom upoważnionym do korzystania z informacji. Ani atak komputerowy, ani atak sieciowy nie powstrzymają ich od informacji, do których mają dostęp.

Wielu specjalistów ds. bezpieczeństwa jest niezadowolonych z uproszczonej taksonomii celów CIA, ponieważ uważają, że firmy mają wiele innych celów związanych z bezpieczeństwem. Jednak cele CIA są dobrym miejscem do rozpoczęcia myślenia o celach bezpieczeństwa.

NARUSZENIA

Gdy zagrożeniu udaje się wyrządzić szkodę firmie, nazywa się to incydentem lub naruszeniem. Firmy oczywiście starają się powstrzymać incydenty, ale zazwyczaj każdego roku muszą stawić czoła kilku naruszeniom, więc reagowanie na incydenty jest umiejętnością krytyczną. Jeśli chodzi o model procesów biznesowych, zagrożenia odsuwają proces biznesowy od realizacji co najmniej jednego z jego celów.

ŚRODKI ZARADCZE

Oczywiście specjaliści ds. bezpieczeństwa próbują powstrzymać zagrożenia. Metody, których używają do udaremniania ataków, nazywane są środkami zaradczymi, zabezpieczeniami, zabezpieczeniami lub kontrolami. Celem środków zaradczych jest utrzymywanie procesów biznesowych na właściwej drodze do osiągnięcia celów biznesowych pomimo obecności zagrożeń i rzeczywistych kompromisów. Narzędzia używane do udaremniania ataków nazywane są środkami zaradczymi, zabezpieczeniami lub kontrolami. Środki zaradcze mogą być techniczne, ludzkie lub (najczęściej) będące połączeniem tych dwóch. Zazwyczaj środki zaradcze dzielą się na trzy typy:

* Zapobiegawcze - zapobiegawcze środki zaradcze zapobiegają powodzeniu ataków. Większość kontroli to kontrole prewencyjne.

* Wykrywanie - wykrywalne środki zaradcze określają, kiedy zagrożenie atakuje, a zwłaszcza gdy odnosi sukces. Szybkie wykrywanie może zminimalizować uszkodzenia.

* Korygujące - środki zaradcze przywracają proces biznesowy na właściwe tory po zdarzeniu. Im szybciej proces biznesowy może wrócić na właściwe tory, tym większe prawdopodobieństwo, że proces biznesowy osiągnie swoje cele.

TEST

a. Dlaczego ważne jest, aby firmy rozumiały środowisko zagrożeń?

b. Nazwij trzy wspólne cele bezpieczeństwa.

c. Krótko wyjaśnij każdy.

d. Co to jest incydent?

e. Jakie są synonimy incydentów?

f. Jakie są środki zaradcze?

g. Jakie są synonimy środka zaradczego?

h. Jakie są cele środków zaradczych?

i . Jakie są trzy rodzaje środków zaradczych?

Studium przypadku: naruszenie danych w TJX

Jeśli ta terminologia wydaje się abstrakcyjna, warto przyjrzeć się konkretnemu atakowi, aby umieścić te terminy w kontekście i pokazać, jak złożone mogą być ataki bezpieczeństwa. Zaczniemy od jednej z największych strat prywatnych informacji o klientach. To jest naruszenie danych TJX.

TJX COMPANIES, INC.

TJX Companies, Inc. (TJX) to grupa ponad 2500 sklepów detalicznych działających w Stanach Zjednoczonych, Kanadzie, Anglii, Irlandii i kilku innych krajach. Firmy te prowadzą działalność pod takimi nazwami jak TJ Maxx i Marshalls. TJX określa się jako „wiodący sprzedawca ubrań i artykułów modowych po obniżonej cenie w Stanach Zjednoczonych i na świecie". Przy tego rodzaju deklaracji misji istnieje silna presja na minimalizację kosztów.

ODKRYCIE

18 grudnia 2006 r. TJX wykrył „podejrzane oprogramowanie" w swoich systemach komputerowych. Trzy dni później TJX wezwał konsultantów ds. bezpieczeństwa, aby zbadali sytuację. 21 grudnia

konsultanci potwierdzili, że włamanie rzeczywiście miało miejsce. Następnego dnia firma poinformowała organy ścigania w Stanach Zjednoczonych i Kanadzie. Pięć dni później konsultanci ds. bezpieczeństwa ustalili, że dane klientów zostały skradzione. Konsultanci wstępnie ustalili, że oprogramowanie włamaniowe działało przez siedem miesięcy, zanim zostało wykryte. Kilka tygodni później konsultanci odkryli, że firma również została kilkakrotnie naruszona w 2005 roku. Podsumowując, konsultanci oszacowali, że zostało skradzionych 45,7 miliona rekordów klientów. To zdecydowanie największa liczba osobistych danych klientów skradzionych z jakiejkolwiek firmy w tym czasie. Złodzieje nie ukradli tych rekordów dla dreszczyku emocji związanych z włamaniem lub dla wzmocnienia swojej reputacji wśród innych hakerów. Zrobili to, aby móc wykorzystać te informacje do dokonania oszukańczych zakupów kartami kredytowymi, wypłacenia tysięcy dolarów z bankomatów i sprzedania skradzionych danych kart kredytowych innym przestępcom. Skradzione fundusze były następnie prane za pośrednictwem międzynarodowych rachunków bankowych. W swojej obronie TJX zauważył, że w większości skradzionych danych większość danych osobowych użytkowników została zamaskowana (zastąpiona gwiazdkami). Zauważył również, że większość kart kredytowych, o których przechowywano informacje, straciła ważność i że firma generalnie nie gromadziła numerów ubezpieczenia społecznego (SSN). Jednak w przypadku 455 000 klientów, którym zwrócono pieniądze bez pokwitowania, zebrano znacznie większą ilość danych osobowych, a także te informacje zostały skradzione. TJX poinformował klientów o naruszeniu danych dopiero prawie miesiąc później. Firma powiedziała, że potrzebuje czasu, aby wzmocnić swoje bezpieczeństwo. Firma poinformowała również, że funkcjonariusze organów ścigania powiedzieli TJX, aby nie ujawniała natychmiast informacji o naruszeniu, aby uniknąć ujawnienia złodziejom danych śledztwa. Oczywiście opóźnienie spowodowało również, że klienci nie zdawali sobie sprawy z niebezpieczeństwa, z którym się spotkali.

WŁAMANIE

Jak doszło do naruszeń? Uważa się, że złodzieje danych włamali się do słabo chronionych sieci bezprzewodowych w niektórych sklepach detalicznych, aby dostać się do centralnego systemu przetwarzania kart kredytowych i debetowych TJX w Massachusetts. Sniffer, słuchał słabo zaszyfrowanego ruchu firmy przechodzącego do i z centrum przetwarzania. Kolejnym problemem było to, że TJX zachowywał pewne poufne informacje o kartach kredytowych, których nie powinno się przechowywać; to właśnie te niewłaściwie zachowane informacje uznali za wartościowe dla złodziei danych. W jaki sposób złodzieje pozostali niewykrytymi, mimo że sniffer działał przez ponad pół roku i pomimo eksfiltracji ponad 80 GB danych? W jaki sposób atakujący umieścili sniffera w sieci TJX, który pozostawał niewykryty przez siedem miesięcy? Wydaje się, że odpowiedź na to pytanie jest taka, że TJX nie posiadał zorganizowanej zdolności wykrywania włamań. Na swoją obronę firma stwierdziła, że „wierzy, że nasze zabezpieczenia były porównywalne z wieloma innymi głównymi sprzedawcami detalicznymi". Jej celem mogło być przygotowanie do obrony przed procesami sądowymi opartymi na zaniedbaniach. Udowodnienie zaniedbania zwykle wymaga udowodnienia, że sprawca był nieuprawniony, w oparciu o ogólną praktykę w terenie. Kanadyjska Komisja ds. Prywatności, która była pierwszym biurem rządowym, które ujawniło ustalenia dotyczące włamania, dokonała następującej oceny bezpieczeństwa TJX w momencie naruszenia:

Firma zebrała zbyt dużo danych osobowych, przechowywała je zbyt długo i polegała na słabej technologii szyfrowania, aby je chronić, co stanowi zagrożenie dla prywatności milionów swoich klientów… Firma nie poradziła sobie z ryzykiem włamania, nie zaszyfrowała danych wystarczająco mocno, nie monitorowała odpowiednio swoich systemów, nie działała zgodnie ze standardami branży kart płatniczych i zebrała zbyt dużo informacji

KARTA PŁATNICZA - STANDARD BEZPIECZEŃSTWA DANYCH

Szereg wcześniejszych (i mniejszych) naruszeń danych skłoniło główne firmy obsługujące karty kredytowe do stworzenia standardu bezpieczeństwa danych kart płatniczych (PCI-DSS). Norma ta określała 12 wymaganych celów kontrolnych, które muszą zostać wdrożone przez firmy akceptujące zakupy kartą kredytową. Brak wdrożenia celów kontrolnych PCI-DSS może skutkować karami, a nawet odebraniem zdolności firmy do przyjmowania płatności kartą kredytową. W momencie wykrycia naruszenia danych firma TJX była daleko w tyle w swoim programie zgodności z PCI-DSS. Firma spełniła tylko 3 z 12 wymaganych celów kontroli. Z notatek wewnętrznych wynika, że firma wiedziała, iż narusza wymagania PCI-DSS, w szczególności w odniesieniu do słabego szyfrowania w sieciach bezprzewodowych sklepów detalicznych. Jednak firma celowo postanowiła nie podejmować szybkich działań w celu rozwiązania tego problemu. W listopadzie 2005 roku jeden z pracowników zauważył proroczo, że „oszczędzanie pieniędzy i zgodność z PCI jest dla nas ważna, ale równie ważna jest ochrona przed intruzami. Mimo że mamy trochę przestrzeni do oddychania z PCI, nadal jesteśmy podatni na ataki z WEP jako kluczem bezpieczeństwa. To musi być ryzyko, które jesteśmy gotowi podjąć, aby zaoszczędzić pieniądze i mieć nadzieję, że nie zostaniemy narażeni ". Kiedy pracownik zauważył, że „mamy trochę przestrzeni do oddychania z PCI", prawdopodobnie odnosił się do faktu, że TJX otrzymało rozszerzenie pozwalające na zachowanie zgodności poza określoną datą zgodności ze standardem. Jak na ironię, ten dodatkowy czas przyznano po tym, jak naruszenia danych już się rozpoczęły. To rozszerzenie było uzależnione od oceny raportu TJX na temat projektu zgodności do czerwca 2006 r. Nie wiadomo, czy TJX spełnił ten wymóg. List upoważniający do przedłużenia został wysłany przez wiceprezesa ds. Kontroli oszustw Visa. Skończyło się na „Doceniam Twoje nieustające wsparcie i zaangażowanie w ochronę branży płatniczej".

UPADEK: PRAWA I DOCHODZENIA

Firma szybko uwikłała się w procesy handlowe i dochodzenia rządowe. Te procesy sądowe obejmowały złożenie informacji, które rzuciły dodatkowe światło na włamania. Na przykład zapieczętowane dowody z kart Visa i MasterCard wykazały, że liczba skradzionych rekordów kont wyniosła 94 miliony - mniej więcej dwa razy więcej niż szacunki TJX. TJX został pozwany przez kilka pojedynczych banków i zrzeszeń banków. TJX rozliczył się, płacąc 24 mln USD pożyczkodawcom wydającym karty MasterCard i 41 mln USD Visa. Zapłacili również 9,75 miliona dolarów na rozstrzygnięcie spraw z 41 stanami. W tej bitwie korporacyjnych gigantów konsumenci byli obsługiwani na końcu. TJX zaproponował ugodę, która obejmowałaby jedynie aktywne środki, takie jak pomoc w kradzieży tożsamości poprzez ubezpieczenie i inne środki dla około 455 000 ofiar, które podały dane osobowe, zwracając towary bez pokwitowania. Inne ofiary otrzymałyby skromny kupon (30 USD) lub możliwość zakupu towarów TJX po obniżonych cenach.

OSKARŻENIE

W dniu 25 sierpnia 2008 roku Departament Sprawiedliwości oskarżył 11 osób o włamanie do TJX i późniejsze wykorzystanie skradzionych informacji. Trzech było Amerykanami i szybko trafili do więzienia. Dwóch kolejnych było w Chinach. Reszta znajdowała się w Europie Wschodniej. Akt oskarżenia podkreśla międzynarodowy charakter cyberprzestępczości. Chociaż trzej Amerykanie dokonali faktycznej kradzieży danych, wydali skradzione informacje za granicą. Dwóch amerykańskich oskarżonych szybko złożyło pozew, aby zeznawać przeciwko domniemanemu przywódcy Albertowi Gonzalezowi z Miami na Florydzie. 25 marca 2010 r. Gonzalez został skazany na 20 lat więzienia. Wyrok wynikał z połączonej sprawy, która dodała OfficeMax, Dave & Buster's i Barnes & Noble do listy przedsiębiorstw, których dotyczy. 26 marca 2010 r. Gonzalez został ponownie skazany na 20 lat i jeden dzień więzienia za kradzież około 130 milionów dodatkowych numerów kart kredytowych z Heartland Payment Systems. Ponieważ wyrok ten ma być odbywany jednocześnie z jego wcześniejszym wyrokiem skazującym, wydłuża on tylko jeden dzień kary. Gonzalez użył ataku SQL na Heartland, aby ukraść

numery kart kredytowych. Firmy, których to dotyczy, to 7-Eleven, J.C. Penny i Wet Seal. To największa znana dotychczas kradzież tożsamości

TEST II

a. Kim były ofiary naruszenia TJX? (Odpowiedzi nie ma w tekście i nie jest to trywialne pytanie).

b. Czy włamanie do TJX było spowodowane pojedynczą słabością zabezpieczeń, czy wieloma słabymi punktami zabezpieczeń? Wyjaśnić.

c. Dlaczego spełnienie celów kontrolnych PCI-DSS prawdopodobnie zapobiegłoby naruszeniu danych przez TJX? To nie jest trywialne pytanie.

d. Czy spełnienie celów kontrolnych PCI-DSS zapewniłoby, że naruszenie danych nie miałoby miejsca? Pomyśl o tym dokładnie. Odpowiedzi nie ma w tekście.

e. Którego z celów CIA nie udało się TJX osiągnąć w tym ataku?

ZAGROŻENIA PRZEZ PRACOWNIKÓW I EX-PRACOWNIKÓW

Przyjrzawszy się ogólnym zagrożeniom, kluczowej terminologii związanej z bezpieczeństwem i konkretnemu kompromisowi, przyjrzymy się teraz konkretnym elementom środowiska zagrożeń korporacyjnych. Zaczniemy od spojrzenia wewnątrz firmy, na zagrożenia stwarzane przez pracowników. Kiedy firmy zaczęły kupować własne komputery w latach sześćdziesiątych XX wieku, szybko odkryły, że niezadowoleni i chciwi pracownicy oraz byli pracownicy stanowią poważne zagrożenie dla bezpieczeństwa. Ponieważ firmy stały się bardziej zależne od technologii informacyjnej, zagrożenia ze strony osób z wewnątrz stały się bardziej niebezpieczne.

Dlaczego pracownicy są niebezpieczni

Pracownicy i byli pracownicy są bardzo niebezpieczni z czterech powodów:

• Zwykle posiadają rozległą wiedzę o systemach.

• Często posiadają poświadczenia potrzebne do uzyskania dostępu do wrażliwych części systemów.

• Znają korporacyjne mechanizmy kontrolne i często wiedzą, jak uniknąć wykrycia.

• Wreszcie, firmy zwykle ufają swoim pracownikom. W rzeczywistości, gdy ochrona nalega, aby pracownik zachowywał się w określony sposób lub wyjaśniał oczywiste naruszenie zasad bezpieczeństwa, często kierownik pracownika chroni pracownika przed „ingerencją w bezpieczeństwo".

Pracownicy i byli pracownicy są bardzo niebezpieczni, ponieważ mają rozległą wiedzę na temat systemów, posiadają poświadczenia potrzebne do uzyskania dostępu do wrażliwych części systemów, często wiedzą, jak uniknąć wykrycia, i mogą skorzystać na zaufaniu, którym zwykle obdarza się „naszych ludzi". Czynniki te często eliminują potrzebę posiadania zaawansowanej wiedzy komputerowej. W rzeczywistości w 23 cyberprzestępstwach związanych z usługami finansowymi popełnionych w latach 1996-2002 87 procent zostało popełnionych bez żadnego zaawansowanego programowania. Pracownicy IT są szczególnie niebezpieczni ze względu na ich niezwykłą wiedzę i dostęp. Pracownicy bezpieczeństwa IT są najbardziej niebezpieczni ze wszystkich. W około połowie przypadków oskarżeni są specjalistami IT, a nawet pracownikami ochrony i byłymi pracownikami. Rzymianie zapytali, Quis custodiet custodes? To tłumaczy się jako „Kto obserwuje obserwatorów?" To jedna z najtrudniejszych kwestii w zarządzaniu bezpieczeństwem IT.

Sabotaż pracowników

Jedną z najstarszych obaw dotyczących pracowników jest sabotaż, czyli niszczenie sprzętu, oprogramowania lub danych. Sabotaż pochodzi od francuskiego słowa oznaczającego obuwie, ponieważ niezadowoleni pracownicy we wczesnych latach rewolucji przemysłowej rzekomo wrzucali drewniane buty do maszyn, aby zatrzymać produkcję. Sabotaż może mieć również motywy finansowe. Kiedy Roger Duronio sabotował 2000 serwerów w UBS PaineWebber, nie tylko karał swojego byłego pracodawcę. Sprzedał również krótko przed akcje UBS PaineWebber, aby skorzystać z późniejszego spadku ceny akcji firmy. Chociaż atak spowodował rozległe szkody, kurs akcji nie spadł, a Duronio stracił pieniądze. Uznany za winnego sabotażu komputerowego i oszustw związanych z papierami wartościowymi, 63-letni Duronio został skazany na osiem lat więzienia federalnego.

„Tim Lloyd, administrator systemów komputerowych, został zwolniony. W odwecie Lloyd umieścił program bomby logicznej na krytycznym serwerze. Kiedy wystąpiły z góry określone warunki, bomba logiczna zniszczyła programy sterujące maszynami produkcyjnymi firmy. Lloyd zabrał również do domu i skasował zapasowe taśmy firmy, aby zapobiec przywróceniu. Sabotaż Lloyda przyniósł natychmiastowe straty biznesowe w wysokości 10 mln USD, koszty przeprogramowania 2 mln USD i 80 zwolnień. Atak doprowadził do trwałej utraty przez firmę pozycji konkurencyjnej na rynku nowoczesnych przyrządów i pomiarów, ponieważ firma nie mogła odbudować zastrzeżonego oprogramowania do projektowania, z którego korzystała”

Hackowanie przez pracowników

Innym problemem jest to, że pracownicy włamują się do komputerów firmy przy użyciu skradzionych danych uwierzytelniających, luk w systemach wewnętrznych lub innych oszukańczych metod. Mogą wtedy sprzeniewierzyć pieniądze, ukraść własność intelektualną lub po prostu spojrzeć na żenujące informacje. Jak zobaczymy później, prawo Stanów Zjednoczonych podaje następującą definicję hakowania - celowego uzyskiwania dostępu do zasobów komputera bez autoryzacji lub z nadmiarem autoryzacji. Definicje hakowania w innych jurysdykcjach są zwykle bardzo podobne.

Hakowanie to celowe uzyskiwanie dostępu do zasobów komputera bez autoryzacji lub z nadmiarem autoryzacji.

Zauważ, że kluczową kwestią jest autoryzacja. Czy masz jawne (lub niejawne) upoważnienie do korzystania z zasobu, do którego uzyskałeś dostęp? Czy byłeś upoważniony do korzystania z części zasobu, ale nie z określonej części, do której uzyskałeś dostęp? Motywacja do włamania jest nieistotna. Kary są takie same, niezależnie od tego, czy próbowałeś ukraść milion dolarów lub po prostu „testowałeś bezpieczeństwo.

Kradzież finansowa pracowników i kradzież własności intelektualnej

Istnieje wiele powodów, dla których pracownicy mają dostęp do zasobów bez pozwolenia lub z nadmiarem pozwolenia. Czasami pracownicy robią to z czystej ciekawości lub w celu znalezienia informacji, które mogą zawstydzić firmę. Czasami jednak mają one czysto kryminalne cele, takie jak kradzież finansowa, która wiąże się z przywłaszczeniem majątku (powiedzmy poprzez przypisanie go sobie za pomocą komputera) lub kradzieżą pieniędzy (na przykład manipulowanie aplikacją, aby zapłacił premię). Innym motywem przestępczym jest kradzież własności intelektualnej firmy (IP), czyli informacji będących własnością firmy i chronionych prawem. IP obejmuje formalnie chronione informacje, takie jak prawa autorskie, patenty, nazwy handlowe i znaki towarowe. Chociaż wiele firm nie ma takich formalnych aktywów intelektualnych, własność intelektualna obejmuje również tajemnice handlowe, czyli fragmenty wrażliwych informacji, które firma zachowuje w tajemnicy.

Obejmują one plany, receptury produktów, procesy biznesowe, cenniki, listy klientów i wiele innych rodzajów informacji, które firma chce zachować w tajemnicy przed konkurentami. Jeśli inna firma uzyska tajemnicę handlową w nielegalny sposób, będzie ona podlegać postępowaniu sądowemu. Niemniej jednak niektórzy pracownicy kradną tajemnice handlowe, aby sprzedać je innej firmie. Własność intelektualna (IP) to informacje należące do firmy i chronione prawem. Tajemnice handlowe

Wymuszenia pracownicze

W niektórych przypadkach pracownik lub były pracownik wykorzysta swoją zdolność do uszkodzenia systemów lub uzyskania dostępu do poufnych informacji w celu wyłudzenia informacji od firmy. W wymuszeniu sprawca próbuje zdobyć pieniądze lub inne dobra, grożąc podjęciem działań sprzecznych z interesem ofiary. Na przykład pracownik może podłożyć bombę logiczną w komputerze firmy. Jeśli pracownik lub były pracownik każe firmie zapłacić pieniądze, aby uniknąć szkód, jest to wymuszenie. Kradzież własności intelektualnej i żądanie pieniędzy w zamian za nieprzekazywanie informacji również jest wymuszeniem. W wymuszeniu sprawca próbuje zdobyć pieniądze lub inne towary, grożąc podjęciem działań sprzecznych z interesem ofiary

Molestowanie seksualne lub rasowe pracowników

Chociaż hakowanie, kradzież i wymuszenia to krytyczne kwestie, molestowanie seksualne lub rasowe wśród pracowników jest jeszcze częstszym problemem. Na przykład molestowanie seksualne może obejmować groźby fizyczne, zemstę po romantycznym zerwaniu, pobieranie i wyświetlanie pornografii lub odwet na niechętnym partnerze seksualnym poprzez wstrzymanie promocji i podwyżek.

NADUŻYCIE INTERNETU

Termin nadużycie jest używany w odniesieniu do działań, które naruszają obowiązujące w firmie zasady korzystania z technologii informatycznych lub zasady etyczne. W niektórych przypadkach pracownicy nadużywają dostępu do Internetu, najczęściej pobierając pornografię, pobierając pirackie media lub oprogramowanie lub tracąc wiele godzin na surfowanie po Internecie w celach osobistych. Nadużycia wahają się od lekko szkodliwego zachowania po czyny przestępcze. Nadużycia obejmują działania, które naruszają obowiązujące w firmie zasady korzystania z IT lub zasady etyczne. Pobieranie pornografii może prowadzić do pozwów o molestowanie seksualne przeciwko firmie, jak również przeciwko osobie odpowiedzialnej. Pobieranie pirackiej muzyki, filmów i oprogramowania może z kolei skutkować wysokimi karami za naruszenie praw autorskich. Pobieranie niezatwierdzonych plików może również prowadzić do kosztownych infekcji złośliwym oprogramowaniem. Podczas gdy wielu pracodawców nie ma nic przeciwko niewielkiej ilości osobistego korzystania z Internetu, niektórzy pracownicy uzależniają się od korzystania z Internetu i spędzają dziesiątki godzin tygodniowo na osobistym surfowaniu po sieci w pracy. Ponadto, gdy pracownicy pobierają wiele plików z Internetu, najprawdopodobniej pobiorą wirusa lub inne złośliwe oprogramowanie. Działy bezpieczeństwa IT zwykle nie lubią szukać dowodów pornografii i nadmiernego korzystania z Internetu, ale w większości firm jest to część pracy.

NIE-INTERNETOWE NADUŻYCIE KOMPUTERA

Innym aspektem nadużyć pracowników jest nieuprawniony dostęp do prywatnych danych osobowych w systemach wewnętrznych przez zaciekawionych pracowników. Tego typu zachowanie wykryto podczas kampanii wyborczej w USA w 2008 roku oraz w kilku hospitalizacjach znanych osób. Nadużywanie wewnętrznych systemów korporacyjnych w celach podglądania nie ogranicza się do pracowników biura głównego. Na przykład ankieta przeprowadzona wśród 300 starszych administratorów IT podczas londyńskiej konferencji i targów poświęconych bezpieczeństwu wykazała,

że jedna trzecia osób przyznała się do przeglądania informacji poufnych lub osobistych w sposób niezwiązany z wykonywaną pracą.

Utrata danych

Szkodliwe zachowania pracowników, którym do tej pory przyjrzeliśmy się, obejmują celowe niewłaściwe działania. Pracownicy mogą również zagrozić bezpieczeństwu swoich firm poprzez zwykłą nieostrożność, utratę laptopów, dysków optycznych i dysków USB. Nieautoryzowane udostępnianie danych na tych komputerach i nośnikach może być katastrofalne dla firmy. Nawet jeśli dane nie są faktycznie wykorzystywane, fakt, że mogłyby zostać wykorzystane, może wymagać od firmy podjęcia kosztownych działań. Badanie przeprowadzone przez Ponemon w 2010 roku wykazało, że całkowity koszt niepowodującego katastrofalnego naruszenia bezpieczeństwa danych wyniósł 3,4 miliona dolarów. Głównymi przyczynami utraty danych były złośliwe lub przestępcze ataki, zaniedbania, usterki systemu lub błędy osób trzecich.

Inni napastnicy „wewnętrzni”

Pracownicy nie są jedynymi zagrożeniami wewnątrz firmy. Wiele firm zatrudnia pracowników kontraktowych, którzy pracują dla firmy przez krótkie okresy czasu. Pracownicy kontraktowi często uzyskują poświadczenia dostępu, które nie są usuwane po zakończeniu ich zaangażowania. W rzeczywistości firmy często zatrudniają inne firmy do wykonywania prac kontraktowych, które odbywają się wewnątrz murów pierwotnej firmy. Te firmy kontraktowe i ich pracownicy często otrzymują również tymczasowe poświadczenia. Ci pracownicy kontraktowi i firmy kontraktowe stwarzają ryzyko prawie identyczne z ryzykiem stwarzanym przez pracowników

TEST III

a. Podaj cztery powody, dla których pracownicy są szczególnie niebezpieczni.

b. Jaki typ pracownika jest najbardziej niebezpieczny?

c. Co to jest sabotaż?

d. Podaj z wpisów definicję hakowania.

e. Co to jest własność intelektualna?

f. Jakie dwa rodzaje rzeczy mogą ukraść pracownicy?

g. Rozróżnij ogólną własność intelektualną i tajemnice handlowe.

h. Co to jest wymuszenie?

i . Co to jest wykorzystywanie komputera pracowników i Internetu?

j. Kto oprócz pracowników stanowi potencjalne zagrożenie „wewnętrzne”

MALWARE

Chociaż pracownicy i inne „wewnętrzne” zagrożenia mogą być niezwykle niebezpieczni, firmy muszą również obawiać się tradycyjnych zewnętrznych napastników, którzy wykorzystują Internet do wysyłania złośliwego oprogramowania do korporacji, włamywania się do firmowych komputerów i wyrządzania innych szkód.

Twórcy złośliwego oprogramowania

Pierwszymi zewnętrznymi atakującymi szkodliwym oprogramowaniem byli twórcy złośliwego oprogramowania. Termin malware ogólnie oznacza „złe oprogramowanie". Najbardziej znanym rodzajem złośliwego oprogramowania jest wirus komputerowy. Do szkodliwego oprogramowania zalicza się również robaki, konie trojańskie, RAT (trojany zdalnego dostępu), spam i kilka innych typów, które zobaczymy w tej sekcji.

Złośliwe oprogramowanie to ogólny termin określający złe oprogramowanie.

Złośliwe oprogramowanie to bardzo poważne zagrożenie. W czerwcu 2006 r. Microsoft opublikował wyniki ankiety przeprowadzonej wśród użytkowników, którzy zezwolili na skanowanie swoich komputerów w poszukiwaniu złośliwego oprogramowania. Skan wykrył 16 milionów sztuk złośliwego oprogramowania na 5,7 milionach zbadanych maszyn.

Wirusy

Wirusy to programy, które przyłączają się do legalnych programów na komputerze ofiary. Później, gdy zainfekowane programy są przenoszone na inne komputery i uruchamiane, wirus dołącza się do innych programów na tych komputerach. Wirusy to programy, które przyłączają się do legalnych programów. Początkowo większość wirusów rozprzestrzeniała się poprzez transfer programów za pośrednictwem dyskietek. W dzisiejszych czasach wirusy rozprzestrzeniają się za pośrednictwem poczty e-mail z zainfekowanymi załącznikami, komunikatorami, programami do udostępniania plików, zainfekowanymi programami ze złośliwych witryn internetowych, a użytkownicy celowo pobierają „bezpłatne oprogramowanie" lub pornografię. Twórcy wirusów atakują popularne systemy operacyjne i aplikacje, aby zmaksymalizować ich szkody. Dzięki aplikacjom sieciowym wirusy mogą się dziś bardzo szybko rozprzestrzeniać.

Robaki

Wirusy to nie jedyny rodzaj złośliwego oprogramowania. Szczególnie ważnym rodzajem złośliwego oprogramowania jest robak. W przeciwieństwie do wirusów robaki to samodzielne programy, które nie dołączają się do innych programów. Robaki to samodzielne programy, które nie przyłączają się do innych programów. Ogólnie robaki działają podobnie jak wirusy i mogą się rozprzestrzeniać na wiele takich samych sposobów. Jednak niektóre robaki mają znacznie bardziej agresywny tryb rozprzestrzeniania się, przeskakując bezpośrednio z jednego komputera na drugi bez interwencji użytkownika na komputerze odbierającym. Takie robaki rozprzestrzeniające się bezpośrednio wykorzystują luki (luki w zabezpieczeniach) w oprogramowaniu. Gdy robak rozprzestrzeniający się bezpośrednio przeskakuje na komputer, który ma określoną lukę, dla której został zaprojektowany, robak może zainstalować się na tym komputerze i wykorzystać ten komputer jako bazę do przeskakiwania na inne komputery - wszystko to bez żadnych działań ze strony użytkownika część.

Robaki rozprzestrzeniające się bezpośrednio przeskakują bezpośrednio na komputery z lukami w zabezpieczeniach; następnie używają tych komputerów do przeskakiwania do innych komputerów. Bezpośrednia propagacja może być bardzo szybka, umożliwiając robakowi wyrządzenie ogromnych szkód, zanim zostanie wykryty i zatrzymany. Badacze z Uniwersytetu Kalifornijskiego w Berkeley oszacowali, że najgorszy przypadek robaka rozprzestrzeniającego się bezpośrednio może wyrządzić szkody w wysokości 50 miliardów dolarów w samych Stanach Zjednoczonych. Bezpośrednia propagacja nie wymaga żadnych działań ze strony użytkownika, więc robaki rozprzestrzeniające się bezpośrednio mogą rozprzestrzeniać się niezwykle szybko.

Zagrożenia mieszane

Gdyby wirusy i robaki nie były wystarczająco złe, rosnąca liczba zagrożeń mieszanych rozprzestrzenia się zarówno w postaci wirusów, jak i robaków. Mogą również publikować się w witrynach internetowych, aby ludzie mogli nieświadomie pobrać. Zagrożenia mieszane, rozprzestrzeniając się na wiele sposobów, zwiększają prawdopodobieństwo sukcesu. MessageLabs przechowuje dane dotyczące wirusów, robaków i zagrożeń mieszanych. We wrześniu 2010 MessageLabs poinformowało, że 1 na 218 wiadomości e-mail zawiera wirusy, robaki lub mieszane zagrożenia. Oszustwa phishingowe stanowiły 1 na 382 wysłanych e-maili, a 92 procent wszystkich e-maili to spam.

Ładunki

Po rozprzestrzenieniu się wirusów i robaków często wykonują one ładunki, czyli fragmenty kodu, które powodują uszkodzenia. Łagodne ładunki po prostu wyświetlają komunikat na ekranie użytkownika lub powodują inne irytujące, ale nieśmiertelne szkody. Niestety, niektóre wirusy i robaki, które mają pozornie nieszkodliwe ładunki lub nawet nie zawierają żadnych ładunków, mogą wyrządzić znaczne szkody. Na przykład, chociaż Slammer nie zawierał ładunku, rozprzestrzeniał się tak szybko, że zatykał sieci tak dużym ruchem, że skutecznie zamykał części Internetu. Z kolei złośliwe ładunki mogą wyrządzić ogromne szkody, na przykład losowo usuwając pliki z dysku twardego ofiary lub instalując inne typy złośliwego oprogramowania opisane w dalszej części tej sekcji. Ładunki wirusów i robaków również często „zmiękczają" komputer, wyłączając oprogramowanie antywirusowe i podejmując inne działania, które narażają go na późniejsze ataki wirusów i robaków.

TEST IV

a. Co to jest złośliwe oprogramowanie?

b. Rozróżnij wirusy i robaki.

c. W jaki sposób większość wirusów rozprzestrzenia się obecnie między komputerami?

d. Opisz, jak bezpośrednio rozprzestrzeniające się robaki przemieszczają się między komputerami.

e. Dlaczego bezpośrednio rozprzestrzeniające się robaki są szczególnie niebezpieczne?

f. Co to jest ładunek wirusa lub robaka?

Konie trojańskie i rootkity

NIEMOBILNE ZŁOŚLIWE OPROGRAMOWANIE

Wirusy, robaki i mieszane zagrożenia nie są jedynymi typami złośliwego oprogramowania, ale są to jedyne rodzaje złośliwego oprogramowania, które mogą się przekazywać innym ofiarom. Inne formy złośliwego oprogramowania mogą rozprzestrzeniać się na komputer tylko wtedy, gdy zostaną tam umieszczone. Przykłady sposobów na uzyskanie złośliwego oprogramowania innego niż mobilne obejmują:

• Umieszczenie go tam przez hakera

• Umieszczenie wirusa lub robaka w tym miejscu jako część ładunku

• Zachęcanie ofiary do pobrania złośliwego oprogramowania z witryny internetowej lub witryny FTP poprzez przedstawianie złośliwego oprogramowania jako użytecznego programu lub pliku danych

• Dołączanie wrogiego kodu mobilnego (opisanego później) do strony internetowej i wykonywanie go na komputerze ofiary, gdy ofiara pobiera stronę internetową.

KONIE TROJAŃSKIE

Większość szkodliwych programów niemobilnych to konie trojańskie. Wczesne konie trojańskie to programy, które udawały jedną rzecz, takie jak gra lub piracka wersja programu komercyjnego, ale w rzeczywistości były złośliwym oprogramowaniem. Wiele z tych klasycznych koni trojańskich nadal istnieje. Jednak dzisiaj, gdy mówimy o koniu trojańskim, mamy na myśli program, który ukrywa się, usuwając plik systemowy i przejmując nazwę pliku systemowego. Konie trojańskie są trudne do wykrycia, ponieważ wyglądają jak legalne pliki systemowe.

Koń trojański to program, który ukrywa się, usuwając plik systemowy i przejmując nazwę pliku systemowego. Konie trojańskie są trudne do wykrycia, ponieważ wyglądają jak legalne pliki systemowe.

TROJANY ZDALNEGO DOSTĘPU

Jednym z powszechnych typów koni trojańskich jest trojan zdalnego dostępu (RAT). RAT zapewnia atakującemu zdalną kontrolę nad komputerem. Atakujący może zdalnie robić figle, takie jak otwieranie i zamykanie napędu CD lub wpisywanie rzeczy na ekranie. Mogą jednak również angażować się w bardziej złośliwe działania. Istnieje wiele legalnych programów do zdalnego dostępu, które pozwalają zdalnemu użytkownikowi pracować na komputerze lub przeprowadzać diagnostykę. Jednak RAT zazwyczaj działają w ukryciu, aby uniknąć wykrycia przez właściciela maszyny.

DOWNLOADERS

Niektóre konie trojańskie to downloadery (czasami nazywane dropperami). Zwykle są to dość małe programy, co utrudnia wykrycie. Jednak po zainstalowaniu pobierają znacznie większego konia trojańskiego, który może wyrządzić znacznie więcej szkód.

SPYWARE

Termin „spyware" odnosi się do szerokiego spektrum programów typu „koń trojański", które zbierają informacje o użytkowniku i udostępniają je atakującemu. Istnieje kilka rodzajów oprogramowania szpiegującego.

• Pliki cookie to małe ciągi tekstowe przechowywane na komputerze przez witryny internetowe. Następnym razem, gdy wejdziesz na stronę internetową, witryna może pobrać plik cookie. Pliki cookie mają wiele zalet, takich jak zapamiętywanie hasła przy każdej wizycie. Pliki cookie mogą również zapamiętać, co wydarzyło się ostatnio w serii ekranów prowadzących do zakupów. Jednak gdy pliki cookie rejestrują zbyt wiele poufnych informacji o Tobie, stają się oprogramowaniem szpiegującym. (Pliki cookie nie są same w sobie końmi trojańskimi, ale dołączamy je do innych typów oprogramowania szpiegującego).

• Rejestratory naciśnięć klawiszy, znane również jako keyloggery, rejestrują wszystkie naciśnięcia klawiszy. Twoje naciśnięcia klawiszy mogą być następnie przeszukiwane pod kątem nazw użytkowników, haseł, numerów ubezpieczenia społecznego, numerów kart kredytowych i innych poufnych informacji. Mogą wysłać te informacje do atakującego. Niektóre keyloggery mogą rejestrować odwiedzane strony internetowe, uruchamiane programy, a nawet robić zrzuty ekranu w określonych odstępach czasu.

• Oprogramowanie szpiegujące do kradzieży haseł informuje o wylogowaniu z odwiedzanego serwera i prosi o ponowne wpisanie nazwy użytkownika i hasła. Jeśli to zrobisz, oprogramowanie szpiegujące wyśle Twoją nazwę użytkownika i hasło do atakującego.

• Oprogramowanie szpiegujące do eksploracji danych przeszukuje dyski twarde pod kątem tych samych typów informacji, które są poszukiwane przez rejestratory naciśnięć klawiszy. Wysyła również te informacje do przeciwnika.

ROOTKITS

Konie trojańskie zastępują legalne programy. Zagrożenie Adeeper to zestaw programów zwanych rootkitami. Na komputerach z systemem Unix konto root jest kontem superużytkownika, które ma pełną władzę nad komputerem. Chociaż to konto superużytkownika nazywa się Administrator na komputerze z systemem Windows, konta superużytkowników są ogólnie określane jako konta root. Rootkity przejmują konto roota i wykorzystują jego przywileje, aby się ukryć. Robią to głównie poprzez zapobieganie wykrywaniu ich obecności przez metody przeglądania plików ich systemu operacyjnego. Programy typu rootkit rzadko są wychwytywane przez zwykłe programy antywirusowe, a programy do wykrywania rootkitów często są specyficzne dla określonych rootkitów

TEST V

a. W jaki sposób można dostarczyć na komputery złośliwe oprogramowanie inne niż mobilne?

b. Co to jest koń trojański?

c. Co to jest RAT?

d. Co to jest downloader?

e. Co to jest oprogramowanie szpiegowskie?

f. Dlaczego pliki cookie mogą być niebezpieczne?

g. Rozróżnij rejestratory naciśnięć klawiszy, oprogramowanie szpiegujące wykradające hasła i oprogramowanie szpiegujące do eksploracji danych.

h. Rozróżnij konie trojańskie i rootkity.

i . Dlaczego rootkity są szczególnie niebezpieczne?

Kod mobilny

Pobrana strona internetowa może zawierać kod wykonywalny, a także tekst, obrazy, dźwięki i wideo. Nazywa się to kodem mobilnym, ponieważ jest wykonywany na każdym komputerze, na którym pobiera się stronę internetową. Javascript to popularny język do pisania kodu mobilnego. Popularne są również kontrolki Microsoft Active X. W większości przypadków kod mobilny jest niewinny i często jest niezbędny, jeśli użytkownik chce skorzystać z funkcji witryny. Jednak jeśli (i tylko wtedy) komputer ma lukę wykorzystywaną przez określony fragment kodu mobilnego, wrogi kod mobilny będzie w stanie wykorzystać tę lukę.

Inżynieria społeczna w złośliwym oprogramowaniu

Ataki socjotechniczne wykorzystują błędny ludzki osąd, przekonując ofiarę do podjęcia działań sprzecznych z polityką bezpieczeństwa. Na przykład, jeśli pracownik otrzyma wiadomość e-mail z ostrzeżeniem o zbliżającym się zwolnieniu grupowym, może otworzyć załącznik i pobrać wirusa, robaka lub konia trojańskiego. Chociaż technologia może zapewnić wiele zabezpieczeń, firmom bardzo trudno jest chronić się przed błędnymi ocenami ludzi.

Ataki socjotechniczne wykorzystują błędny ludzki osąd, przekonując ofiarę do podjęcia działań sprzecznych z polityką bezpieczeństwa.

SPAM

Zmorą wszystkich użytkowników poczty elektronicznej jest spam, który jest definiowany jako niechciana komercyjna poczta e-mail. Chociaż ISP, korporacyjne i osobiste filtry spamu znacznie zredukowały ilość spamu, ludzie wciąż są bombardowani spamem. Oprócz tego, że są irytujące, wiadomości spamowe często są fałszywe lub reklamują niebezpieczne produkty. Dodatkowo, Spam stał się powszechnym narzędziem dystrybucji wirusów, robaków, koni trojańskich i wielu innych rodzajów złośliwego oprogramowania. Jak wspomniano wcześniej, MessageLabs poinformowało, że we wrześniu 2010 r. 92% wszystkich wiadomości e-mail stanowiło spam. Niektórzy dostawcy usług hostingowych zauważyli podiesienie stawki na 96 procent lub więcej. Nawet obciążenie sieci spowodowane zwykłym przesyłaniem i przechowywaniem spamu może być znaczące. Jest to szczególnie ważne, ponieważ wielu spamerów wysyła obecnie spam zawierający obrazy zamiast treści tekstowych, aby uniknąć wykrycia przez programy do skanowania spamu. Spam ze spamem graficznym jest znacznie większy niż tradycyjne wiadomości tekstowe ze spamem.

PHISHING

W przypadku ataków phishingowych ofiary otrzymują wiadomości e-mail, które wyglądają na pochodzące z banku lub innej firmy, z którą ofiara prowadzi interesy. Wiadomość może nawet skierować ofiarę na autentycznie wyglądającą stronę internetową. Oficjalny wygląd wiadomości i strony internetowej często oszukuje ofiarę do podania poufnych informacji. Niewielki, ale znaczący odsetek wszystkich osób, które otrzymują wiadomości phishingowe, odpowiada na nie, ponieważ wiadomości te wydają się tak autentyczne. Badanie AGartner z 2007 roku wykazało, że konsumenci w USA zostali okradzeni z 3,2 miliarda dolarów w wyniku phishingu w tym roku. Phishing powoduje również wiele kosztownych telefonów do pomocy technicznej w firmach.

SPEAR PHISHING

Normalne ataki phishingowe są zwykle atrakcyjne dla wielu osób, aby mogły oszukać jak najwięcej ofiar. W przeciwieństwie do tego ataki typu spear phishing są wymierzone w pojedyncze osoby lub małe grupy osób. Na przykład, jeśli celem atakującego jest nakłonienie dyrektora generalnego korporacji do pobrania konia trojańskiego, atakujący może stworzyć wiadomość e-mail, która dotyczy pilnej kwestii dla dyrektora generalnego, wydaje się pochodzić od zaufanej osoby i zawiera konkretne szczegóły, które prawdopodobnie zna tylko zaufana osoba.

OSZUSTWA

Niektóre wiadomości e-mail zawierają fałszywe informacje. W niektórych przypadkach te oszustwa po prostu powodują, że ofiara czuje się głupio, gdy mówi innym ludziom, czego się „nauczyła". W innych przypadkach oszustwa próbują przekonać ofiarę do uszkodzenia własnego systemu, usuwając krytyczne pliki systemowe.

TEST VI

a. Co to jest kod mobilny?

b. Co to jest inżynieria społeczna?

c. Co to jest spam?

d. Co to jest phishing?

e. Rozróżnij zwykły phishing i spear phishing.

f. Dlaczego oszustwa są złe?

HAKERZY I ATAKI

W latach siedemdziesiątych do twórców złośliwego oprogramowania dołączyli hakerzy z zewnątrz, którzy zaczęli włamywać się do firmowych komputerów podłączonych do modemów. Obecnie prawie każda firma jest podłączona do Internetu, w którym znajdują się miliony zewnętrznych hakerów. Hakerzy są w stanie włamać się do sieci firmowych, wykraść poufne dane lub wyrządzić szkody w krytycznej infrastrukturze z odległości tysięcy mil.

Tradycyjne motywy

Większość tradycyjnych zewnętrznych hakerów nie powodowała rozległych szkód ani nie dokonywała kradzieży dla pieniędzy. Motywowali ich przede wszystkim dreszczyk emocji związany z włamaniami, potwierdzenie ich umiejętności i poczucie siły. Ponadto zewnętrzni hakerzy często komunikowali się ze sobą. Wykazując zdolność włamywania się do dobrze bronionych hostów, hakerzy mogli zwiększyć swoją reputację wśród swoich rówieśników ,osoba atakująca nadal istnieje. Często tradycyjni hakerzy skupiali się na zawstydzeniu ofiary. Na przykład w 2009 roku wandale włamali się do skomputeryzowanego znaku drogowego w Austin w Teksasie i zmienili jego komunikat na: „Koniec jest blisko! Uwaga! Zombie przed nami! ”50 Jednak wielu tradycyjnych zewnętrznych hakerów angażuje się w bezpośrednie kradzieże, wymuszenia i inne szkody, aby wesprzeć swoje„ hobby.

TEST VII

a. Jakie były motywacje tradycyjnych zewnętrznych hakerów?

b. Czy tradycyjni hakerzy zewnętrzni zaangażowali się w kradzież?

Anatomia włamania

Chociaż istnieje wiele różnych sposobów włamania się do komputera, istnieje ogólny proces, który często stosują osoby atakujące, próbując włamać się do firmowych komputerów. Jest to podobne do tego, co zrobiłby złodziej, gdyby chciał fizycznie ukraść firmowe komputery.

WYBÓR CELU

Haker może losowo przeszukać wszystkie możliwe firmy w celu znalezienia potencjalnego celu lub wyszukać konkretną firmę po nazwie. Nazwę domeny firmy można rozpoznać za pomocą prostego wyszukiwania WHOIS (www.whois.net). Korporacje zazwyczaj mają bloki ciągłych adresów IP, które przydzielają komputerom wewnętrznym. Gdy haker zna zakres docelowych adresów IP, może rozpocząć badanie sieci w poszukiwaniu podatnych hostów.

SONDY REKONESANSOWE

Zanim złodziej włamie się do domu, często „szuka” okolicznych domów w poszukiwaniu zagrożonych domów. Atakujący zbiera następnie informacje o potencjalnych domach ofiar, aby zdecydować, do których z nich się włamać. Hakerzy mają również tendencję do przeprowadzania rozpoznania przed włamaniem do komputera. Atakujący często wysyła pakiety sondujące do sieci. Te pakiety sondujące są przeznaczone do wywoływania odpowiedzi z wewnętrznych hostów i routerów. Jeśli hosty wewnętrzne lub routery odpowiedzą na te pakiety sondujące, ich odpowiedzi mogą wiele powiedzieć atakującemu o sieci.

Skanowanie adresów IP: Pierwsza runda pakietów sondujących ma na celu znalezienie aktywnych hostów. Atakujący wysyła sondy skanujące adresy IP na wszystkie adresy IP w docelowym zakresie.

Sondy te często używają komunikatów odpowiedzi echa i echa protokołu ICMP (Internet Control Message Protocol) omówione w module A. Gdy host otrzyma komunikat ICMP Echo, powinien odesłać komunikat odpowiedzi ICMP Echo. Gdy atakujący otrzyma wiadomość odpowiedzi ICMP Echo z adresu IP, wie, że pod tym adresem IP znajduje się aktywny host.

Skanowanie portów: gdy osoba atakująca zna adresy IP aktywnych hostów, musi wiedzieć, jakie programy działają na zidentyfikowanych hostach, ponieważ większość ataków opiera się na lukach w określonych programach. Na hostach serwerów aplikacje odpowiadają numerom portów. Używając metafory „domu", port byłby odpowiednikiem drzwi w domu. Na przykład 80 to dobrze znany numer portu dla serwerów WWW HTTP. Jeśli port 80 jest otwarty, komputer jest prawdopodobnie serwerem WWW. Istnieje wiele dobrze znanych numerów portów od 0 do 1023. Każdy z nich wskazuje na obecność określonego typu aplikacji. Atakujący wysyła sondy skanujące porty do każdego zidentyfikowanego hosta w celu określenia, które aplikacje są na nim uruchomione. Zazwyczaj program skanujący porty żąda połączenia z programem na porcie o określonym numerze.54 Jeśli cel odeśle zgodę na kontynuację, atakujący wie, że host docelowy uruchamia program na porcie o tym numerze.

EXPLOITY

Po zidentyfikowaniu potencjalnych hostów i portów ofiary można rozpocząć atak. W tym przypadku atakujący wysyła pakiety exploitów do hostów ofiary zamiast pakietów sondujących. Specyficzna metoda ataku używana przez atakującego do włamania się do komputera nazywana jest exploitem atakującego, a czynność polegająca na implementacji exploita nazywana jest wykorzystaniem hosta. Jeśli exploit powiedzie się, osoba atakująca „posiada" przynajmniej konto i może „posiadać" sam komputer. Posiadanie komputera pozwala napastnikowi robić wszystko, czego sobie życzy.

SPOOFING

Każdy pakiet zawiera źródłowy adres IP, który jest jak adres zwrotny na kopercie. Źródłowy adres IP jest niebezpieczny dla hakerów, ponieważ umożliwia korporacjom zlokalizowanie atakujących. Atakujący mogą udaremnić próby ich znalezienia, podszywając się pod źródłowy adres IP, czyli umieszczając inny adres IP w polu źródłowego adresu IP. W ten sposób ofiara nie może poznać prawdziwego adresu IP atakującego. Nie wszystkie pakiety można sfałszować. Na przykład osoba atakująca zwykle musi być w stanie odczytać odpowiedzi na pakiety sondujące. Odpowiedzi ofiar są zawsze wysyłane do hosta, którego adres IP znajduje się w polu źródłowego adresu IP sondy. Jeśli atakujący sfałszuje adres IP w pakietach sondujących, nie otrzyma odpowiedzi. Wiele exploitów musi również otrzymać odpowiedź, aby odnieść sukces. Atakujący, którzy muszą otrzymać odpowiedzi, często korzystają z łańcucha atakujących komputerów, które zostały wcześniej przejęte przez atakującego. Polecenia są przekazywane przez łańcuch do końcowego komputera, który wysyła sondę lub pakiety ataku. Odpowiedzi są również przekazywane przez łańcuch z powrotem do atakującego. Ofiara zwykle będzie w stanie prześledzić atak do ostatniego komputera w łańcuchu i być może do jednego lub dwóch więcej hostów w łańcuchu. Rzadko kiedy ofiara może prześledzić całą drogę ataku do hosta atakującego, ponieważ łańcuch komputerów przechodzi przez wiele firm, stanów i krajów.

TEST VIII

a. Rozróżnij skanowanie adresów IP i skanowanie portów.

b. Co to jest exploit?

c. Co oznacza „posiadanie" komputera?

d. Co to jest fałszowanie adresu IP?

e. Dlaczego odbywa się fałszowanie adresu IP?

f. Kiedy osoba atakująca nie może używać fałszowania adresu IP?

g. Kiedy atakujący muszą używać prawidłowych adresów źródłowych IP w protokołach sondujących lub exploitów, w jaki sposób mogą ukrywać swoją tożsamość?

Inżynieria społeczna w ataku

Wiele zewnętrznych (i wewnętrznych) ataków wykorzystuje socjotechnikę, która, jak widzieliśmy wcześniej, ma na celu nakłonienie użytkowników do zrobienia czegoś, co jest sprzeczne z interesem bezpieczeństwa. W porównaniu z zabezpieczeniami technicznymi łatwowierność człowieka jest często znacznie łatwiejsza do wykorzystania. Na przykład haker dzwoni do sekretarki, która twierdzi, że współpracuje z jej szefem. Następnie haker prosi o poufne informacje, takie jak hasło, a nawet plik z ograniczeniami. Inne przykłady inżynierii społecznej obejmują podążanie za kimś przez bezpieczne drzwi bez wprowadzania kodu dostępu (nazywa się to piggybacking) i patrzenie przez ramię, gdy wpisuje hasło (nazywa się to surfowaniem przez ramię). W ramach pretekstu, atakujący dzwoni podając się za określonego klienta, aby uzyskać prywatne informacje o tym kliencie.

TEST IX

a. W jaki sposób można wykorzystać inżynierię społeczną, aby uzyskać dostęp do poufnego pliku?

b. Co to jest piggybacking?

d. Co to jest surfing przez ramiona?

e. Co to jest pretekst?

Ataki typu „odmowa usługi”

Innym rodzajem ataku zewnętrznego jest atak typu „odmowa usługi” (DoS). Atak DoS ma na celu uniemożliwienie dostępu do serwera lub sieci uprawnionym użytkownikom. W odniesieniu do omówionej wcześniej taksonomii celów bezpieczeństwa CIA, ataki DoS są atakami na dostępność.

Atak typu „odmowa usługi” (DoS) ma na celu uniemożliwienie dostępu do serwera lub sieci uprawnionym użytkownikom poprzez zalewanie ich pakietami ataków.

Najczęstszy rodzaj ataku DoS, to atak rozproszona odmowa usługi (DDoS). W tym exploicie atakujący najpierw umieszcza programy zwane botami na wielu hostach internetowych (klientach, serwerach lub obu). Później, gdy nadejdzie czas na rozpoczęcie ataku DoS, botmaster (lub handler) wysyła wiadomość do wszystkich botów. Następnie boty zaczynają zalewać serwer lub sieć wymienioną w komunikacie o ataku pakietami ataku. Wkrótce przeciążone serwery i sieci nie będą mogły służyć swoim legalnym użytkownikom. Na przykład, aby zaatakować serwer, boty mogą zalać serwer żądaniami otwarcia połączenia TCP (segmenty TCP SYN). Serwer rezerwuje określoną ilość mocy za każdym razem, gdy otrzymuje segment SYN. Zalewając komputer segmentami SYN, osoba atakująca może spowodować wyczerpanie zasobów serwera, a tym samym awarię lub niemożność odpowiedzi na dalsze próby otwarcia połączenia od uprawnionych użytkowników. Jeśli strumień ataku jest szczególnie intensywny, cała sieć korporacji ofiary nie będzie mogła komunikować się przez Internet. Istnieją inne sposoby wykonania ataku DoS. W rozdziale 4 przyjrzymy się dodatkowym metodom ataków DoS i sposobom łagodzenia ich skutków. Przyjrzy się również innym typom ataków sieciowych, takim jak ARP Poisoning, oraz sposobom zabezpieczenia sieci przed atakami z zewnątrz.

TEST X

a. Co to jest atak DoS?

b. Opisz atak DDoS.

d. Opisz szczegółowo atak SYN flooding.

e. Dlaczego wiele botnetów ma z czasem wielu właścicieli?

Poziomy umiejętności

Filmy z Hollywood często przedstawiają hakerów jako geniuszy, którzy potrafią włamać się na ściśle chronione serwery w ciągu kilku sekund. W rzeczywistości wysoko wykwalifikowani hakerzy zwykle potrzebują dni lub nawet miesięcy ciężkiej pracy, aby włamać się do dobrze chronionego systemu - jeśli w ogóle im się uda. W tym czasie będą próbowali wielu różnych ataków. Innymi słowy, wykwalifikowani hakerzy charakteryzują się zarówno dużą wiedzą techniczną, jak i zawziętą wytrwałością. Aby zautomatyzować niektóre aspekty swoich ataków, hakerzy często piszą programy zwane skryptami hakerskimi. Termin skrypt tradycyjnie oznacza dość prymitywny program napisany prostym językiem. Dzisiejsze skrypty hakerów mają jednak często łatwe w użyciu graficzne interfejsy użytkownika i wyglądają jak oprogramowanie komercyjne. Ponadto zautomatyzowane skrypty i oprogramowanie hakerów są łatwo dostępne w Internecie. Te łatwe w użyciu skrypty hakerskie stworzyły nowy typ hakera – script kiddies. Jest to obraźliwe określenie, które wykwalifikowani hakerzy nadają stosunkowo niewykwalifikowanym hakerom, którzy używają tych gotowych skryptów. Chociaż indywidualnie script kiddies mają znacznie mniejsze szanse na włamanie się do komputera niż wykwalifikowani hakerzy, jest o wiele więcej script kiddies niż wykwalifikowanych hakerów. To sprawia, że script kiddies jako społeczność są niezwykle niebezpieczni. Ponadto duża liczba ataków typu script kiddies utrudnia korporacjom zidentyfikowanie niewielkiej liczby bardzo niebezpiecznych ataków, na które napotykają firmy ze strony bardzo wykwalifikowanych napastników i które wymagają szczególnej uwagi. W lipcu 2002 r. Firma Riptech (obecnie należąca do Symantec Corp.) szczegółowo przeanalizowała dane 400 swoich klientów. Zauważył, że tylko około 1 procent ataków stanowiły wyrafinowane ataki agresywne. Jednak gdy pojawiły się wyrafinowane agresywne ataki, były one 26 razy bardziej narażone na poważne szkody niż nawet umiarkowanie wyrafinowane agresywne ataki. Twórcy wirusów i innych złośliwych programów również napisali programy do tworzenia nowego złośliwego oprogramowania. Tworzenie wirusów za pomocą tych narzędzi stało się tak łatwe, że Sven Jaschan, 18-letni niemiecki student, który nigdy wcześniej nie napisał wirusa, był odpowiedzialny za 70% aktywności wirusa w pierwszej połowie 2004 roku (http: // www.sophos.com). Obecnie dostępne są narzędzia do tworzenia wszelkiego rodzaju exploitów. Jeden z najważniejszych to Metasploit Framework, który ułatwia przyjęcie nowej metody eksploatacji i szybko przekształca ją w pełny program ataku. Metasploit jest używany zarówno przez osoby atakujące do przeprowadzania ataków, jak i przez specjalistów ds. bezpieczeństwa do testowania podatności ich systemów na określone exploity.

TEST XI

a. Jakie są dwie główne cechy wykwalifikowanych hakerów?

b. Dlaczego dzieciaki skryptów są niebezpieczne? (Podaj dwa powody.)

c. Dlaczego złośliwe oprogramowanie i zestawy narzędzi do exploitów zwiększają zagrożenie związane ze skryptami dzieciaków?

ERA KRYMINALNA

Dominacja przez karierę przestępców.

Przed około 2003 rokiem większość zewnętrznych napastników stanowili pracownicy, byli pracownicy lub tradycyjni napastnicy zewnętrzni zainteresowani jedynie sławą i poczuciem władzy. Obecnie jednak większość zewnętrznych napastników to przestępcy zawodowi, którzy atakują, aby nielegalnie zarabiać pieniądze. Mają tradycyjne motywy kryminalne, a wiele z ich strategii ataku to komputerowe adaptacje tradycyjnych przestępstw.

Obecnie większość zewnętrznych napastników to przestępcy zawodowi.

Wbrew powszechnemu przekonaniu przestępcy nie zwlekają z korzystaniem z nowych technologii. W 1888 roku inspektor John Bonfield z policji w Chicago powiedział: „Jest dobrze znanym faktem, że żadna inna część populacji nie korzysta łatwiej i szybciej z najnowszych triumfów nauki niż klasa przestępcza". W latach trzydziestych John Dillinger i wielu innych przestępców wykorzystywało niedrogie samochody do rabowania banków i znikania, zanim policja zdążyła ich zatrzymać. Tablice rejestracyjne zostały wprowadzone przede wszystkim po to, by pomóc policji i zmniejszyć zalety mobilnych przestępców. Ponadto przestępcy nie rozróżniają między różnymi rodzajami przestępstw. Na przykład w 2003 r. Firma VeriSign zbadała adresy IP, z których nadeszły ataki. Okazało się, że istnieje silna korelacja między adresami IP używanymi podczas hakowania a adresami wykorzystywanymi w oszustwach. Aby podać inny przykład, policja, która przeszukiwała miejsca wykorzystywane do kradzieży tożsamości, znalazła fajki metanowe i inne materiały wskazujące na to, że przestępcy byli uzależnieni od metamfetaminy, wykorzystując kradzież tożsamości online w celu wsparcia swoich nałogów. Kradli informacje i sprzedawali je innym grupom przestępczym.

Cyberprzestępczość

Cyberprzestępczość - wykonywanie przestępstw w Internecie - stała się niezwykle dużym problemem w bardzo krótkim czasie. Według Departamentu Skarbu USA w 2005 r. Liczba postępowań dotyczących cyberprzestępczości przewyższyła liczbę postępowań dotyczących nielegalnej sprzedaży narkotyków63. W 2004 r. Przestępstwa internetowe stanowiły zaledwie 1,3% wszystkich zarejestrowanych przestępstw w Niemczech, ale stanowiły 57 procent szkód materialnych spowodowanych przez przestępstwa. W 2009 roku do FBI wpłynęło 336655 skarg dotyczących przestępstw związanych z Internetem, w których odnotowano straty w wysokości 559,7 miliona dolarów.65 Cyberprzestępczość nie staje się ważnym problemem dla bezpieczeństwa w Internecie. Stał się już dominującym problemem.

MIĘDZYNARODOWE GANGI

Ze względu na wzajemne powiązania Internetu granice państwowe i paszporty nie mają znaczenia. W rezultacie przedsiębiorstwa przestępcze mogą swobodnie popełniać różnorodne cyberprzestępstwa, nie martwiąc się, że zagraniczne kraje będą je ścigać za przestępstwa popełnione przeciwko ofiarom na ich terytorium. Kiedy dochodzi do ścigania, zazwyczaj dzieje się tak tylko dzięki kreatywności prokuratorów. Jednym z problemów międzynarodowych gangów jest to, że wielu sprzedawców internetowych nie wysyła przesyłek poza Stany Zjednoczone. Aby obejść ten problem, gangi przestępcze angażują przeładunkowych w Stanach Zjednoczonych. Osoby te odbierają wysłane towary w biurach USA, a następnie wysyłają je do gangu przestępczego w innym kraju. Za każdą przeładowaną paczkę przeładunkowi płaci się opłatę. Często przeładunki są pozyskiwane przez Internet i nigdy nie zdają sobie sprawy, że robią cokolwiek, aby pomóc przestępcy. Podobnie, międzynarodowe gangi używają mułów pieniężnych do przesyłania pieniędzy (w zamian za niewielką opłatę procentową płaconą mułowi pieniężnemu). Często przeładunki i muły pieniężne są rekrutowani za pośrednictwem internetowych witryn z ofertami pracy.

CZARNE RYNKI I SPECJALIZACJA RYNKOWA

Tradycyjni przestępcy zawsze współpracowali. Na przykład paserzy kupują skradzione towary od złodziei po obniżonej cenie, a następnie odsprzedają je jako pozornie legalne punkty sprzedaży, w których pochodzenie towarów nie będzie oczywiste. Na całym świecie istnieje wiele stron internetowych zawierających skradzione informacje konsumenckie. Istnieją nawet aktualne stawki za numery kart kredytowych, których cena jest określana na podstawie tego, jak dobrze numery kart zostały zweryfikowane, na przykład dokonując niewielkiego zakupu z każdym numerem karty, aby upewnić się, że numer jest aktywny. Większość czarnych rynków zajmuje się informacjami dotyczącymi kart kredytowych i tożsamości. Istnieją jednak również czarne rynki dla złośliwego oprogramowania, botnetów i nowo odkrytych luk w zabezpieczeniach. Kiedy analityk odkrywa lukę w zabezpieczeniach w oprogramowaniu, zwykle powiadamia firmę programistyczną, która przyznaje analitykowi kredyt po wydaniu poprawki. Jednak firmy produkujące oprogramowanie rzadko płacą odkrywcom luk. W rezultacie rosnąca liczba analityków sprzedaje informacje o odkryciach luk na jednym z kilku czarnych rynków. Inni programiści piszą oprogramowanie exploit i sprzedają je na czarnych rynkach. Obecnie w większości przypadków oprogramowanie służące do wykorzystywania luk jest sprzedawane z zapewnieniem pomocy technicznej online i bezpłatnych aktualizacji. Po zakupie płatności mogą być nawet przechowywane na rachunku escrow, dopóki kupujący nie przetestuje oprogramowania eksploatacyjnego. Pod wieloma względami cyberprzestępczość dojrzewa, podobnie jak wiele tradycyjnych rynków. Na początku na nowym rynku zwykle dominują firmy typu all-in-one. Później pojawiła się specjalizacja pionowa i pozioma. W cyberprzestępczości niektórzy przestępcy szukają exploitów, inni opracowują zestawy narzędzi, inni specjalizują się w dystrybucji i zarządzaniu botnetami, jeszcze inni prowadzą rynki kradzieży tożsamości i numerów kart kredytowych, a jeszcze inni tworzą wspólne kody i biblioteki. Z biegiem czasu szybko pojawiają się nowe nisze rynkowe.

TEST XII

a. Jaki jest obecnie dominujący typ napastnika?

b. Czy cyberprzestępczość jest dziś nieistotna w porównaniu z przestępstwami niezwiązanymi z komputerami?

c. Dlaczego międzynarodowe gangi są trudne do ścigania?

d. Dlaczego międzynarodowe gangi używają przeładunków?

e. Jak używają przeładunków?

f. Jak używają mułów pieniężnych?

Oszustwo, kradzież i wymuszenie

Oszustwa, kradzieże i wymuszenia to tradycyjne ataki przestępcze. Dzisiaj przestępcy nauczyli się wykonywać te przestępstwa za pośrednictwem sieci.

OSZUSTWO

Przestępcy próbują nielegalnie zdobyć pieniądze na wiele sposobów. Wymienimy tylko kilka. Jedną z cech charakterystycznych wielu z tych ataków przestępczych jest to, że obejmują oszustwa. W przypadku oszustwa napastnik oszukuje ofiarę, aby zrobiła coś wbrew interesom finansowym ofiary. Na przykład w podanym później przykładzie T-Data napastnik oszukał firmę, aby przekazała mu sprzęt, udając, że jest prawdziwą firmą, która zapłaci.

W przypadku oszustwa napastnik oszukuje ofiarę, aby zrobiła coś wbrew interesom finansowym ofiary.

Nie ma nic nowego w oszustwach. W świecie fizycznym oszustwa są popełniane od początku istnienia ludzkości. Cyberprzestępcy po prostu uczą się, jak przeprowadzać klasyczne oszustwa w sieciach komputerowych. Na przykład większość wiadomości spamowych wykorzystuje klasyczne metody oszustwa i ma klasyczne cele. W innych przypadkach przestępcy tworzą nowe oszustwa specyficzne dla sieci. Na przykład wiele witryn otrzymuje płatności od reklamodawców za kliknięcie. Za każdym razem, gdy odwiedzający witrynę kliknie łącze reklamowe w witrynie, reklamodawca płaci za oryginalną witrynę niewielką opłatę. W przypadku oszustw związanych z kliknięciami właściciel przestępczej witryny tworzy program do wielokrotnego klikania odsyłacza. Każde z tych fałszywych kliknięć zabiera reklamodawcy pieniądze bez generowania potencjalnych klientów.

KRADZIEŻ FINANSOWA I INTELEKTUALNA

Tak jak przestępcy zawodowi od dawna włamywali się do domów i rabowali banki, tak przestępcy zawodowi w Internecie dopuszczają się kradzieży finansowych. W innych przypadkach przestępcy zawodowi kradną własność intelektualną firmy w celu sprzedaży innym przestępcom lub konkurentom korporacyjnym. Jak wspomniano wcześniej w tym rozdziale, własność intelektualna składa się z formalnie chronionych informacji, takich jak patenty i inne informacje oraz tajemnice handlowe, które są wrażliwymi informacjami, które firma podejmuje, aby chronić, takie jak plany korporacyjne, a nawet cenniki. Według sondażu Price Waterhouse Coopers, nawet w 1999 roku firmy z listy Fortune 1000 straciły ponad 45 miliardów dolarów w wyniku kradzieży tajemnic handlowych. Działo się to na długo zanim kradzież własności intelektualnej przez Internet stała się poważnym zagrożeniem.

WYMUSZANIE Z KORPORACJI

Wymuszenie polega na użyciu groźby krzywdy, aby skłonić ofiarę do zapłacenia pieniędzy, aby uniknąć krzywdy. Wymuszenie od dawna jest podstawą ataków przestępczych w prawdziwym świecie. Jednym ze sposobów wykorzystania IT do wymuszenia na firmie jest grożenie jej atakiem, chyba że zostanie zapłacona opłata za ochronę. Czasami, gdy przestępca kradnie informacje, wymusza na firmie grożenie ujawnieniem informacji, chyba że zapłacone zostaną „ciche pieniądze". W wielu przypadkach negatywny rozgłos generowany, gdy haker ujawnia skradzione informacje, może być bardziej szkodliwy niż koszt finansowy samej informacji. Firmy mogą tracić klientów, ponieważ są postrzegane jako niechętne lub niezdolne do ochrony informacji o klientach.

TEST XIII

a. Co to jest oszustwo?

b. Co to jest fałszywe kliknięcie?

c. W jaki sposób przestępcy dokonują wymuszeń online?

Kradzież poufnych danych o klientach i pracownikach

Przestępcy mają tendencję do poszukiwania „miękkich celów", które dają duże zyski przy niewielkim wysiłku. Często oznacza to kierowanie reklam do pojedynczych osób, a nie do korporacji. Przyjrzymy się kilku atakom na osoby w kolejności rosnącej dotkliwości.

CARDING

Prawdopodobnie najczęstszym przestępczym atakiem na osoby fizyczne jest kradzież numeru karty kredytowej - praktyka znana jako carding. Carderzy „trafiają w dziesiątkę", jeśli poznają numer karty kredytowej, imię i nazwisko właściciela karty oraz trzycyfrowy numer weryfikacyjny karty. Gdy złodziej uzyska informacje, których potrzebuje, może dokonywać zakupów do momentu unieważnienia karty.

Na szczęście, jeśli ofiary kart kredytowych szybko zgłoszą oszustwo związane z numerem karty kredytowej, zgodnie z prawem Stanów Zjednoczonych są zobowiązane do zapłacenia tylko 50 USD, a większość sprzedawców kart kredytowych zrzeka się nawet tej odpowiedzialności.

KRADZIEŻ RACHUNKU BANKOWEGO

Jeśli jednak złodziej ukradnie dane uwierzytelniające wymagane do przeprowadzenia transakcji online w imieniu ofiary, może on opróżnić konto bankowe ofiary. Kradzież konta bankowego jest poważniejsza niż kradzież numeru karty kredytowej.

KRADZIEŻ KONTA ONLINE

W 2006 roku przestępcy zaczęli kradnąć internetowe konta giełdowe ze względu na luki w zabezpieczeniach w witrynach giełdowych. Zamiast ukraść kilkaset dolarów za pomocą skradzionych kart kredytowych, kradzieże kont giełdowych często sięgały tysięcy dolarów.

KRADZIEŻ TOŻSAMOŚCI

Jeśli złodziej może ukraść jeszcze więcej informacji, może zaangażować się w kradzież tożsamości, podczas której złodziej podszywa się pod ofiarę na tyle dobrze, aby zaangażować się w duże transakcje finansowe. Transakcje te mogą obejmować zaciąganie dużych pożyczek i dokonywanie dużych zakupów w imieniu ofiary. Ofiary kradzieży tożsamości mogą ponieść ogromne szkody, a niektóre z nich zostały nawet aresztowane za działania złodziei tożsamości. Kradzież tożsamości jest znacznie poważniejsza niż kradzież numeru karty kredytowej. Przestępcy od dawna kradną informacje o tożsamości konsumentów bez korzystania z komputerów. Na przykład, karty kredytowe tradycyjnie zapisywali numery kart kredytowych podczas zakupów w sklepach detalicznych. Jednak dzięki sieciom komputerowym złodzieje byli w stanie wykraść informacje o tożsamości konsumentów setek, tysięcy, a nawet milionów ofiar. Najczęściej hakerzy włamują się do słabo chronionych komputerów firmowych, aby wykraść te informacje. Jednak zgubione lub skradzione laptopy i taśmy z kopiami zapasowymi są również kopalnią złota dla złodziei informacji konsumenckich. Ponadto często w grę wchodzą nieuczciwi insiderów. W 2006 roku firma Gartner przeprowadziła ankietę wśród 5000 klientów banków w USA. Na podstawie danych z ankiety firma Gartner oszacowała, że 3 miliony Amerykanów padło ofiarą oszustw internetowych w ciągu ostatnich sześciu lat i że każdy z nich stracił średnio 900 dolarów. Inne badanie wykazało średnią stratę prawie 4000 USD, wykazało, że ofiary spędzały średnio 81 godzin na próbach rozwiązania swoich spraw i wykazało, że jedna czwarta nigdy nie została w pełni odzyskana. Niektóre straty mogą być znacznie gorsze, na przykład, jeśli złodziej tożsamości prawo własności do domu ofiary dla siebie, a następnie sprzedaje dom.

POŁĄCZENIE KORPORACYJNE

Karta, kradzież konta bankowego i kradzież tożsamości to nie tylko problemy konsumentów. To także problemy korporacyjne. Kiedy firmy zgłaszają, że włamano się do ich baz danych klientów i że tysiące lub miliony osób otrzymały informacje o ich tożsamości, reakcje klientów i inwestorów mogą być znaczne. Ponadto firmom mogą grozić sankcje rządowe. Na przykład w Stanach Zjednoczonych Federalna Komisja Handlu ma szerokie uprawnienia do nakładania kar na firmy, które nie wdrażają odpowiednio ochrony danych klientów. Komisja może również zlecić drogie niezależne audyty postępowania firmy z prywatnymi informacjami przez dziesięć lub więcej lat po wystąpieniu problemu. Wreszcie, poważne naruszenia często obejmują zwolnienie menedżerów funkcjonalnych odpowiedzialnych za naruszone systemy.

KRADZIEŻ TOŻSAMOŚCI FIRMY

Chociaż kradzież tożsamości zdarza się najczęściej osobom fizycznym, może się również zdarzyć w korporacjach. Zbierając informacje o firmie w Internecie, złodzieje tożsamości korporacyjnej mogą ubiegać się o firmowe karty kredytowe, otrzymywać je i używać w imieniu firmy będącej ofiarą. Mogą również przyjmować zamówienia kartą kredytową w imieniu firmy ofiary. Mogą nawet złożyć dokumenty, aby zmienić adres prawny firmy będącej ofiarą przestępstwa i zmienić imię i nazwisko osoby zarządzającej firmą.

TEST XIV

a. Co to jest carding?

b. Opisz kradzież konta bankowego i kradzieży konta online.

c. Rozróżnij kradzież karty kredytowej i kradzież tożsamości.

e. Dlaczego kradzież tożsamości jest poważniejsza niż kradzież numeru karty kredytowej?

f. W jaki sposób przestępcy zwykle uzyskują informacje potrzebne do kradzieży karty kredytowej i kradzieży tożsamości?

g. W jaki sposób firmy mogą zostać skrzywdzone, jeśli pozwolą na kradzież danych osobowych, nad którymi mają kontrolę?

h. Co to jest kradzież tożsamości korporacyjnej?

ZAGROŻENIA KONKURENCJI

Konkurenci korporacyjni również mogą być atakującymi. Mogą angażować się w wiele rodzajów ataków. Skoncentrujemy się na atakach na poufność i dostępność.

Szpiegostwo handlowe

W przypadku gromadzenia informacji publicznych konkurent przejrzy witrynę internetową firmy i inne informacje publiczne, aby znaleźć dane, które sama firma poszkodowana ujawnia. Konkurent może również sprawdzać strony na Facebooku pod kątem pracowników i innych informacji publicznych. Odnotowano kilka spraw sądowych w celu zbadania legalności takich działań, ale z definicji tajemnice handlowe są chronione prawem tylko wtedy, gdy firma podejmuje rozsądne wysiłki, aby zachować je w tajemnicy. Należy pamiętać, że herkulesowe wysiłki nie są konieczne, a jedynie rozsądne, które odzwierciedlają wrażliwość aktywów i praktyk bezpieczeństwa w branży.

Tajemnice handlowe są chronione prawem tylko wtedy, gdy firma podejmuje rozsądne starania, aby zachować je w tajemnicy.

Częstym celem ataków korporacyjnych jest nielegalna kradzież tajemnic handlowych firmy - praktyka zwana szpiegostwem tajemnicy handlowej. W najbardziej rażącej formie konkurent przechwyci komunikację firmy ofiary, zhakuje jej serwery lub przekupi pracownika firmy ofiary w celu kradzieży informacji. Lub może zatrudnić jednego z Twoich byłych pracowników i zażądać lub zaakceptować Twoje tajemnice handlowe od tej osoby. Szpiegostwo komercyjne nie ogranicza się do konkurentów korporacyjnych. Podobno od zakończenia zimnej wojny wiele krajowych agencji wywiadowczych przeszło do szpiegostwa handlowego. Robert Gates, dyrektor CIA w latach 1991–1993, poinformował, że rządowe szpiegostwo gospodarcze jest szeroko rozpowszechnione83. Wskazał on szczególnie Francję, Rosję, Chiny, Koreę Południową, Niemcy, Izrael, Indie i Pakistan jako zaangażowane w intensywne szpiegostwo korporacyjne. W 2007 roku w rocznym raporcie amerykańsko-chińskiej

komisji ds. Przeglądu gospodarczego i bezpieczeństwa dla Kongresu stwierdzono, że „chińska działalność szpiegowska w USA jest tak rozległa, że stanowi największe zagrożenie dla bezpieczeństwa amerykańskich technologii".

Ataki typu „odmowa usługi"

Konkurenci mogą również angażować się w różnego rodzaju ataki na Twoją firmę, takie jak ataki DoS. Chociaż te ataki na dostępność są rzadkie, mogą być katastrofalne dla firm, które polegają na dochodach z działalności online.

TEST XV

a. Należy rozróżnić między zbieraniem informacji publicznej a szpiegostwem tajemnicy handlowej

b. Co firma musi zrobić ze swoimi tajemnicami handlowymi, jeśli chce mieć możliwość ścigania osób lub firm, które ją kradną?

c. Jak silne muszą być te zabezpieczenia?

d. Kto może prowadzić szpiegostwo przeciwko firmie?

CYBERWOJNA I CYBERTERROR

Przestępcy stanowią poważne zagrożenie dla korporacji. Jednak ataki cyberterrorystów mogą wyrządzić szkody na znacznie większą skalę niż te spowodowane atakami przestępczymi. Są to ataki zorganizowanych grup terrorystycznych, a nawet rządów krajowych. Ataki te mogą mieć bezprecedensową skalę, na którą przygotowanych jest niewiele korporacyjnych planów bezpieczeństwa.

Cyberwojna

Dzisiaj, kiedy kraje idą na wojnę, używają broni i bomb. Jednak mogą również wyrządzić ogromne szkody za pomocą komputerów.

Cyberwojna to ataki komputerowe dokonywane przez rządy krajowe.

Przed rozpoczęciem działań wojennych walczący mogą zaangażować się w szpiegostwo komputerowe, aby poznać sekrety swoich przeciwników. Chiny są szczególnie aktywne w szpiegostwie cyberwojennym. Szpiegostwo cybernetyczne z Chin stanowi poważny problem od 1999 r. Rząd chiński był zaangażowany w ataki wymierzone w Departament Stanu, Departament Handlu, senatorów, kongresmenów i laboratoria wojskowe Stanów Zjednoczonych lub był ich sponsorem. Ataki cyberwojenne mogą być przeprowadzane bez angażowania się w działania fizyczne i nadal powodują ogromne szkody. Kraje mogą użyć ataków cyberwojny, aby wyrządzić ogromne szkody jednemu w infrastrukturze finansowej innej osoby, aby zakłócać wzajemne infrastruktury komunikacyjne i uszkadzać infrastrukturę informatyczną kraju, a wszystko to w charakterze prekursorów rzeczywistych fizycznych działań wojennych.

Cyberterror

Kolejnym koszmarnym scenariuszem jest cyberterror, w którym napastnikiem jest terrorysta lub grupa terrorystów. Oczywiście cyberterroryści mogą bezpośrednio atakować zasoby technologii informacyjnej. Mogą uszkodzić infrastrukturę finansową, komunikacyjną i użyteczności publicznej kraju. Najczęściej cyberterroryści wykorzystują Internet jako narzędzie rekrutacji za pośrednictwem stron internetowych i koordynowania swoich działań. Mogą również wykorzystywać cyberterror w połączeniu z fizycznymi atakami, na przykład zakłócając systemy komunikacyjne służb ratowniczych lub

zakłócając energię elektryczną w celu spowodowania korków i zwiększenia terroru. Bardziej subtelnie, ale równie niebezpiecznie, wiele organizacji terrorystycznych zwraca się do przestępstw komputerowych, aby finansować swoją działalność terrorystyczną, tak jak zwracają się do niewolniczej prostytucji i innych przestępstw fizycznych.

TEST XVI

a. Rozróżnij cyberwojnę i cyberterror.

b. W jaki sposób kraje mogą wykorzystywać ataki cyberwojny?

c. Jak terroryści mogą wykorzystywać IT?

WNIOSEK

Przyjrzeliśmy się środowisku zagrożeń, które istnieje. Jednak środowisko zagrożeń szybko się zmienia. Co roku lub co dwa lata pojawia się radykalnie nowy typ ataku, który gwałtownie rośnie. Specjaliści ds. Bezpieczeństwa muszą stale dokonywać ponownej oceny środowiska zagrożeń. Ponadto za każdym razem, gdy ofiary wprowadzają środki zaradcze, napastnicy analizują je i często znajdują sposoby, aby je obejść. Bezpieczeństwo nie dotyczy błędów programistycznych; zajmuje się inteligentnymi przeciwnikami, którzy nieustannie dostosowują się do wysiłków korporacji. Wreszcie ataki stają się coraz bardziej wyrafinowane i dotkliwe.

TEST XVII

Na jakie trzy szerokie sposoby środowisko zagrożeń może się zmienić w przyszłości?

PODSUMOWANIE

Zaczęliśmy od przyjrzenia się kilku ważnym fragmentom terminologii związanej z bezpieczeństwem. Najpierw przyjrzeliśmy się trzem celom bezpieczeństwa: poufności, integralności i dostępności. Następnie zdefiniowaliśmy termin incydenty (zwane także naruszeniami lub kompromisami). Wreszcie zdefiniowaliśmy środki zaradcze (zwane również zabezpieczeniami lub kontrolami). Kontrole ogólnie są klasyfikowane jako zapobiegawcze, wykrywające i korygujące. To wprowadzenie zakończyło się ważnym przykładem przypadku - włamań do TJX - który ilustruje złożoność rzeczywistych sytuacji bezpieczeństwa. Chociaż wiele osób wyobraża sobie ataki nadchodzące przez Internet, myśląc o bezpieczeństwie IT, wielu specjalistów ds. Bezpieczeństwa uważa, że pracownicy i byli pracownicy są największym zagrożeniem dla korporacji. Specjaliści od bezpieczeństwa IT mogą być największym zagrożeniem ze wszystkich. Pracownicy angażują się w szeroki zakres ataków, w tym spędzanie zbyt dużo czasu w Internecie, kradzieże finansowe, sabotaż i kradzież własności intelektualnej. Malware to ogólna nazwa złego oprogramowania i obejmuje wirusy, robaki, zagrożenia mieszane, kod mobilny i konie trojańskie. Prawie każda firma ma wiele zagrożeń dla złośliwego oprogramowania każdego roku. Wiele ataków złośliwego oprogramowania wykorzystuje socjotechnikę, w której ofiara zostaje oszukana w celu zrobienia czegoś wbrew politykom bezpieczeństwa, na przykład otwarcia załącznika wiadomości e-mail zawierającego złośliwe oprogramowanie, ponieważ temat i treść wiadomości e-mail sprawiają, że otwarcie załącznika wydaje się sensowne lub kuszące. Ludzie postrzegają napastników jako hakerów filmowych z Hollywood, którzy mogą niemal natychmiast włamać się do komputerów. W rzeczywistości hakerzy często potrzebują dużo czasu, aby włamać się do komputerów. Najpierw wysyłają pakiety sondujące do sieci, aby zidentyfikować potencjalne ofiary hosta i aplikacje działające na komputerach. Gdy haker zrozumie sieć, używa programu typu exploit, aby dokonać włamania (włamania). Haker może wtedy wyrządzić szkody w wolnym czasie. Hakerzy mogą wykorzystać inżynierię społeczną, aby oszukać ofiary. Mogą również przeprowadzać ataki typu

„odmowa usługi” (DoS), aby zmniejszyć dostępność systemu. Oprócz wysoko wykwalifikowanych hakerów, poważne zagrożenie dla korporacji stanowi ogromna społeczność dzieciaków od scenariuszy. Wiele osób zaskakuje fakt, że tradycyjni zewnętrzni napastnicy motywowani reputacją i dreszczykiem emocji zostali w dużej mierze zastąpieni przez karierę przestępców. Ci przestępcy zawodowi wykorzystują IT do angażowania się w tradycyjne ataki przestępcze, takie jak kradzież finansowa, kradzież własności intelektualnej (IP), wymuszenia, karty, kradzież kont bankowych, kradzież tożsamości i szpiegostwo. Karierowi przestępcy często tworzą i wykorzystują duże botnety do przeprowadzania swoich ataków. Korporacje stają w obliczu wielu innych pojawiających się problemów związanych z bezpieczeństwem, w tym kradzieży i nadużyć pracowników, szpiegostwa przez konkurentów i krajowe agencje wywiadowcze oraz koszmarnych scenariuszy cyberwojny i cyberterroru. Ponadto środowisko zagrożeń szybko się zmienia - zawsze w kierunku bardziej wyrafinowanych i poważnych ataków.

Przemyślane pytania

1. Osoba atakująca włamuje się do korporacyjnej bazy danych i usuwa krytyczne pliki. Na jakim celu bezpieczeństwa koncentruje się ten atak?

2. W jaki sposób detektywistyczne środki zaradcze mogą działać jako środki zapobiegawcze? (Odpowiedzi nie ma w tekście).

3. (a) Jeśli przypadkowo znajdziesz czyjeś hasło i użyjesz go, aby dostać się do systemu, czy jest to włamanie? Wyjaśnij. (b) Ktoś wysyła Ci „grę”. Po uruchomieniu loguje Cię na serwerze IRS. Czy to hacking? Wyjaśnij. (c) Czy możesz zostać za to oskarżony? (d) Masz dostęp do swojej strony głównej na serwerze. Przypadkowo odkrywasz, że jeśli naciśniesz określony klawisz, możesz dostać się do cudzych plików. Spędzasz tylko kilka minut na rozglądaniu się. Czy to hacking? Wyjaśnij.

4. Firma Addamark Technologies stwierdziła, że jej serwery WWW były dostępne bez upoważnienia przez pracownika konkurenta Arcsight. Wiceprezes ds. Marketingu firmy Arcsight odrzucił włamanie, mówiąc: „To po prostu ekran, który prosi o podanie nazwy użytkownika i hasła. Pracownik nie miał wrażenia, że zrobił coś nielegalnego”. Wiceprezes dodał, że pracownik nie zostanie ukarany. Skomentuj obronę Arcsight VP.

5. Podaj trzy przykłady inżynierii społecznej niewymienione w tekście.

6. Jak myślisz, dlaczego atakujący DDoS używają zombie do atakowania ofiar zamiast wysyłania pakietów ataku bezpośrednio do ofiar? Podaj dwa powody.

7. Dlaczego użycie skryptu stworzonego przez hakera nie miałoby dać doświadczenia hakowania przez ekspertów?

8. Jak myślisz, jakie są zalety i wady spłacania szantażystów?

9. Konkurent odwiedza twoją publiczną stronę internetową i odkrywa, że może dostać się do katalogu, o którym nie wiedziałeś, że może zostać osiągnięty. Znajdują tam listę klientów i wykorzystują ją na swoją korzyść. Czy włamali się na twój serwer WWW? Jaki problem możesz napotkać, pozywając ich za kradzież tajemnic handlowych?

WPROWADZENIE

Dzisiejszy świat jest niebezpiecznym miejscem dla korporacji. Internet umożliwił firmom dostęp do miliardów klientów i innych partnerów biznesowych, ale dał również przestępcom dostęp do setek milionów korporacji i osób fizycznych. Przestępcy mogą atakować witryny internetowe, bazy danych i krytyczne systemy informacyjne bez przekraczania granicy kraju będącego gospodarzem korporacji. Korporacje stały się krytycznie zależne od technologii informatycznych (IT) jako części ich ogólnej przewagi konkurencyjnej. Aby chronić swoją infrastrukturę IT przed różnymi zagrożeniami i późniejszą rentownością, korporacje muszą mieć kompleksowe zasady bezpieczeństwa IT, ugruntowane procedury, wzmocnione aplikacje i bezpieczny sprzęt.

Podstawowa terminologia dotycząca bezpieczeństwa

Środowisko zagrożenia

Jeśli firmy mają być w stanie się bronić, potrzebują zrozumienia środowiska zagrożeń - to znaczy typów napastników i ataków, z którymi borykają się firmy. „Zrozumieć środowisko zagrożenia" to fantazyjny sposób powiedzenia „Poznaj swojego wroga". Jeśli nie wiesz, jak możesz zostać zaatakowany, nie możesz planować obrony. Ta część skupi się prawie wyłącznie na środowisku zagrożeń.

Środowisko zagrożeń składa się z typów napastników i ataków, z którymi mierzą się firmy

CELE BEZPIECZEŃSTWA

Korporacje i podgrupy w korporacjach mają cele bezpieczeństwa - warunki, które chcą osiągnąć pracownicy ochrony. Trzy wspólne podstawowe cele określane są łącznie jako CIA. To nie jest Centralna Agencja Wywiadowcza. CIA oznacza raczej poufność (confidentiality), integralność (integrity) i dostępność (availability)

* Poufność - Poufność oznacza, że ludzie nie mogą czytać poufnych informacji, ani gdy znajdują się one na komputerze, ani gdy podróżują przez sieć.

* Integralność-integralność oznacza, że osoby atakujące nie mogą zmieniać ani niszczyć informacji, ani gdy znajdują się one na komputerze, ani gdy podróżują przez sieć. Lub przynajmniej, jeśli informacja zostanie zmieniona lub zniszczona, odbiorca może wykryć zmianę lub przywrócić zniszczone dane.

* Dostępność-Dostępność oznacza, że nie uniemożliwia się tego osobom upoważnionym do korzystania z informacji. Ani atak komputerowy, ani atak sieciowy nie powstrzymają ich od informacji, do których mają dostęp.

Wielu specjalistów ds. bezpieczeństwa jest niezadowolonych z uproszczonej taksonomii celów CIA, ponieważ uważają, że firmy mają wiele innych celów związanych z bezpieczeństwem. Jednak cele CIA są dobrym miejscem do rozpoczęcia myślenia o celach bezpieczeństwa.

NARUSZENIA

Gdy zagrożeniu udaje się wyrządzić szkodę firmie, nazywa się to incydentem lub naruszeniem. Firmy oczywiście starają się powstrzymać incydenty, ale zazwyczaj każdego roku muszą stawić czoła kilku naruszeniom, więc reagowanie na incydenty jest umiejętnością krytyczną. Jeśli chodzi o model procesów biznesowych, zagrożenia odsuwają proces biznesowy od realizacji co najmniej jednego z jego celów.

ŚRODKI ZARADCZE

Oczywiście specjaliści ds. bezpieczeństwa próbują powstrzymać zagrożenia. Metody, których używają do udaremniania ataków, nazywane są środkami zaradczymi, zabezpieczeniami, zabezpieczeniami lub kontrolami. Celem środków zaradczych jest utrzymywanie procesów biznesowych na właściwej drodze do osiągnięcia celów biznesowych pomimo obecności zagrożeń i rzeczywistych kompromisów. Narzędzia używane do udaremniania ataków nazywane są środkami zaradczymi, zabezpieczeniami lub kontrolami. Środki zaradcze mogą być techniczne, ludzkie lub (najczęściej) będące połączeniem tych dwóch. Zazwyczaj środki zaradcze dzielą się na trzy typy:

* Zapobiegawcze - zapobiegawcze środki zaradcze zapobiegają powodzeniu ataków. Większość kontroli to kontrole prewencyjne.

* Wykrywanie - wykrywalne środki zaradcze określają, kiedy zagrożenie atakuje, a zwłaszcza gdy odnosi sukces. Szybkie wykrywanie może zminimalizować uszkodzenia.

* Korygujące - środki zaradcze przywracają proces biznesowy na właściwe tory po zdarzeniu. Im szybciej proces biznesowy może wrócić na właściwe tory, tym większe prawdopodobieństwo, że proces biznesowy osiągnie swoje cele.

TEST

a. Dlaczego ważne jest, aby firmy rozumiały środowisko zagrożeń?

b. Nazwij trzy wspólne cele bezpieczeństwa.

c. Krótko wyjaśnij każdy.

d. Co to jest incydent?

e. Jakie są synonimy incydentów?

f. Jakie są środki zaradcze?

g. Jakie są synonimy środka zaradczego?

h. Jakie są cele środków zaradczych?

i . Jakie są trzy rodzaje środków zaradczych?

Studium przypadku: naruszenie danych w TJX

Jeśli ta terminologia wydaje się abstrakcyjna, warto przyjrzeć się konkretnemu atakowi, aby umieścić te terminy w kontekście i pokazać, jak złożone mogą być ataki bezpieczeństwa. Zaczniemy od jednej z największych strat prywatnych informacji o klientach. To jest naruszenie danych TJX.

TJX COMPANIES, INC.

TJX Companies, Inc. (TJX) to grupa ponad 2500 sklepów detalicznych działających w Stanach Zjednoczonych, Kanadzie, Anglii, Irlandii i kilku innych krajach. Firmy te prowadzą działalność pod takimi nazwami jak TJ Maxx i Marshalls. TJX określa się jako „wiodący sprzedawca ubrań i artykułów modowych po obniżonej cenie w Stanach Zjednoczonych i na świecie". Przy tego rodzaju deklaracji misji istnieje silna presja na minimalizację kosztów.

ODKRYCIE

18 grudnia 2006 r. TJX wykrył „podejrzane oprogramowanie" w swoich systemach komputerowych. Trzy dni później TJX wezwał konsultantów ds. bezpieczeństwa, aby zbadali sytuację. 21 grudnia

konsultanci potwierdzili, że włamanie rzeczywiście miało miejsce. Następnego dnia firma poinformowała organy ścigania w Stanach Zjednoczonych i Kanadzie. Pięć dni później konsultanci ds. bezpieczeństwa ustalili, że dane klientów zostały skradzione. Konsultanci wstępnie ustalili, że oprogramowanie włamaniowe działało przez siedem miesięcy, zanim zostało wykryte. Kilka tygodni później konsultanci odkryli, że firma również została kilkakrotnie naruszona w 2005 roku. Podsumowując, konsultanci oszacowali, że zostało skradzionych 45,7 miliona rekordów klientów. To zdecydowanie największa liczba osobistych danych klientów skradzionych z jakiejkolwiek firmy w tym czasie. Złodzieje nie ukradli tych rekordów dla dreszczyku emocji związanych z włamaniem lub dla wzmocnienia swojej reputacji wśród innych hakerów. Zrobili to, aby móc wykorzystać te informacje do dokonania oszukańczych zakupów kartami kredytowymi, wypłacenia tysięcy dolarów z bankomatów i sprzedania skradzionych danych kart kredytowych innym przestępcom. Skradzione fundusze były następnie prane za pośrednictwem międzynarodowych rachunków bankowych. W swojej obronie TJX zauważył, że w większości skradzionych danych większość danych osobowych użytkowników została zamaskowana (zastąpiona gwiazdkami). Zauważył również, że większość kart kredytowych, o których przechowywano informacje, straciła ważność i że firma generalnie nie gromadziła numerów ubezpieczenia społecznego (SSN). Jednak w przypadku 455 000 klientów, którym zwrócono pieniądze bez pokwitowania, zebrano znacznie większą ilość danych osobowych, a także te informacje zostały skradzione. TJX poinformował klientów o naruszeniu danych dopiero prawie miesiąc później. Firma powiedziała, że potrzebuje czasu, aby wzmocnić swoje bezpieczeństwo. Firma poinformowała również, że funkcjonariusze organów ścigania powiedzieli TJX, aby nie ujawniała natychmiast informacji o naruszeniu, aby uniknąć ujawnienia złodziejom danych śledztwa. Oczywiście opóźnienie spowodowało również, że klienci nie zdawali sobie sprawy z niebezpieczeństwa, z którym się spotkali.

WŁAMANIE

Jak doszło do naruszeń? Uważa się, że złodzieje danych włamali się do słabo chronionych sieci bezprzewodowych w niektórych sklepach detalicznych, aby dostać się do centralnego systemu przetwarzania kart kredytowych i debetowych TJX w Massachusetts. Sniffer, słuchał słabo zaszyfrowanego ruchu firmy przechodzącego do i z centrum przetwarzania. Kolejnym problemem było to, że TJX zachowywał pewne poufne informacje o kartach kredytowych, których nie powinno się przechowywać; to właśnie te niewłaściwie zachowane informacje uznali za wartościowe dla złodziei danych. W jaki sposób złodzieje pozostali niewykrytymi, mimo że sniffer działał przez ponad pół roku i pomimo eksfiltracji ponad 80 GB danych? W jaki sposób atakujący umieścili sniffera w sieci TJX, który pozostawał niewykryty przez siedem miesięcy? Wydaje się, że odpowiedź na to pytanie jest taka, że TJX nie posiadał zorganizowanej zdolności wykrywania włamań. Na swoją obronę firma stwierdziła, że „wierzy, że nasze zabezpieczenia były porównywalne z wieloma innymi głównymi sprzedawcami detalicznymi". Jej celem mogło być przygotowanie do obrony przed procesami sądowymi opartymi na zaniedbaniach. Udowodnienie zaniedbania zwykle wymaga udowodnienia, że sprawca był nieuprawniony, w oparciu o ogólną praktykę w terenie. Kanadyjska Komisja ds. Prywatności, która była pierwszym biurem rządowym, które ujawniło ustalenia dotyczące włamania, dokonała następującej oceny bezpieczeństwa TJX w momencie naruszenia:

Firma zebrała zbyt dużo danych osobowych, przechowywała je zbyt długo i polegała na słabej technologii szyfrowania, aby je chronić, co stanowi zagrożenie dla prywatności milionów swoich klientów… Firma nie poradziła sobie z ryzykiem włamania, nie zaszyfrowała danych wystarczająco mocno, nie monitorowała odpowiednio swoich systemów, nie działała zgodnie ze standardami branży kart płatniczych i zebrała zbyt dużo informacji

KARTA PŁATNICZA - STANDARD BEZPIECZEŃSTWA DANYCH

Szereg wcześniejszych (i mniejszych) naruszeń danych skłoniło główne firmy obsługujące karty kredytowe do stworzenia standardu bezpieczeństwa danych kart płatniczych (PCI-DSS). Norma ta określała 12 wymaganych celów kontrolnych, które muszą zostać wdrożone przez firmy akceptujące zakupy kartą kredytową. Brak wdrożenia celów kontrolnych PCI-DSS może skutkować karami, a nawet odebraniem zdolności firmy do przyjmowania płatności kartą kredytową. W momencie wykrycia naruszenia danych firma TJX była daleko w tyle w swoim programie zgodności z PCI-DSS. Firma spełniła tylko 3 z 12 wymaganych celów kontroli. Z notatek wewnętrznych wynika, że firma wiedziała, iż narusza wymagania PCI-DSS, w szczególności w odniesieniu do słabego szyfrowania w sieciach bezprzewodowych sklepów detalicznych. Jednak firma celowo postanowiła nie podejmować szybkich działań w celu rozwiązania tego problemu. W listopadzie 2005 roku jeden z pracowników zauważył proroczo, że „oszczędzanie pieniędzy i zgodność z PCI jest dla nas ważna, ale równie ważna jest ochrona przed intruzami. Mimo że mamy trochę przestrzeni do oddychania z PCI, nadal jesteśmy podatni na ataki z WEP jako kluczem bezpieczeństwa. To musi być ryzyko, które jesteśmy gotowi podjąć, aby zaoszczędzić pieniądze i mieć nadzieję, że nie zostaniemy narażeni ". Kiedy pracownik zauważył, że „mamy trochę przestrzeni do oddychania z PCI", prawdopodobnie odnosił się do faktu, że TJX otrzymało rozszerzenie pozwalające na zachowanie zgodności poza określoną datą zgodności ze standardem. Jak na ironię, ten dodatkowy czas przyznano po tym, jak naruszenia danych już się rozpoczęły. To rozszerzenie było uzależnione od oceny raportu TJX na temat projektu zgodności do czerwca 2006 r. Nie wiadomo, czy TJX spełnił ten wymóg. List upoważniający do przedłużenia został wysłany przez wiceprezesa ds. Kontroli oszustw Visa. Skończyło się na „Doceniam Twoje nieustające wsparcie i zaangażowanie w ochronę branży płatniczej".

UPADEK: PRAWA I DOCHODZENIA

Firma szybko uwikłała się w procesy handlowe i dochodzenia rządowe. Te procesy sądowe obejmowały złożenie informacji, które rzuciły dodatkowe światło na włamania. Na przykład zapieczętowane dowody z kart Visa i MasterCard wykazały, że liczba skradzionych rekordów kont wyniosła 94 miliony - mniej więcej dwa razy więcej niż szacunki TJX. TJX został pozwany przez kilka pojedynczych banków i zrzeszeń banków. TJX rozliczył się, płacąc 24 mln USD pożyczkodawcom wydającym karty MasterCard i 41 mln USD Visa. Zapłacili również 9,75 miliona dolarów na rozstrzygnięcie spraw z 41 stanami. W tej bitwie korporacyjnych gigantów konsumenci byli obsługiwani na końcu. TJX zaproponował ugodę, która obejmowałaby jedynie aktywne środki, takie jak pomoc w kradzieży tożsamości poprzez ubezpieczenie i inne środki dla około 455 000 ofiar, które podały dane osobowe, zwracając towary bez pokwitowania. Inne ofiary otrzymałyby skromny kupon (30 USD) lub możliwość zakupu towarów TJX po obniżonych cenach.

OSKARŻENIE

W dniu 25 sierpnia 2008 roku Departament Sprawiedliwości oskarżył 11 osób o włamanie do TJX i późniejsze wykorzystanie skradzionych informacji. Trzech było Amerykanami i szybko trafili do więzienia. Dwóch kolejnych było w Chinach. Reszta znajdowała się w Europie Wschodniej. Akt oskarżenia podkreśla międzynarodowy charakter cyberprzestępczości. Chociaż trzej Amerykanie dokonali faktycznej kradzieży danych, wydali skradzione informacje za granicą. Dwóch amerykańskich oskarżonych szybko złożyło pozew, aby zeznawać przeciwko domniemanemu przywódcy Albertowi Gonzalezowi z Miami na Florydzie. 25 marca 2010 r. Gonzalez został skazany na 20 lat więzienia. Wyrok wynikał z połączonej sprawy, która dodała OfficeMax, Dave & Buster's i Barnes & Noble do listy przedsiębiorstw, których dotyczy. 26 marca 2010 r. Gonzalez został ponownie skazany na 20 lat i jeden dzień więzienia za kradzież około 130 milionów dodatkowych numerów kart kredytowych z Heartland Payment Systems. Ponieważ wyrok ten ma być odbywany jednocześnie z jego wcześniejszym wyrokiem skazującym, wydłuża on tylko jeden dzień kary. Gonzalez użył ataku SQL na Heartland, aby ukraść

numery kart kredytowych. Firmy, których to dotyczy, to 7-Eleven, J.C. Penny i Wet Seal. To największa znana dotychczas kradzież tożsamości

TEST II

a. Kim były ofiary naruszenia TJX? (Odpowiedzi nie ma w tekście i nie jest to trywialne pytanie).

b. Czy włamanie do TJX było spowodowane pojedynczą słabością zabezpieczeń, czy wieloma słabymi punktami zabezpieczeń? Wyjaśnić.

c. Dlaczego spełnienie celów kontrolnych PCI-DSS prawdopodobnie zapobiegłoby naruszeniu danych przez TJX? To nie jest trywialne pytanie.

d. Czy spełnienie celów kontrolnych PCI-DSS zapewniłoby, że naruszenie danych nie miałoby miejsca? Pomyśl o tym dokładnie. Odpowiedzi nie ma w tekście.

e. Którego z celów CIA nie udało się TJX osiągnąć w tym ataku?

ZAGROŻENIA PRZEZ PRACOWNIKÓW I EX-PRACOWNIKÓW

Przyjrzawszy się ogólnym zagrożeniom, kluczowej terminologii związanej z bezpieczeństwem i konkretnemu kompromisowi, przyjrzymy się teraz konkretnym elementom środowiska zagrożeń korporacyjnych. Zaczniemy od spojrzenia wewnątrz firmy, na zagrożenia stwarzane przez pracowników. Kiedy firmy zaczęły kupować własne komputery w latach sześćdziesiątych XX wieku, szybko odkryły, że niezadowoleni i chciwi pracownicy oraz byli pracownicy stanowią poważne zagrożenie dla bezpieczeństwa. Ponieważ firmy stały się bardziej zależne od technologii informacyjnej, zagrożenia ze strony osób z wewnątrz stały się bardziej niebezpieczne.

Dlaczego pracownicy są niebezpieczni

Pracownicy i byli pracownicy są bardzo niebezpieczni z czterech powodów:

• Zwykle posiadają rozległą wiedzę o systemach.

• Często posiadają poświadczenia potrzebne do uzyskania dostępu do wrażliwych części systemów.

• Znają korporacyjne mechanizmy kontrolne i często wiedzą, jak uniknąć wykrycia.

• Wreszcie, firmy zwykle ufają swoim pracownikom. W rzeczywistości, gdy ochrona nalega, aby pracownik zachowywał się w określony sposób lub wyjaśniał oczywiste naruszenie zasad bezpieczeństwa, często kierownik pracownika chroni pracownika przed „ingerencją w bezpieczeństwo".

Pracownicy i byli pracownicy są bardzo niebezpieczni, ponieważ mają rozległą wiedzę na temat systemów, posiadają poświadczenia potrzebne do uzyskania dostępu do wrażliwych części systemów, często wiedzą, jak uniknąć wykrycia, i mogą skorzystać na zaufaniu, którym zwykle obdarza się „naszych ludzi". Czynniki te często eliminują potrzebę posiadania zaawansowanej wiedzy komputerowej. W rzeczywistości w 23 cyberprzestępstwach związanych z usługami finansowymi popełnionych w latach 1996-2002 87 procent zostało popełnionych bez żadnego zaawansowanego programowania. Pracownicy IT są szczególnie niebezpieczni ze względu na ich niezwykłą wiedzę i dostęp. Pracownicy bezpieczeństwa IT są najbardziej niebezpieczni ze wszystkich. W około połowie przypadków oskarżeni są specjalistami IT, a nawet pracownikami ochrony i byłymi pracownikami. Rzymianie zapytali, Quis custodiet custodes? To tłumaczy się jako „Kto obserwuje obserwatorów?" To jedna z najtrudniejszych kwestii w zarządzaniu bezpieczeństwem IT.

Sabotaż pracowników

Jedną z najstarszych obaw dotyczących pracowników jest sabotaż, czyli niszczenie sprzętu, oprogramowania lub danych. Sabotaż pochodzi od francuskiego słowa oznaczającego obuwie, ponieważ niezadowoleni pracownicy we wczesnych latach rewolucji przemysłowej rzekomo wrzucali drewniane buty do maszyn, aby zatrzymać produkcję. Sabotaż może mieć również motywy finansowe. Kiedy Roger Duronio sabotował 2000 serwerów w UBS PaineWebber, nie tylko karał swojego byłego pracodawcę. Sprzedał również krótko przed akcje UBS PaineWebber, aby skorzystać z późniejszego spadku ceny akcji firmy. Chociaż atak spowodował rozległe szkody, kurs akcji nie spadł, a Duronio stracił pieniądze. Uznany za winnego sabotażu komputerowego i oszustw związanych z papierami wartościowymi, 63-letni Duronio został skazany na osiem lat więzienia federalnego.

„Tim Lloyd, administrator systemów komputerowych, został zwolniony. W odwecie Lloyd umieścił program bomby logicznej na krytycznym serwerze. Kiedy wystąpiły z góry określone warunki, bomba logiczna zniszczyła programy sterujące maszynami produkcyjnymi firmy. Lloyd zabrał również do domu i skasował zapasowe taśmy firmy, aby zapobiec przywróceniu. Sabotaż Lloyda przyniósł natychmiastowe straty biznesowe w wysokości 10 mln USD, koszty przeprogramowania 2 mln USD i 80 zwolnień. Atak doprowadził do trwałej utraty przez firmę pozycji konkurencyjnej na rynku nowoczesnych przyrządów i pomiarów, ponieważ firma nie mogła odbudować zastrzeżonego oprogramowania do projektowania, z którego korzystała”

Hackowanie przez pracowników

Innym problemem jest to, że pracownicy włamują się do komputerów firmy przy użyciu skradzionych danych uwierzytelniających, luk w systemach wewnętrznych lub innych oszukańczych metod. Mogą wtedy sprzeniewierzyć pieniądze, ukraść własność intelektualną lub po prostu spojrzeć na żenujące informacje. Jak zobaczymy później, prawo Stanów Zjednoczonych podaje następującą definicję hakowania - celowego uzyskiwania dostępu do zasobów komputera bez autoryzacji lub z nadmiarem autoryzacji. Definicje hakowania w innych jurysdykcjach są zwykle bardzo podobne.

Hakowanie to celowe uzyskiwanie dostępu do zasobów komputera bez autoryzacji lub z nadmiarem autoryzacji.

Zauważ, że kluczową kwestią jest autoryzacja. Czy masz jawne (lub niejawne) upoważnienie do korzystania z zasobu, do którego uzyskałeś dostęp? Czy byłeś upoważniony do korzystania z części zasobu, ale nie z określonej części, do której uzyskałeś dostęp? Motywacja do włamania jest nieistotna. Kary są takie same, niezależnie od tego, czy próbowałeś ukraść milion dolarów lub po prostu „testowałeś bezpieczeństwo.

Kradzież finansowa pracowników i kradzież własności intelektualnej

Istnieje wiele powodów, dla których pracownicy mają dostęp do zasobów bez pozwolenia lub z nadmiarem pozwolenia. Czasami pracownicy robią to z czystej ciekawości lub w celu znalezienia informacji, które mogą zawstydzić firmę. Czasami jednak mają one czysto kryminalne cele, takie jak kradzież finansowa, która wiąże się z przywłaszczeniem majątku (powiedzmy poprzez przypisanie go sobie za pomocą komputera) lub kradzieżą pieniędzy (na przykład manipulowanie aplikacją, aby zapłacił premię). Innym motywem przestępczym jest kradzież własności intelektualnej firmy (IP), czyli informacji będących własnością firmy i chronionych prawem. IP obejmuje formalnie chronione informacje, takie jak prawa autorskie, patenty, nazwy handlowe i znaki towarowe. Chociaż wiele firm nie ma takich formalnych aktywów intelektualnych, własność intelektualna obejmuje również tajemnice handlowe, czyli fragmenty wrażliwych informacji, które firma zachowuje w tajemnicy.

Obejmują one plany, receptury produktów, procesy biznesowe, cenniki, listy klientów i wiele innych rodzajów informacji, które firma chce zachować w tajemnicy przed konkurentami. Jeśli inna firma uzyska tajemnicę handlową w nielegalny sposób, będzie ona podlegać postępowaniu sądowemu. Niemniej jednak niektórzy pracownicy kradną tajemnice handlowe, aby sprzedać je innej firmie. Własność intelektualna (IP) to informacje należące do firmy i chronione prawem. Tajemnice handlowe

Wymuszenia pracownicze

W niektórych przypadkach pracownik lub były pracownik wykorzysta swoją zdolność do uszkodzenia systemów lub uzyskania dostępu do poufnych informacji w celu wyłudzenia informacji od firmy. W wymuszeniu sprawca próbuje zdobyć pieniądze lub inne dobra, grożąc podjęciem działań sprzecznych z interesem ofiary. Na przykład pracownik może podłożyć bombę logiczną w komputerze firmy. Jeśli pracownik lub były pracownik każe firmie zapłacić pieniądze, aby uniknąć szkód, jest to wymuszenie. Kradzież własności intelektualnej i żądanie pieniędzy w zamian za nieprzekazywanie informacji również jest wymuszeniem. W wymuszeniu sprawca próbuje zdobyć pieniądze lub inne towary, grożąc podjęciem działań sprzecznych z interesem ofiary

Molestowanie seksualne lub rasowe pracowników

Chociaż hakowanie, kradzież i wymuszenia to krytyczne kwestie, molestowanie seksualne lub rasowe wśród pracowników jest jeszcze częstszym problemem. Na przykład molestowanie seksualne może obejmować groźby fizyczne, zemstę po romantycznym zerwaniu, pobieranie i wyświetlanie pornografii lub odwet na niechętnym partnerze seksualnym poprzez wstrzymanie promocji i podwyżek.

NADUŻYCIE INTERNETU

Termin nadużycie jest używany w odniesieniu do działań, które naruszają obowiązujące w firmie zasady korzystania z technologii informatycznych lub zasady etyczne. W niektórych przypadkach pracownicy nadużywają dostępu do Internetu, najczęściej pobierając pornografię, pobierając pirackie media lub oprogramowanie lub tracąc wiele godzin na surfowanie po Internecie w celach osobistych. Nadużycia wahają się od lekko szkodliwego zachowania po czyny przestępcze. Nadużycia obejmują działania, które naruszają obowiązujące w firmie zasady korzystania z IT lub zasady etyczne. Pobieranie pornografii może prowadzić do pozwów o molestowanie seksualne przeciwko firmie, jak również przeciwko osobie odpowiedzialnej. Pobieranie pirackiej muzyki, filmów i oprogramowania może z kolei skutkować wysokimi karami za naruszenie praw autorskich. Pobieranie niezatwierdzonych plików może również prowadzić do kosztownych infekcji złośliwym oprogramowaniem. Podczas gdy wielu pracodawców nie ma nic przeciwko niewielkiej ilości osobistego korzystania z Internetu, niektórzy pracownicy uzależniają się od korzystania z Internetu i spędzają dziesiątki godzin tygodniowo na osobistym surfowaniu po sieci w pracy. Ponadto, gdy pracownicy pobierają wiele plików z Internetu, najprawdopodobniej pobiorą wirusa lub inne złośliwe oprogramowanie. Działy bezpieczeństwa IT zwykle nie lubią szukać dowodów pornografii i nadmiernego korzystania z Internetu, ale w większości firm jest to część pracy.

NIE-INTERNETOWE NADUŻYCIE KOMPUTERA

Innym aspektem nadużyć pracowników jest nieuprawniony dostęp do prywatnych danych osobowych w systemach wewnętrznych przez zaciekawionych pracowników. Tego typu zachowanie wykryto podczas kampanii wyborczej w USA w 2008 roku oraz w kilku hospitalizacjach znanych osób. Nadużywanie wewnętrznych systemów korporacyjnych w celach podglądania nie ogranicza się do pracowników biura głównego. Na przykład ankieta przeprowadzona wśród 300 starszych administratorów IT podczas londyńskiej konferencji i targów poświęconych bezpieczeństwu wykazała,

że jedna trzecia osób przyznała się do przeglądania informacji poufnych lub osobistych w sposób niezwiązany z wykonywaną pracą.

Utrata danych

Szkodliwe zachowania pracowników, którym do tej pory przyjrzeliśmy się, obejmują celowe niewłaściwe działania. Pracownicy mogą również zagrozić bezpieczeństwu swoich firm poprzez zwykłą nieostrożność, utratę laptopów, dysków optycznych i dysków USB. Nieautoryzowane udostępnianie danych na tych komputerach i nośnikach może być katastrofalne dla firmy. Nawet jeśli dane nie są faktycznie wykorzystywane, fakt, że mogłyby zostać wykorzystane, może wymagać od firmy podjęcia kosztownych działań. Badanie przeprowadzone przez Ponemon w 2010 roku wykazało, że całkowity koszt niepowodującego katastrofalnego naruszenia bezpieczeństwa danych wyniósł 3,4 miliona dolarów. Głównymi przyczynami utraty danych były złośliwe lub przestępcze ataki, zaniedbania, usterki systemu lub błędy osób trzecich.

Inni napastnicy „wewnętrzni”

Pracownicy nie są jedynymi zagrożeniami wewnątrz firmy. Wiele firm zatrudnia pracowników kontraktowych, którzy pracują dla firmy przez krótkie okresy czasu. Pracownicy kontraktowi często uzyskują poświadczenia dostępu, które nie są usuwane po zakończeniu ich zaangażowania. W rzeczywistości firmy często zatrudniają inne firmy do wykonywania prac kontraktowych, które odbywają się wewnątrz murów pierwotnej firmy. Te firmy kontraktowe i ich pracownicy często otrzymują również tymczasowe poświadczenia. Ci pracownicy kontraktowi i firmy kontraktowe stwarzają ryzyko prawie identyczne z ryzykiem stwarzanym przez pracowników

TEST III

a. Podaj cztery powody, dla których pracownicy są szczególnie niebezpieczni.

b. Jaki typ pracownika jest najbardziej niebezpieczny?

c. Co to jest sabotaż?

d. Podaj z wpisów definicję hakowania.

e. Co to jest własność intelektualna?

f. Jakie dwa rodzaje rzeczy mogą ukraść pracownicy?

g. Rozróżnij ogólną własność intelektualną i tajemnice handlowe.

h. Co to jest wymuszenie?

i . Co to jest wykorzystywanie komputera pracowników i Internetu?

j. Kto oprócz pracowników stanowi potencjalne zagrożenie „wewnętrzne”

MALWARE

Chociaż pracownicy i inne „wewnętrzne” zagrożenia mogą być niezwykle niebezpieczni, firmy muszą również obawiać się tradycyjnych zewnętrznych napastników, którzy wykorzystują Internet do wysyłania złośliwego oprogramowania do korporacji, włamywania się do firmowych komputerów i wyrządzania innych szkód.

Twórcy złośliwego oprogramowania

Pierwszymi zewnętrznymi atakującymi szkodliwym oprogramowaniem byli twórcy złośliwego oprogramowania. Termin malware ogólnie oznacza „złe oprogramowanie". Najbardziej znanym rodzajem złośliwego oprogramowania jest wirus komputerowy. Do szkodliwego oprogramowania zalicza się również robaki, konie trojańskie, RAT (trojany zdalnego dostępu), spam i kilka innych typów, które zobaczymy w tej sekcji.

Złośliwe oprogramowanie to ogólny termin określający złe oprogramowanie.

Złośliwe oprogramowanie to bardzo poważne zagrożenie. W czerwcu 2006 r. Microsoft opublikował wyniki ankiety przeprowadzonej wśród użytkowników, którzy zezwolili na skanowanie swoich komputerów w poszukiwaniu złośliwego oprogramowania. Skan wykrył 16 milionów sztuk złośliwego oprogramowania na 5,7 milionach zbadanych maszyn.

Wirusy

Wirusy to programy, które przyłączają się do legalnych programów na komputerze ofiary. Później, gdy zainfekowane programy są przenoszone na inne komputery i uruchamiane, wirus dołącza się do innych programów na tych komputerach. Wirusy to programy, które przyłączają się do legalnych programów. Początkowo większość wirusów rozprzestrzeniała się poprzez transfer programów za pośrednictwem dyskietek. W dzisiejszych czasach wirusy rozprzestrzeniają się za pośrednictwem poczty e-mail z zainfekowanymi załącznikami, komunikatorami, programami do udostępniania plików, zainfekowanymi programami ze złośliwych witryn internetowych, a użytkownicy celowo pobierają „bezpłatne oprogramowanie" lub pornografię. Twórcy wirusów atakują popularne systemy operacyjne i aplikacje, aby zmaksymalizować ich szkody. Dzięki aplikacjom sieciowym wirusy mogą się dziś bardzo szybko rozprzestrzeniać.

Robaki

Wirusy to nie jedyny rodzaj złośliwego oprogramowania. Szczególnie ważnym rodzajem złośliwego oprogramowania jest robak. W przeciwieństwie do wirusów robaki to samodzielne programy, które nie dołączają się do innych programów. Robaki to samodzielne programy, które nie przyłączają się do innych programów. Ogólnie robaki działają podobnie jak wirusy i mogą się rozprzestrzeniać na wiele takich samych sposobów. Jednak niektóre robaki mają znacznie bardziej agresywny tryb rozprzestrzeniania się, przeskakując bezpośrednio z jednego komputera na drugi bez interwencji użytkownika na komputerze odbierającym. Takie robaki rozprzestrzeniające się bezpośrednio wykorzystują luki (luki w zabezpieczeniach) w oprogramowaniu. Gdy robak rozprzestrzeniający się bezpośrednio przeskakuje na komputer, który ma określoną lukę, dla której został zaprojektowany, robak może zainstalować się na tym komputerze i wykorzystać ten komputer jako bazę do przeskakiwania na inne komputery - wszystko to bez żadnych działań ze strony użytkownika część.

Robaki rozprzestrzeniające się bezpośrednio przeskakują bezpośrednio na komputery z lukami w zabezpieczeniach; następnie używają tych komputerów do przeskakiwania do innych komputerów. Bezpośrednia propagacja może być bardzo szybka, umożliwiając robakowi wyrządzenie ogromnych szkód, zanim zostanie wykryty i zatrzymany. Badacze z Uniwersytetu Kalifornijskiego w Berkeley oszacowali, że najgorszy przypadek robaka rozprzestrzeniającego się bezpośrednio może wyrządzić szkody w wysokości 50 miliardów dolarów w samych Stanach Zjednoczonych. Bezpośrednia propagacja nie wymaga żadnych działań ze strony użytkownika, więc robaki rozprzestrzeniające się bezpośrednio mogą rozprzestrzeniać się niezwykle szybko.

Zagrożenia mieszane

Gdyby wirusy i robaki nie były wystarczająco złe, rosnąca liczba zagrożeń mieszanych rozprzestrzenia się zarówno w postaci wirusów, jak i robaków. Mogą również publikować się w witrynach internetowych, aby ludzie mogli nieświadomie pobrać. Zagrożenia mieszane, rozprzestrzeniając się na wiele sposobów, zwiększają prawdopodobieństwo sukcesu. MessageLabs przechowuje dane dotyczące wirusów, robaków i zagrożeń mieszanych. We wrześniu 2010 MessageLabs poinformowało, że 1 na 218 wiadomości e-mail zawiera wirusy, robaki lub mieszane zagrożenia. Oszustwa phishingowe stanowiły 1 na 382 wysłanych e-maili, a 92 procent wszystkich e-maili to spam.

Ładunki

Po rozprzestrzenieniu się wirusów i robaków często wykonują one ładunki, czyli fragmenty kodu, które powodują uszkodzenia. Łagodne ładunki po prostu wyświetlają komunikat na ekranie użytkownika lub powodują inne irytujące, ale nieśmiertelne szkody. Niestety, niektóre wirusy i robaki, które mają pozornie nieszkodliwe ładunki lub nawet nie zawierają żadnych ładunków, mogą wyrządzić znaczne szkody. Na przykład, chociaż Slammer nie zawierał ładunku, rozprzestrzeniał się tak szybko, że zatykał sieci tak dużym ruchem, że skutecznie zamykał części Internetu. Z kolei złośliwe ładunki mogą wyrządzić ogromne szkody, na przykład losowo usuwając pliki z dysku twardego ofiary lub instalując inne typy złośliwego oprogramowania opisane w dalszej części tej sekcji. Ładunki wirusów i robaków również często „zmiękczają" komputer, wyłączając oprogramowanie antywirusowe i podejmując inne działania, które narażają go na późniejsze ataki wirusów i robaków.

TEST IV

a. Co to jest złośliwe oprogramowanie?

b. Rozróżnij wirusy i robaki.

c. W jaki sposób większość wirusów rozprzestrzenia się obecnie między komputerami?

d. Opisz, jak bezpośrednio rozprzestrzeniające się robaki przemieszczają się między komputerami.

e. Dlaczego bezpośrednio rozprzestrzeniające się robaki są szczególnie niebezpieczne?

f. Co to jest ładunek wirusa lub robaka?

Konie trojańskie i rootkity

NIEMOBILNE ZŁOŚLIWE OPROGRAMOWANIE

Wirusy, robaki i mieszane zagrożenia nie są jedynymi typami złośliwego oprogramowania, ale są to jedyne rodzaje złośliwego oprogramowania, które mogą się przekazywać innym ofiarom. Inne formy złośliwego oprogramowania mogą rozprzestrzeniać się na komputer tylko wtedy, gdy zostaną tam umieszczone. Przykłady sposobów na uzyskanie złośliwego oprogramowania innego niż mobilne obejmują:

• Umieszczenie go tam przez hakera

• Umieszczenie wirusa lub robaka w tym miejscu jako część ładunku

• Zachęcanie ofiary do pobrania złośliwego oprogramowania z witryny internetowej lub witryny FTP poprzez przedstawianie złośliwego oprogramowania jako użytecznego programu lub pliku danych

• Dołączanie wrogiego kodu mobilnego (opisanego później) do strony internetowej i wykonywanie go na komputerze ofiary, gdy ofiara pobiera stronę internetową.

KONIE TROJAŃSKIE

Większość szkodliwych programów niemobilnych to konie trojańskie. Wczesne konie trojańskie to programy, które udawały jedną rzecz, takie jak gra lub piracka wersja programu komercyjnego, ale w rzeczywistości były złośliwym oprogramowaniem. Wiele z tych klasycznych koni trojańskich nadal istnieje. Jednak dzisiaj, gdy mówimy o koniu trojańskim, mamy na myśli program, który ukrywa się, usuwając plik systemowy i przejmując nazwę pliku systemowego. Konie trojańskie są trudne do wykrycia, ponieważ wyglądają jak legalne pliki systemowe.

Koń trojański to program, który ukrywa się, usuwając plik systemowy i przejmując nazwę pliku systemowego. Konie trojańskie są trudne do wykrycia, ponieważ wyglądają jak legalne pliki systemowe.

TROJANY ZDALNEGO DOSTĘPU

Jednym z powszechnych typów koni trojańskich jest trojan zdalnego dostępu (RAT). RAT zapewnia atakującemu zdalną kontrolę nad komputerem. Atakujący może zdalnie robić figle, takie jak otwieranie i zamykanie napędu CD lub wpisywanie rzeczy na ekranie. Mogą jednak również angażować się w bardziej złośliwe działania. Istnieje wiele legalnych programów do zdalnego dostępu, które pozwalają zdalnemu użytkownikowi pracować na komputerze lub przeprowadzać diagnostykę. Jednak RAT zazwyczaj działają w ukryciu, aby uniknąć wykrycia przez właściciela maszyny.

DOWNLOADERS

Niektóre konie trojańskie to downloadery (czasami nazywane dropperami). Zwykle są to dość małe programy, co utrudnia wykrycie. Jednak po zainstalowaniu pobierają znacznie większego konia trojańskiego, który może wyrządzić znacznie więcej szkód.

SPYWARE

Termin „spyware" odnosi się do szerokiego spektrum programów typu „koń trojański", które zbierają informacje o użytkowniku i udostępniają je atakującemu. Istnieje kilka rodzajów oprogramowania szpiegującego.

• Pliki cookie to małe ciągi tekstowe przechowywane na komputerze przez witryny internetowe. Następnym razem, gdy wejdziesz na stronę internetową, witryna może pobrać plik cookie. Pliki cookie mają wiele zalet, takich jak zapamiętywanie hasła przy każdej wizycie. Pliki cookie mogą również zapamiętać, co wydarzyło się ostatnio w serii ekranów prowadzących do zakupów. Jednak gdy pliki cookie rejestrują zbyt wiele poufnych informacji o Tobie, stają się oprogramowaniem szpiegującym. (Pliki cookie nie są same w sobie końmi trojańskimi, ale dołączamy je do innych typów oprogramowania szpiegującego).

• Rejestratory naciśnięć klawiszy, znane również jako keyloggery, rejestrują wszystkie naciśnięcia klawiszy. Twoje naciśnięcia klawiszy mogą być następnie przeszukiwane pod kątem nazw użytkowników, haseł, numerów ubezpieczenia społecznego, numerów kart kredytowych i innych poufnych informacji. Mogą wysłać te informacje do atakującego. Niektóre keyloggery mogą rejestrować odwiedzane strony internetowe, uruchamiane programy, a nawet robić zrzuty ekranu w określonych odstępach czasu.

• Oprogramowanie szpiegujące do kradzieży haseł informuje o wylogowaniu z odwiedzanego serwera i prosi o ponowne wpisanie nazwy użytkownika i hasła. Jeśli to zrobisz, oprogramowanie szpiegujące wyśle Twoją nazwę użytkownika i hasło do atakującego.

• Oprogramowanie szpiegujące do eksploracji danych przeszukuje dyski twarde pod kątem tych samych typów informacji, które są poszukiwane przez rejestratory naciśnięć klawiszy. Wysyła również te informacje do przeciwnika.

ROOTKITS

Konie trojańskie zastępują legalne programy. Zagrożenie Adeeper to zestaw programów zwanych rootkitami. Na komputerach z systemem Unix konto root jest kontem superużytkownika, które ma pełną władzę nad komputerem. Chociaż to konto superużytkownika nazywa się Administrator na komputerze z systemem Windows, konta superużytkowników są ogólnie określane jako konta root. Rootkity przejmują konto roota i wykorzystują jego przywileje, aby się ukryć. Robią to głównie poprzez zapobieganie wykrywaniu ich obecności przez metody przeglądania plików ich systemu operacyjnego. Programy typu rootkit rzadko są wychwytywane przez zwykłe programy antywirusowe, a programy do wykrywania rootkitów często są specyficzne dla określonych rootkitów

TEST V

a. W jaki sposób można dostarczyć na komputery złośliwe oprogramowanie inne niż mobilne?

b. Co to jest koń trojański?

c. Co to jest RAT?

d. Co to jest downloader?

e. Co to jest oprogramowanie szpiegowskie?

f. Dlaczego pliki cookie mogą być niebezpieczne?

g. Rozróżnij rejestratory naciśnięć klawiszy, oprogramowanie szpiegujące wykradające hasła i oprogramowanie szpiegujące do eksploracji danych.

h. Rozróżnij konie trojańskie i rootkity.

i . Dlaczego rootkity są szczególnie niebezpieczne?

Kod mobilny

Pobrana strona internetowa może zawierać kod wykonywalny, a także tekst, obrazy, dźwięki i wideo. Nazywa się to kodem mobilnym, ponieważ jest wykonywany na każdym komputerze, na którym pobiera się stronę internetową. Javascript to popularny język do pisania kodu mobilnego. Popularne są również kontrolki Microsoft Active X. W większości przypadków kod mobilny jest niewinny i często jest niezbędny, jeśli użytkownik chce skorzystać z funkcji witryny. Jednak jeśli (i tylko wtedy) komputer ma lukę wykorzystywaną przez określony fragment kodu mobilnego, wrogi kod mobilny będzie w stanie wykorzystać tę lukę.

Inżynieria społeczna w złośliwym oprogramowaniu

Ataki socjotechniczne wykorzystują błędny ludzki osąd, przekonując ofiarę do podjęcia działań sprzecznych z polityką bezpieczeństwa. Na przykład, jeśli pracownik otrzyma wiadomość e-mail z ostrzeżeniem o zbliżającym się zwolnieniu grupowym, może otworzyć załącznik i pobrać wirusa, robaka lub konia trojańskiego. Chociaż technologia może zapewnić wiele zabezpieczeń, firmom bardzo trudno jest chronić się przed błędnymi ocenami ludzi.

Ataki socjotechniczne wykorzystują błędny ludzki osąd, przekonując ofiarę do podjęcia działań sprzecznych z polityką bezpieczeństwa.

SPAM

Zmorą wszystkich użytkowników poczty elektronicznej jest spam, który jest definiowany jako niechciana komercyjna poczta e-mail. Chociaż ISP, korporacyjne i osobiste filtry spamu znacznie zredukowały ilość spamu, ludzie wciąż są bombardowani spamem. Oprócz tego, że są irytujące, wiadomości spamowe często są fałszywe lub reklamują niebezpieczne produkty. Dodatkowo, Spam stał się powszechnym narzędziem dystrybucji wirusów, robaków, koni trojańskich i wielu innych rodzajów złośliwego oprogramowania. Jak wspomniano wcześniej, MessageLabs poinformowało, że we wrześniu 2010 r. 92% wszystkich wiadomości e-mail stanowiło spam. Niektórzy dostawcy usług hostingowych zauważyli podiesienie stawki na 96 procent lub więcej. Nawet obciążenie sieci spowodowane zwykłym przesyłaniem i przechowywaniem spamu może być znaczące. Jest to szczególnie ważne, ponieważ wielu spamerów wysyła obecnie spam zawierający obrazy zamiast treści tekstowych, aby uniknąć wykrycia przez programy do skanowania spamu. Spam ze spamem graficznym jest znacznie większy niż tradycyjne wiadomości tekstowe ze spamem.

PHISHING

W przypadku ataków phishingowych ofiary otrzymują wiadomości e-mail, które wyglądają na pochodzące z banku lub innej firmy, z którą ofiara prowadzi interesy. Wiadomość może nawet skierować ofiarę na autentycznie wyglądającą stronę internetową. Oficjalny wygląd wiadomości i strony internetowej często oszukuje ofiarę do podania poufnych informacji. Niewielki, ale znaczący odsetek wszystkich osób, które otrzymują wiadomości phishingowe, odpowiada na nie, ponieważ wiadomości te wydają się tak autentyczne. Badanie AGartner z 2007 roku wykazało, że konsumenci w USA zostali okradzeni z 3,2 miliarda dolarów w wyniku phishingu w tym roku. Phishing powoduje również wiele kosztownych telefonów do pomocy technicznej w firmach.

SPEAR PHISHING

Normalne ataki phishingowe są zwykle atrakcyjne dla wielu osób, aby mogły oszukać jak najwięcej ofiar. W przeciwieństwie do tego ataki typu spear phishing są wymierzone w pojedyncze osoby lub małe grupy osób. Na przykład, jeśli celem atakującego jest nakłonienie dyrektora generalnego korporacji do pobrania konia trojańskiego, atakujący może stworzyć wiadomość e-mail, która dotyczy pilnej kwestii dla dyrektora generalnego, wydaje się pochodzić od zaufanej osoby i zawiera konkretne szczegóły, które prawdopodobnie zna tylko zaufana osoba.

OSZUSTWA

Niektóre wiadomości e-mail zawierają fałszywe informacje. W niektórych przypadkach te oszustwa po prostu powodują, że ofiara czuje się głupio, gdy mówi innym ludziom, czego się „nauczyła". W innych przypadkach oszustwa próbują przekonać ofiarę do uszkodzenia własnego systemu, usuwając krytyczne pliki systemowe.

TEST VI

a. Co to jest kod mobilny?

b. Co to jest inżynieria społeczna?

c. Co to jest spam?

d. Co to jest phishing?

e. Rozróżnij zwykły phishing i spear phishing.

f. Dlaczego oszustwa są złe?

HAKERZY I ATAKI

W latach siedemdziesiątych do twórców złośliwego oprogramowania dołączyli hakerzy z zewnątrz, którzy zaczęli włamywać się do firmowych komputerów podłączonych do modemów. Obecnie prawie każda firma jest podłączona do Internetu, w którym znajdują się miliony zewnętrznych hakerów. Hakerzy są w stanie włamać się do sieci firmowych, wykraść poufne dane lub wyrządzić szkody w krytycznej infrastrukturze z odległości tysięcy mil.

Tradycyjne motywy

Większość tradycyjnych zewnętrznych hakerów nie powodowała rozległych szkód ani nie dokonywała kradzieży dla pieniędzy. Motywowali ich przede wszystkim dreszczyk emocji związany z włamaniami, potwierdzenie ich umiejętności i poczucie siły. Ponadto zewnętrzni hakerzy często komunikowali się ze sobą. Wykazując zdolność włamywania się do dobrze bronionych hostów, hakerzy mogli zwiększyć swoją reputację wśród swoich rówieśników ,osoba atakująca nadal istnieje. Często tradycyjni hakerzy skupiali się na zawstydzeniu ofiary. Na przykład w 2009 roku wandale włamali się do skomputeryzowanego znaku drogowego w Austin w Teksasie i zmienili jego komunikat na: „Koniec jest blisko! Uwaga! Zombie przed nami! ”50 Jednak wielu tradycyjnych zewnętrznych hakerów angażuje się w bezpośrednie kradzieże, wymuszenia i inne szkody, aby wesprzeć swoje„ hobby.

TEST VII

a. Jakie były motywacje tradycyjnych zewnętrznych hakerów?

b. Czy tradycyjni hakerzy zewnętrzni zaangażowali się w kradzież?

Anatomia włamania

Chociaż istnieje wiele różnych sposobów włamania się do komputera, istnieje ogólny proces, który często stosują osoby atakujące, próbując włamać się do firmowych komputerów. Jest to podobne do tego, co zrobiłby złodziej, gdyby chciał fizycznie ukraść firmowe komputery.

WYBÓR CELU

Haker może losowo przeszukać wszystkie możliwe firmy w celu znalezienia potencjalnego celu lub wyszukać konkretną firmę po nazwie. Nazwę domeny firmy można rozpoznać za pomocą prostego wyszukiwania WHOIS (www.whois.net). Korporacje zazwyczaj mają bloki ciągłych adresów IP, które przydzielają komputerom wewnętrznym. Gdy haker zna zakres docelowych adresów IP, może rozpocząć badanie sieci w poszukiwaniu podatnych hostów.

SONDY REKONESANSOWE

Zanim złodziej włamie się do domu, często „szuka” okolicznych domów w poszukiwaniu zagrożonych domów. Atakujący zbiera następnie informacje o potencjalnych domach ofiar, aby zdecydować, do których z nich się włamać. Hakerzy mają również tendencję do przeprowadzania rozpoznania przed włamaniem do komputera. Atakujący często wysyła pakiety sondujące do sieci. Te pakiety sondujące są przeznaczone do wywoływania odpowiedzi z wewnętrznych hostów i routerów. Jeśli hosty wewnętrzne lub routery odpowiedzą na te pakiety sondujące, ich odpowiedzi mogą wiele powiedzieć atakującemu o sieci.

Skanowanie adresów IP: Pierwsza runda pakietów sondujących ma na celu znalezienie aktywnych hostów. Atakujący wysyła sondy skanujące adresy IP na wszystkie adresy IP w docelowym zakresie.

Sondy te często używają komunikatów odpowiedzi echa i echa protokołu ICMP (Internet Control Message Protocol) omówione w module A. Gdy host otrzyma komunikat ICMP Echo, powinien odesłać komunikat odpowiedzi ICMP Echo. Gdy atakujący otrzyma wiadomość odpowiedzi ICMP Echo z adresu IP, wie, że pod tym adresem IP znajduje się aktywny host.

Skanowanie portów: gdy osoba atakująca zna adresy IP aktywnych hostów, musi wiedzieć, jakie programy działają na zidentyfikowanych hostach, ponieważ większość ataków opiera się na lukach w określonych programach. Na hostach serwerów aplikacje odpowiadają numerom portów. Używając metafory „domu", port byłby odpowiednikiem drzwi w domu. Na przykład 80 to dobrze znany numer portu dla serwerów WWW HTTP. Jeśli port 80 jest otwarty, komputer jest prawdopodobnie serwerem WWW. Istnieje wiele dobrze znanych numerów portów od 0 do 1023. Każdy z nich wskazuje na obecność określonego typu aplikacji. Atakujący wysyła sondy skanujące porty do każdego zidentyfikowanego hosta w celu określenia, które aplikacje są na nim uruchomione. Zazwyczaj program skanujący porty żąda połączenia z programem na porcie o określonym numerze.54 Jeśli cel odeśle zgodę na kontynuację, atakujący wie, że host docelowy uruchamia program na porcie o tym numerze.

EXPLOITY

Po zidentyfikowaniu potencjalnych hostów i portów ofiary można rozpocząć atak. W tym przypadku atakujący wysyła pakiety exploitów do hostów ofiary zamiast pakietów sondujących. Specyficzna metoda ataku używana przez atakującego do włamania się do komputera nazywana jest exploitem atakującego, a czynność polegająca na implementacji exploita nazywana jest wykorzystaniem hosta. Jeśli exploit powiedzie się, osoba atakująca „posiada" przynajmniej konto i może „posiadać" sam komputer. Posiadanie komputera pozwala napastnikowi robić wszystko, czego sobie życzy.

SPOOFING

Każdy pakiet zawiera źródłowy adres IP, który jest jak adres zwrotny na kopercie. Źródłowy adres IP jest niebezpieczny dla hakerów, ponieważ umożliwia korporacjom zlokalizowanie atakujących. Atakujący mogą udaremnić próby ich znalezienia, podszywając się pod źródłowy adres IP, czyli umieszczając inny adres IP w polu źródłowego adresu IP. W ten sposób ofiara nie może poznać prawdziwego adresu IP atakującego. Nie wszystkie pakiety można sfałszować. Na przykład osoba atakująca zwykle musi być w stanie odczytać odpowiedzi na pakiety sondujące. Odpowiedzi ofiar są zawsze wysyłane do hosta, którego adres IP znajduje się w polu źródłowego adresu IP sondy. Jeśli atakujący sfałszuje adres IP w pakietach sondujących, nie otrzyma odpowiedzi. Wiele exploitów musi również otrzymać odpowiedź, aby odnieść sukces. Atakujący, którzy muszą otrzymać odpowiedzi, często korzystają z łańcucha atakujących komputerów, które zostały wcześniej przejęte przez atakującego. Polecenia są przekazywane przez łańcuch do końcowego komputera, który wysyła sondę lub pakiety ataku. Odpowiedzi są również przekazywane przez łańcuch z powrotem do atakującego. Ofiara zwykle będzie w stanie prześledzić atak do ostatniego komputera w łańcuchu i być może do jednego lub dwóch więcej hostów w łańcuchu. Rzadko kiedy ofiara może prześledzić całą drogę ataku do hosta atakującego, ponieważ łańcuch komputerów przechodzi przez wiele firm, stanów i krajów.

TEST VIII

a. Rozróżnij skanowanie adresów IP i skanowanie portów.

b. Co to jest exploit?

c. Co oznacza „posiadanie" komputera?

d. Co to jest fałszowanie adresu IP?

e. Dlaczego odbywa się fałszowanie adresu IP?

f. Kiedy osoba atakująca nie może używać fałszowania adresu IP?

g. Kiedy atakujący muszą używać prawidłowych adresów źródłowych IP w protokołach sondujących lub exploitów, w jaki sposób mogą ukrywać swoją tożsamość?

Inżynieria społeczna w ataku

Wiele zewnętrznych (i wewnętrznych) ataków wykorzystuje socjotechnikę, która, jak widzieliśmy wcześniej, ma na celu nakłonienie użytkowników do zrobienia czegoś, co jest sprzeczne z interesem bezpieczeństwa. W porównaniu z zabezpieczeniami technicznymi łatwowierność człowieka jest często znacznie łatwiejsza do wykorzystania. Na przykład haker dzwoni do sekretarki, która twierdzi, że współpracuje z jej szefem. Następnie haker prosi o poufne informacje, takie jak hasło, a nawet plik z ograniczeniami. Inne przykłady inżynierii społecznej obejmują podążanie za kimś przez bezpieczne drzwi bez wprowadzania kodu dostępu (nazywa się to piggybacking) i patrzenie przez ramię, gdy wpisuje hasło (nazywa się to surfowaniem przez ramię). W ramach pretekstu, atakujący dzwoni podając się za określonego klienta, aby uzyskać prywatne informacje o tym kliencie.

TEST IX

a. W jaki sposób można wykorzystać inżynierię społeczną, aby uzyskać dostęp do poufnego pliku?

b. Co to jest piggybacking?

d. Co to jest surfing przez ramiona?

e. Co to jest pretekst?

Ataki typu „odmowa usługi”

Innym rodzajem ataku zewnętrznego jest atak typu „odmowa usługi” (DoS). Atak DoS ma na celu uniemożliwienie dostępu do serwera lub sieci uprawnionym użytkownikom. W odniesieniu do omówionej wcześniej taksonomii celów bezpieczeństwa CIA, ataki DoS są atakami na dostępność.

Atak typu „odmowa usługi” (DoS) ma na celu uniemożliwienie dostępu do serwera lub sieci uprawnionym użytkownikom poprzez zalewanie ich pakietami ataków.

Najczęstszy rodzaj ataku DoS, to atak rozproszona odmowa usługi (DDoS). W tym exploicie atakujący najpierw umieszcza programy zwane botami na wielu hostach internetowych (klientach, serwerach lub obu). Później, gdy nadejdzie czas na rozpoczęcie ataku DoS, botmaster (lub handler) wysyła wiadomość do wszystkich botów. Następnie boty zaczynają zalewać serwer lub sieć wymienioną w komunikacie o ataku pakietami ataku. Wkrótce przeciążone serwery i sieci nie będą mogły służyć swoim legalnym użytkownikom. Na przykład, aby zaatakować serwer, boty mogą zalać serwer żądaniami otwarcia połączenia TCP (segmenty TCP SYN). Serwer rezerwuje określoną ilość mocy za każdym razem, gdy otrzymuje segment SYN. Zalewając komputer segmentami SYN, osoba atakująca może spowodować wyczerpanie zasobów serwera, a tym samym awarię lub niemożność odpowiedzi na dalsze próby otwarcia połączenia od uprawnionych użytkowników. Jeśli strumień ataku jest szczególnie intensywny, cała sieć korporacji ofiary nie będzie mogła komunikować się przez Internet. Istnieją inne sposoby wykonania ataku DoS. W rozdziale 4 przyjrzymy się dodatkowym metodom ataków DoS i sposobom łagodzenia ich skutków. Przyjrzy się również innym typom ataków sieciowych, takim jak ARP Poisoning, oraz sposobom zabezpieczenia sieci przed atakami z zewnątrz.

TEST X

a. Co to jest atak DoS?

b. Opisz atak DDoS.

d. Opisz szczegółowo atak SYN flooding.

e. Dlaczego wiele botnetów ma z czasem wielu właścicieli?

Poziomy umiejętności

Filmy z Hollywood często przedstawiają hakerów jako geniuszy, którzy potrafią włamać się na ściśle chronione serwery w ciągu kilku sekund. W rzeczywistości wysoko wykwalifikowani hakerzy zwykle potrzebują dni lub nawet miesięcy ciężkiej pracy, aby włamać się do dobrze chronionego systemu - jeśli w ogóle im się uda. W tym czasie będą próbowali wielu różnych ataków. Innymi słowy, wykwalifikowani hakerzy charakteryzują się zarówno dużą wiedzą techniczną, jak i zawziętą wytrwałością. Aby zautomatyzować niektóre aspekty swoich ataków, hakerzy często piszą programy zwane skryptami hakerskimi. Termin skrypt tradycyjnie oznacza dość prymitywny program napisany prostym językiem. Dzisiejsze skrypty hakerów mają jednak często łatwe w użyciu graficzne interfejsy użytkownika i wyglądają jak oprogramowanie komercyjne. Ponadto zautomatyzowane skrypty i oprogramowanie hakerów są łatwo dostępne w Internecie. Te łatwe w użyciu skrypty hakerskie stworzyły nowy typ hakera – script kiddies. Jest to obraźliwe określenie, które wykwalifikowani hakerzy nadają stosunkowo niewykwalifikowanym hakerom, którzy używają tych gotowych skryptów. Chociaż indywidualnie script kiddies mają znacznie mniejsze szanse na włamanie się do komputera niż wykwalifikowani hakerzy, jest o wiele więcej script kiddies niż wykwalifikowanych hakerów. To sprawia, że script kiddies jako społeczność są niezwykle niebezpieczni. Ponadto duża liczba ataków typu script kiddies utrudnia korporacjom zidentyfikowanie niewielkiej liczby bardzo niebezpiecznych ataków, na które napotykają firmy ze strony bardzo wykwalifikowanych napastników i które wymagają szczególnej uwagi. W lipcu 2002 r. Firma Riptech (obecnie należąca do Symantec Corp.) szczegółowo przeanalizowała dane 400 swoich klientów. Zauważył, że tylko około 1 procent ataków stanowiły wyrafinowane ataki agresywne. Jednak gdy pojawiły się wyrafinowane agresywne ataki, były one 26 razy bardziej narażone na poważne szkody niż nawet umiarkowanie wyrafinowane agresywne ataki. Twórcy wirusów i innych złośliwych programów również napisali programy do tworzenia nowego złośliwego oprogramowania. Tworzenie wirusów za pomocą tych narzędzi stało się tak łatwe, że Sven Jaschan, 18-letni niemiecki student, który nigdy wcześniej nie napisał wirusa, był odpowiedzialny za 70% aktywności wirusa w pierwszej połowie 2004 roku (http: // www.sophos.com). Obecnie dostępne są narzędzia do tworzenia wszelkiego rodzaju exploitów. Jeden z najważniejszych to Metasploit Framework, który ułatwia przyjęcie nowej metody eksploatacji i szybko przekształca ją w pełny program ataku. Metasploit jest używany zarówno przez osoby atakujące do przeprowadzania ataków, jak i przez specjalistów ds. bezpieczeństwa do testowania podatności ich systemów na określone exploity.

TEST XI

a. Jakie są dwie główne cechy wykwalifikowanych hakerów?

b. Dlaczego dzieciaki skryptów są niebezpieczne? (Podaj dwa powody.)

c. Dlaczego złośliwe oprogramowanie i zestawy narzędzi do exploitów zwiększają zagrożenie związane ze skryptami dzieciaków?

ERA KRYMINALNA

Dominacja przez karierę przestępców.

Przed około 2003 rokiem większość zewnętrznych napastników stanowili pracownicy, byli pracownicy lub tradycyjni napastnicy zewnętrzni zainteresowani jedynie sławą i poczuciem władzy. Obecnie jednak większość zewnętrznych napastników to przestępcy zawodowi, którzy atakują, aby nielegalnie zarabiać pieniądze. Mają tradycyjne motywy kryminalne, a wiele z ich strategii ataku to komputerowe adaptacje tradycyjnych przestępstw.

Obecnie większość zewnętrznych napastników to przestępcy zawodowi.

Wbrew powszechnemu przekonaniu przestępcy nie zwlekają z korzystaniem z nowych technologii. W 1888 roku inspektor John Bonfield z policji w Chicago powiedział: „Jest dobrze znanym faktem, że żadna inna część populacji nie korzysta łatwiej i szybciej z najnowszych triumfów nauki niż klasa przestępcza". W latach trzydziestych John Dillinger i wielu innych przestępców wykorzystywało niedrogie samochody do rabowania banków i znikania, zanim policja zdążyła ich zatrzymać. Tablice rejestracyjne zostały wprowadzone przede wszystkim po to, by pomóc policji i zmniejszyć zalety mobilnych przestępców. Ponadto przestępcy nie rozróżniają między różnymi rodzajami przestępstw. Na przykład w 2003 r. Firma VeriSign zbadała adresy IP, z których nadeszły ataki. Okazało się, że istnieje silna korelacja między adresami IP używanymi podczas hakowania a adresami wykorzystywanymi w oszustwach. Aby podać inny przykład, policja, która przeszukiwała miejsca wykorzystywane do kradzieży tożsamości, znalazła fajki metanowe i inne materiały wskazujące na to, że przestępcy byli uzależnieni od metamfetaminy, wykorzystując kradzież tożsamości online w celu wsparcia swoich nałogów. Kradli informacje i sprzedawali je innym grupom przestępczym.

Cyberprzestępczość

Cyberprzestępczość - wykonywanie przestępstw w Internecie - stała się niezwykle dużym problemem w bardzo krótkim czasie. Według Departamentu Skarbu USA w 2005 r. Liczba postępowań dotyczących cyberprzestępczości przewyższyła liczbę postępowań dotyczących nielegalnej sprzedaży narkotyków63. W 2004 r. Przestępstwa internetowe stanowiły zaledwie 1,3% wszystkich zarejestrowanych przestępstw w Niemczech, ale stanowiły 57 procent szkód materialnych spowodowanych przez przestępstwa. W 2009 roku do FBI wpłynęło 336655 skarg dotyczących przestępstw związanych z Internetem, w których odnotowano straty w wysokości 559,7 miliona dolarów.65 Cyberprzestępczość nie staje się ważnym problemem dla bezpieczeństwa w Internecie. Stał się już dominującym problemem.

MIĘDZYNARODOWE GANGI

Ze względu na wzajemne powiązania Internetu granice państwowe i paszporty nie mają znaczenia. W rezultacie przedsiębiorstwa przestępcze mogą swobodnie popełniać różnorodne cyberprzestępstwa, nie martwiąc się, że zagraniczne kraje będą je ścigać za przestępstwa popełnione przeciwko ofiarom na ich terytorium. Kiedy dochodzi do ścigania, zazwyczaj dzieje się tak tylko dzięki kreatywności prokuratorów. Jednym z problemów międzynarodowych gangów jest to, że wielu sprzedawców internetowych nie wysyła przesyłek poza Stany Zjednoczone. Aby obejść ten problem, gangi przestępcze angażują przeładunkowych w Stanach Zjednoczonych. Osoby te odbierają wysłane towary w biurach USA, a następnie wysyłają je do gangu przestępczego w innym kraju. Za każdą przeładowaną paczkę przeładunkowi płaci się opłatę. Często przeładunki są pozyskiwane przez Internet i nigdy nie zdają sobie sprawy, że robią cokolwiek, aby pomóc przestępcy. Podobnie, międzynarodowe gangi używają mułów pieniężnych do przesyłania pieniędzy (w zamian za niewielką opłatę procentową płaconą mułowi pieniężnemu). Często przeładunki i muły pieniężne są rekrutowani za pośrednictwem internetowych witryn z ofertami pracy.

CZARNE RYNKI I SPECJALIZACJA RYNKOWA

Tradycyjni przestępcy zawsze współpracowali. Na przykład paserzy kupują skradzione towary od złodziei po obniżonej cenie, a następnie odsprzedają je jako pozornie legalne punkty sprzedaży, w których pochodzenie towarów nie będzie oczywiste. Na całym świecie istnieje wiele stron internetowych zawierających skradzione informacje konsumenckie. Istnieją nawet aktualne stawki za numery kart kredytowych, których cena jest określana na podstawie tego, jak dobrze numery kart zostały zweryfikowane, na przykład dokonując niewielkiego zakupu z każdym numerem karty, aby upewnić się, że numer jest aktywny. Większość czarnych rynków zajmuje się informacjami dotyczącymi kart kredytowych i tożsamości. Istnieją jednak również czarne rynki dla złośliwego oprogramowania, botnetów i nowo odkrytych luk w zabezpieczeniach. Kiedy analityk odkrywa lukę w zabezpieczeniach w oprogramowaniu, zwykle powiadamia firmę programistyczną, która przyznaje analitykowi kredyt po wydaniu poprawki. Jednak firmy produkujące oprogramowanie rzadko płacą odkrywcom luk. W rezultacie rosnąca liczba analityków sprzedaje informacje o odkryciach luk na jednym z kilku czarnych rynków. Inni programiści piszą oprogramowanie exploit i sprzedają je na czarnych rynkach. Obecnie w większości przypadków oprogramowanie służące do wykorzystywania luk jest sprzedawane z zapewnieniem pomocy technicznej online i bezpłatnych aktualizacji. Po zakupie płatności mogą być nawet przechowywane na rachunku escrow, dopóki kupujący nie przetestuje oprogramowania eksploatacyjnego. Pod wieloma względami cyberprzestępczość dojrzewa, podobnie jak wiele tradycyjnych rynków. Na początku na nowym rynku zwykle dominują firmy typu all-in-one. Później pojawiła się specjalizacja pionowa i pozioma. W cyberprzestępczości niektórzy przestępcy szukają exploitów, inni opracowują zestawy narzędzi, inni specjalizują się w dystrybucji i zarządzaniu botnetami, jeszcze inni prowadzą rynki kradzieży tożsamości i numerów kart kredytowych, a jeszcze inni tworzą wspólne kody i biblioteki. Z biegiem czasu szybko pojawiają się nowe nisze rynkowe.

TEST XII

a. Jaki jest obecnie dominujący typ napastnika?

b. Czy cyberprzestępczość jest dziś nieistotna w porównaniu z przestępstwami niezwiązanymi z komputerami?

c. Dlaczego międzynarodowe gangi są trudne do ścigania?

d. Dlaczego międzynarodowe gangi używają przeładunków?

e. Jak używają przeładunków?

f. Jak używają mułów pieniężnych?

Oszustwo, kradzież i wymuszenie

Oszustwa, kradzieże i wymuszenia to tradycyjne ataki przestępcze. Dzisiaj przestępcy nauczyli się wykonywać te przestępstwa za pośrednictwem sieci.

OSZUSTWO

Przestępcy próbują nielegalnie zdobyć pieniądze na wiele sposobów. Wymienimy tylko kilka. Jedną z cech charakterystycznych wielu z tych ataków przestępczych jest to, że obejmują oszustwa. W przypadku oszustwa napastnik oszukuje ofiarę, aby zrobiła coś wbrew interesom finansowym ofiary. Na przykład w podanym później przykładzie T-Data napastnik oszukał firmę, aby przekazała mu sprzęt, udając, że jest prawdziwą firmą, która zapłaci.

W przypadku oszustwa napastnik oszukuje ofiarę, aby zrobiła coś wbrew interesom finansowym ofiary.

Nie ma nic nowego w oszustwach. W świecie fizycznym oszustwa są popełniane od początku istnienia ludzkości. Cyberprzestępcy po prostu uczą się, jak przeprowadzać klasyczne oszustwa w sieciach komputerowych. Na przykład większość wiadomości spamowych wykorzystuje klasyczne metody oszustwa i ma klasyczne cele. W innych przypadkach przestępcy tworzą nowe oszustwa specyficzne dla sieci. Na przykład wiele witryn otrzymuje płatności od reklamodawców za kliknięcie. Za każdym razem, gdy odwiedzający witrynę kliknie łącze reklamowe w witrynie, reklamodawca płaci za oryginalną witrynę niewielką opłatę. W przypadku oszustw związanych z kliknięciami właściciel przestępczej witryny tworzy program do wielokrotnego klikania odsyłacza. Każde z tych fałszywych kliknięć zabiera reklamodawcy pieniądze bez generowania potencjalnych klientów.

KRADZIEŻ FINANSOWA I INTELEKTUALNA

Tak jak przestępcy zawodowi od dawna włamywali się do domów i rabowali banki, tak przestępcy zawodowi w Internecie dopuszczają się kradzieży finansowych. W innych przypadkach przestępcy zawodowi kradną własność intelektualną firmy w celu sprzedaży innym przestępcom lub konkurentom korporacyjnym. Jak wspomniano wcześniej w tym rozdziale, własność intelektualna składa się z formalnie chronionych informacji, takich jak patenty i inne informacje oraz tajemnice handlowe, które są wrażliwymi informacjami, które firma podejmuje, aby chronić, takie jak plany korporacyjne, a nawet cenniki. Według sondażu Price Waterhouse Coopers, nawet w 1999 roku firmy z listy Fortune 1000 straciły ponad 45 miliardów dolarów w wyniku kradzieży tajemnic handlowych. Działo się to na długo zanim kradzież własności intelektualnej przez Internet stała się poważnym zagrożeniem.

WYMUSZANIE Z KORPORACJI

Wymuszenie polega na użyciu groźby krzywdy, aby skłonić ofiarę do zapłacenia pieniędzy, aby uniknąć krzywdy. Wymuszenie od dawna jest podstawą ataków przestępczych w prawdziwym świecie. Jednym ze sposobów wykorzystania IT do wymuszenia na firmie jest grożenie jej atakiem, chyba że zostanie zapłacona opłata za ochronę. Czasami, gdy przestępca kradnie informacje, wymusza na firmie grożenie ujawnieniem informacji, chyba że zapłacone zostaną „ciche pieniądze". W wielu przypadkach negatywny rozgłos generowany, gdy haker ujawnia skradzione informacje, może być bardziej szkodliwy niż koszt finansowy samej informacji. Firmy mogą tracić klientów, ponieważ są postrzegane jako niechętne lub niezdolne do ochrony informacji o klientach.

TEST XIII

a. Co to jest oszustwo?

b. Co to jest fałszywe kliknięcie?

c. W jaki sposób przestępcy dokonują wymuszeń online?

Kradzież poufnych danych o klientach i pracownikach

Przestępcy mają tendencję do poszukiwania „miękkich celów", które dają duże zyski przy niewielkim wysiłku. Często oznacza to kierowanie reklam do pojedynczych osób, a nie do korporacji. Przyjrzymy się kilku atakom na osoby w kolejności rosnącej dotkliwości.

CARDING

Prawdopodobnie najczęstszym przestępczym atakiem na osoby fizyczne jest kradzież numeru karty kredytowej - praktyka znana jako carding. Carderzy „trafiają w dziesiątkę", jeśli poznają numer karty kredytowej, imię i nazwisko właściciela karty oraz trzycyfrowy numer weryfikacyjny karty. Gdy złodziej uzyska informacje, których potrzebuje, może dokonywać zakupów do momentu unieważnienia karty.

Na szczęście, jeśli ofiary kart kredytowych szybko zgłoszą oszustwo związane z numerem karty kredytowej, zgodnie z prawem Stanów Zjednoczonych są zobowiązane do zapłacenia tylko 50 USD, a większość sprzedawców kart kredytowych zrzeka się nawet tej odpowiedzialności.

KRADZIEŻ RACHUNKU BANKOWEGO

Jeśli jednak złodziej ukradnie dane uwierzytelniające wymagane do przeprowadzenia transakcji online w imieniu ofiary, może on opróżnić konto bankowe ofiary. Kradzież konta bankowego jest poważniejsza niż kradzież numeru karty kredytowej.

KRADZIEŻ KONTA ONLINE

W 2006 roku przestępcy zaczęli kradnąć internetowe konta giełdowe ze względu na luki w zabezpieczeniach w witrynach giełdowych. Zamiast ukraść kilkaset dolarów za pomocą skradzionych kart kredytowych, kradzieże kont giełdowych często sięgały tysięcy dolarów.

KRADZIEŻ TOŻSAMOŚCI

Jeśli złodziej może ukraść jeszcze więcej informacji, może zaangażować się w kradzież tożsamości, podczas której złodziej podszywa się pod ofiarę na tyle dobrze, aby zaangażować się w duże transakcje finansowe. Transakcje te mogą obejmować zaciąganie dużych pożyczek i dokonywanie dużych zakupów w imieniu ofiary. Ofiary kradzieży tożsamości mogą ponieść ogromne szkody, a niektóre z nich zostały nawet aresztowane za działania złodziei tożsamości. Kradzież tożsamości jest znacznie poważniejsza niż kradzież numeru karty kredytowej. Przestępcy od dawna kradną informacje o tożsamości konsumentów bez korzystania z komputerów. Na przykład, karty kredytowe tradycyjnie zapisywali numery kart kredytowych podczas zakupów w sklepach detalicznych. Jednak dzięki sieciom komputerowym złodzieje byli w stanie wykraść informacje o tożsamości konsumentów setek, tysięcy, a nawet milionów ofiar. Najczęściej hakerzy włamują się do słabo chronionych komputerów firmowych, aby wykraść te informacje. Jednak zgubione lub skradzione laptopy i taśmy z kopiami zapasowymi są również kopalnią złota dla złodziei informacji konsumenckich. Ponadto często w grę wchodzą nieuczciwi insiderów. W 2006 roku firma Gartner przeprowadziła ankietę wśród 5000 klientów banków w USA. Na podstawie danych z ankiety firma Gartner oszacowała, że 3 miliony Amerykanów padło ofiarą oszustw internetowych w ciągu ostatnich sześciu lat i że każdy z nich stracił średnio 900 dolarów. Inne badanie wykazało średnią stratę prawie 4000 USD, wykazało, że ofiary spędzały średnio 81 godzin na próbach rozwiązania swoich spraw i wykazało, że jedna czwarta nigdy nie została w pełni odzyskana. Niektóre straty mogą być znacznie gorsze, na przykład, jeśli złodziej tożsamości prawo własności do domu ofiary dla siebie, a następnie sprzedaje dom.

POŁĄCZENIE KORPORACYJNE

Karta, kradzież konta bankowego i kradzież tożsamości to nie tylko problemy konsumentów. To także problemy korporacyjne. Kiedy firmy zgłaszają, że włamano się do ich baz danych klientów i że tysiące lub miliony osób otrzymały informacje o ich tożsamości, reakcje klientów i inwestorów mogą być znaczne. Ponadto firmom mogą grozić sankcje rządowe. Na przykład w Stanach Zjednoczonych Federalna Komisja Handlu ma szerokie uprawnienia do nakładania kar na firmy, które nie wdrażają odpowiednio ochrony danych klientów. Komisja może również zlecić drogie niezależne audyty postępowania firmy z prywatnymi informacjami przez dziesięć lub więcej lat po wystąpieniu problemu. Wreszcie, poważne naruszenia często obejmują zwolnienie menedżerów funkcjonalnych odpowiedzialnych za naruszone systemy.

KRADZIEŻ TOŻSAMOŚCI FIRMY

Chociaż kradzież tożsamości zdarza się najczęściej osobom fizycznym, może się również zdarzyć w korporacjach. Zbierając informacje o firmie w Internecie, złodzieje tożsamości korporacyjnej mogą ubiegać się o firmowe karty kredytowe, otrzymywać je i używać w imieniu firmy będącej ofiarą. Mogą również przyjmować zamówienia kartą kredytową w imieniu firmy ofiary. Mogą nawet złożyć dokumenty, aby zmienić adres prawny firmy będącej ofiarą przestępstwa i zmienić imię i nazwisko osoby zarządzającej firmą.

TEST XIV

a. Co to jest carding?

b. Opisz kradzież konta bankowego i kradzieży konta online.

c. Rozróżnij kradzież karty kredytowej i kradzież tożsamości.

e. Dlaczego kradzież tożsamości jest poważniejsza niż kradzież numeru karty kredytowej?

f. W jaki sposób przestępcy zwykle uzyskują informacje potrzebne do kradzieży karty kredytowej i kradzieży tożsamości?

g. W jaki sposób firmy mogą zostać skrzywdzone, jeśli pozwolą na kradzież danych osobowych, nad którymi mają kontrolę?

h. Co to jest kradzież tożsamości korporacyjnej?

ZAGROŻENIA KONKURENCJI

Konkurenci korporacyjni również mogą być atakującymi. Mogą angażować się w wiele rodzajów ataków. Skoncentrujemy się na atakach na poufność i dostępność.

Szpiegostwo handlowe

W przypadku gromadzenia informacji publicznych konkurent przejrzy witrynę internetową firmy i inne informacje publiczne, aby znaleźć dane, które sama firma poszkodowana ujawnia. Konkurent może również sprawdzać strony na Facebooku pod kątem pracowników i innych informacji publicznych. Odnotowano kilka spraw sądowych w celu zbadania legalności takich działań, ale z definicji tajemnice handlowe są chronione prawem tylko wtedy, gdy firma podejmuje rozsądne wysiłki, aby zachować je w tajemnicy. Należy pamiętać, że herkulesowe wysiłki nie są konieczne, a jedynie rozsądne, które odzwierciedlają wrażliwość aktywów i praktyk bezpieczeństwa w branży.

Tajemnice handlowe są chronione prawem tylko wtedy, gdy firma podejmuje rozsądne starania, aby zachować je w tajemnicy.

Częstym celem ataków korporacyjnych jest nielegalna kradzież tajemnic handlowych firmy - praktyka zwana szpiegostwem tajemnicy handlowej. W najbardziej rażącej formie konkurent przechwyci komunikację firmy ofiary, zhakuje jej serwery lub przekupi pracownika firmy ofiary w celu kradzieży informacji. Lub może zatrudnić jednego z Twoich byłych pracowników i zażądać lub zaakceptować Twoje tajemnice handlowe od tej osoby. Szpiegostwo komercyjne nie ogranicza się do konkurentów korporacyjnych. Podobno od zakończenia zimnej wojny wiele krajowych agencji wywiadowczych przeszło do szpiegostwa handlowego. Robert Gates, dyrektor CIA w latach 1991–1993, poinformował, że rządowe szpiegostwo gospodarcze jest szeroko rozpowszechnione83. Wskazał on szczególnie Francję, Rosję, Chiny, Koreę Południową, Niemcy, Izrael, Indie i Pakistan jako zaangażowane w intensywne szpiegostwo korporacyjne. W 2007 roku w rocznym raporcie amerykańsko-chińskiej

komisji ds. Przeglądu gospodarczego i bezpieczeństwa dla Kongresu stwierdzono, że „chińska działalność szpiegowska w USA jest tak rozległa, że stanowi największe zagrożenie dla bezpieczeństwa amerykańskich technologii".

Ataki typu „odmowa usługi"

Konkurenci mogą również angażować się w różnego rodzaju ataki na Twoją firmę, takie jak ataki DoS. Chociaż te ataki na dostępność są rzadkie, mogą być katastrofalne dla firm, które polegają na dochodach z działalności online.

TEST XV

a. Należy rozróżnić między zbieraniem informacji publicznej a szpiegostwem tajemnicy handlowej

b. Co firma musi zrobić ze swoimi tajemnicami handlowymi, jeśli chce mieć możliwość ścigania osób lub firm, które ją kradną?

c. Jak silne muszą być te zabezpieczenia?

d. Kto może prowadzić szpiegostwo przeciwko firmie?

CYBERWOJNA I CYBERTERROR

Przestępcy stanowią poważne zagrożenie dla korporacji. Jednak ataki cyberterrorystów mogą wyrządzić szkody na znacznie większą skalę niż te spowodowane atakami przestępczymi. Są to ataki zorganizowanych grup terrorystycznych, a nawet rządów krajowych. Ataki te mogą mieć bezprecedensową skalę, na którą przygotowanych jest niewiele korporacyjnych planów bezpieczeństwa.

Cyberwojna

Dzisiaj, kiedy kraje idą na wojnę, używają broni i bomb. Jednak mogą również wyrządzić ogromne szkody za pomocą komputerów.

Cyberwojna to ataki komputerowe dokonywane przez rządy krajowe.

Przed rozpoczęciem działań wojennych walczący mogą zaangażować się w szpiegostwo komputerowe, aby poznać sekrety swoich przeciwników. Chiny są szczególnie aktywne w szpiegostwie cyberwojennym. Szpiegostwo cybernetyczne z Chin stanowi poważny problem od 1999 r. Rząd chiński był zaangażowany w ataki wymierzone w Departament Stanu, Departament Handlu, senatorów, kongresmenów i laboratoria wojskowe Stanów Zjednoczonych lub był ich sponsorem. Ataki cyberwojenne mogą być przeprowadzane bez angażowania się w działania fizyczne i nadal powodują ogromne szkody. Kraje mogą użyć ataków cyberwojny, aby wyrządzić ogromne szkody jednemu w infrastrukturze finansowej innej osoby, aby zakłócać wzajemne infrastruktury komunikacyjne i uszkadzać infrastrukturę informatyczną kraju, a wszystko to w charakterze prekursorów rzeczywistych fizycznych działań wojennych.

Cyberterror

Kolejnym koszmarnym scenariuszem jest cyberterror, w którym napastnikiem jest terrorysta lub grupa terrorystów. Oczywiście cyberterroryści mogą bezpośrednio atakować zasoby technologii informacyjnej. Mogą uszkodzić infrastrukturę finansową, komunikacyjną i użyteczności publicznej kraju. Najczęściej cyberterroryści wykorzystują Internet jako narzędzie rekrutacji za pośrednictwem stron internetowych i koordynowania swoich działań. Mogą również wykorzystywać cyberterror w połączeniu z fizycznymi atakami, na przykład zakłócając systemy komunikacyjne służb ratowniczych lub

zakłócając energię elektryczną w celu spowodowania korków i zwiększenia terroru. Bardziej subtelnie, ale równie niebezpiecznie, wiele organizacji terrorystycznych zwraca się do przestępstw komputerowych, aby finansować swoją działalność terrorystyczną, tak jak zwracają się do niewolniczej prostytucji i innych przestępstw fizycznych.

TEST XVI

a. Rozróżnij cyberwojnę i cyberterror.

b. W jaki sposób kraje mogą wykorzystywać ataki cyberwojny?

c. Jak terroryści mogą wykorzystywać IT?

WNIOSEK

Przyjrzeliśmy się środowisku zagrożeń, które istnieje. Jednak środowisko zagrożeń szybko się zmienia. Co roku lub co dwa lata pojawia się radykalnie nowy typ ataku, który gwałtownie rośnie. Specjaliści ds. Bezpieczeństwa muszą stale dokonywać ponownej oceny środowiska zagrożeń. Ponadto za każdym razem, gdy ofiary wprowadzają środki zaradcze, napastnicy analizują je i często znajdują sposoby, aby je obejść. Bezpieczeństwo nie dotyczy błędów programistycznych; zajmuje się inteligentnymi przeciwnikami, którzy nieustannie dostosowują się do wysiłków korporacji. Wreszcie ataki stają się coraz bardziej wyrafinowane i dotkliwe.

TEST XVII

Na jakie trzy szerokie sposoby środowisko zagrożeń może się zmienić w przyszłości?

PODSUMOWANIE

Zaczęliśmy od przyjrzenia się kilku ważnym fragmentom terminologii związanej z bezpieczeństwem. Najpierw przyjrzeliśmy się trzem celom bezpieczeństwa: poufności, integralności i dostępności. Następnie zdefiniowaliśmy termin incydenty (zwane także naruszeniami lub kompromisami). Wreszcie zdefiniowaliśmy środki zaradcze (zwane również zabezpieczeniami lub kontrolami). Kontrole ogólnie są klasyfikowane jako zapobiegawcze, wykrywające i korygujące. To wprowadzenie zakończyło się ważnym przykładem przypadku - włamań do TJX - który ilustruje złożoność rzeczywistych sytuacji bezpieczeństwa. Chociaż wiele osób wyobraża sobie ataki nadchodzące przez Internet, myśląc o bezpieczeństwie IT, wielu specjalistów ds. Bezpieczeństwa uważa, że pracownicy i byli pracownicy są największym zagrożeniem dla korporacji. Specjaliści od bezpieczeństwa IT mogą być największym zagrożeniem ze wszystkich. Pracownicy angażują się w szeroki zakres ataków, w tym spędzanie zbyt dużo czasu w Internecie, kradzieże finansowe, sabotaż i kradzież własności intelektualnej. Malware to ogólna nazwa złego oprogramowania i obejmuje wirusy, robaki, zagrożenia mieszane, kod mobilny i konie trojańskie. Prawie każda firma ma wiele zagrożeń dla złośliwego oprogramowania każdego roku. Wiele ataków złośliwego oprogramowania wykorzystuje socjotechnikę, w której ofiara zostaje oszukana w celu zrobienia czegoś wbrew politykom bezpieczeństwa, na przykład otwarcia załącznika wiadomości e-mail zawierającego złośliwe oprogramowanie, ponieważ temat i treść wiadomości e-mail sprawiają, że otwarcie załącznika wydaje się sensowne lub kuszące. Ludzie postrzegają napastników jako hakerów filmowych z Hollywood, którzy mogą niemal natychmiast włamać się do komputerów. W rzeczywistości hakerzy często potrzebują dużo czasu, aby włamać się do komputerów. Najpierw wysyłają pakiety sondujące do sieci, aby zidentyfikować potencjalne ofiary hosta i aplikacje działające na komputerach. Gdy haker zrozumie sieć, używa programu typu exploit, aby dokonać włamania (włamania). Haker może wtedy wyrządzić szkody w wolnym czasie. Hakerzy mogą wykorzystać inżynierię społeczną, aby oszukać ofiary. Mogą również przeprowadzać ataki typu

„odmowa usługi” (DoS), aby zmniejszyć dostępność systemu. Oprócz wysoko wykwalifikowanych hakerów, poważne zagrożenie dla korporacji stanowi ogromna społeczność dzieciaków od scenariuszy. Wiele osób zaskakuje fakt, że tradycyjni zewnętrzni napastnicy motywowani reputacją i dreszczykiem emocji zostali w dużej mierze zastąpieni przez karierę przestępców. Ci przestępcy zawodowi wykorzystują IT do angażowania się w tradycyjne ataki przestępcze, takie jak kradzież finansowa, kradzież własności intelektualnej (IP), wymuszenia, karty, kradzież kont bankowych, kradzież tożsamości i szpiegostwo. Karierowi przestępcy często tworzą i wykorzystują duże botnety do przeprowadzania swoich ataków. Korporacje stają w obliczu wielu innych pojawiających się problemów związanych z bezpieczeństwem, w tym kradzieży i nadużyć pracowników, szpiegostwa przez konkurentów i krajowe agencje wywiadowcze oraz koszmarnych scenariuszy cyberwojny i cyberterroru. Ponadto środowisko zagrożeń szybko się zmienia - zawsze w kierunku bardziej wyrafinowanych i poważnych ataków.

Przemyślane pytania

1. Osoba atakująca włamuje się do korporacyjnej bazy danych i usuwa krytyczne pliki. Na jakim celu bezpieczeństwa koncentruje się ten atak?

2. W jaki sposób detektywistyczne środki zaradcze mogą działać jako środki zapobiegawcze? (Odpowiedzi nie ma w tekście).

3. (a) Jeśli przypadkowo znajdziesz czyjeś hasło i użyjesz go, aby dostać się do systemu, czy jest to włamanie? Wyjaśnij. (b) Ktoś wysyła Ci „grę”. Po uruchomieniu loguje Cię na serwerze IRS. Czy to hacking? Wyjaśnij. (c) Czy możesz zostać za to oskarżony? (d) Masz dostęp do swojej strony głównej na serwerze. Przypadkowo odkrywasz, że jeśli naciśniesz określony klawisz, możesz dostać się do cudzych plików. Spędzasz tylko kilka minut na rozglądaniu się. Czy to hacking? Wyjaśnij.

4. Firma Addamark Technologies stwierdziła, że jej serwery WWW były dostępne bez upoważnienia przez pracownika konkurenta Arcsight. Wiceprezes ds. Marketingu firmy Arcsight odrzucił włamanie, mówiąc: „To po prostu ekran, który prosi o podanie nazwy użytkownika i hasła. Pracownik nie miał wrażenia, że zrobił coś nielegalnego”. Wiceprezes dodał, że pracownik nie zostanie ukarany. Skomentuj obronę Arcsight VP.

5. Podaj trzy przykłady inżynierii społecznej niewymienione w tekście.

6. Jak myślisz, dlaczego atakujący DDoS używają zombie do atakowania ofiar zamiast wysyłania pakietów ataku bezpośrednio do ofiar? Podaj dwa powody.

7. Dlaczego użycie skryptu stworzonego przez hakera nie miałoby dać doświadczenia hakowania przez ekspertów?

8. Jak myślisz, jakie są zalety i wady spłacania szantażystów?

9. Konkurent odwiedza twoją publiczną stronę internetową i odkrywa, że może dostać się do katalogu, o którym nie wiedziałeś, że może zostać osiągnięty. Znajdują tam listę klientów i wykorzystują ją na swoją korzyść. Czy włamali się na twój serwer WWW? Jaki problem możesz napotkać, pozywając ich za kradzież tajemnic handlowych?

Planowanie i Zasady

Bezpieczeństwo to proces, a nie produkt. - BRUCE SCHNEIER

Obrona

Wcześniejsze wpisy był migawką zagrożeń, przed którymi stoją dzisiejsze korporacje. Zakończyliśmy mrocznym spojrzeniem na przyszłość - liczba zagrożeń wzrośnie i stanie się bardziej niebezpieczna. W pozostałej części opiszemy, jak korporacje mogą reagować na zagrożenia dla ich zasobów. To nie jest tekst o tym, jak atakować korporacje. Chodzi o obronę. Obrona to główne zadanie specjalisty ds. bezpieczeństwa IT. Obrona firmy i jej aktywów może być złożonym procesem. Po opanowaniu zasad i praktyk obronnych pomoże Ci szczegółowe zrozumienie ataków. To jest tekst dla osób, które nie mają doświadczenia w bezpieczeństwie IT. Skupienie się na atakach, choć ekscytujące, wypchnęłoby zawartość, której uczniowie potrzebują, aby przygotować ich do ich prawdziwej pracy, czyli obrony. Należy również pamiętać, że głównym celem firmy jest wzrost wartości dla akcjonariuszy (tj. generowanie zysku). Bezpieczeństwo IT powinno być mocne i chroniące, a jednocześnie przejrzyste i dyskretne. Dobrą metaforą bezpieczeństwa IT jest szkło kuloodporne. Szkło kuloodporne chroni człowieka i pozwala mu jednocześnie wykonywać codzienną pracę. W ten sam sposób bezpieczeństwo IT powinno chronić firmę, nie utrudniając jej podstawowego celu - generowania zysku.

TEST XVIII

a. Dlaczego skupiamy się na obronie, a nie na ataku?

b. Czy bezpieczeństwo IT może być zbyt bezpieczne? W jaki sposób?

ZARZĄDZANIE TO TRUDNA CZĘŚĆ

Jednym z powodów, dla których ludzie koncentrują się na technologii, jest to, że łatwiej jest myśleć o technologii niż o zarządzaniu. Technologia jest widoczna i jest wiele rzeczy, które możemy powiedzieć o technologiach bezpieczeństwa. Ponadto większość tych koncepcji technologicznych jest dobrze zdefiniowana i dlatego łatwo je omówić. Zarządzanie jest natomiast abstrakcyjne. Nie możesz wyświetlać zdjęć urządzeń ani rozmawiać na temat terminów szczegółowych diagramów lub algorytmów oprogramowania. Do omówienia jest mniej ogólnych zasad, a większości z nich nie można zastosować w praktyce bez dobrze zdefiniowanych i złożonych procesów. Zarządzanie bezpieczeństwem jest jednak znacznie ważniejsze niż technologia bezpieczeństwa. Jeden z urzędników z amerykańskiej federalnej administracji usług publicznych mówił o pomocy szeregu federalnych agencji w reorganizacji ich technologii bezpieczeństwa. W każdym przypadku agencje od razu cieszyły się dobrą ochroną. Jednak ich bezpieczeństwo szybko się pogorszyło. Agencje te dysponowały odpowiednią technologią, ale brakowało im zdolności zarządzania, aby zapewnić długoterminowe działanie zabezpieczeń.

KOMPLEKSOWE BEZPIECZEŃSTWO

Nic dziwnego, że te agencje zawiodły. Po pierwsze, napastnicy muszą znaleźć tylko jeden sposób, aby dostać się do korporacji. Z drugiej strony organizacje potrzebują kompleksowych zabezpieczeń, zamykających wszystkie drogi ataku do swoich systemów na osoby atakujące. Kompleksowe bezpieczeństwo nie jest dziełem przypadku.

AWARIE NAJSŁABSZEGO OGNIWA

Innym powodem, dla którego zarządzanie bezpieczeństwem jest trudne, jest to, że niektóre zabezpieczenia składają się z wielu komponentów, które muszą działać razem, aby środek zaradczy był

skuteczny. Administrator firewalla opracowuje reguły filtrowania. Następnie zapora sieciowa sprawdza wszystkie pakiety przez nią przechodzące. Porzuca możliwe do sprawdzenia pakiety ataku i przechowuje informacje o porzuconych pakietach w pliku dziennika. Administrator zapory powinien codziennie sprawdzać plik dziennika. Jeśli wystąpi jakakolwiek awaria w tym procesie, zapora sieciowa staje się bezużyteczna. Jeśli pominięta zostanie ważna reguła filtrowania, przejdą przez nią możliwe do udowodnienia pakiety ataku. Jeśli administrator nie odczytuje codziennie plików dziennika, problem może pozostać niewykryty przez tygodnie lub miesiące. W łańcuchach działań w ramach jednego środka zaradczego wszystko musi być zrobione dobrze. Jeśli choć jeden krok nie zostanie dobrze zaimplementowany, bezpieczeństwo może wydawać się dobre, ale nie będzie prawdziwej ochrony. Jeśli awaria pojedynczego elementu systemu zrujnuje bezpieczeństwo, nazywa się to awarią najsłabszego łącza. W wielu przypadkach działania człowieka są najsłabszym ogniwem zabezpieczeń.

Jeśli awaria pojedynczego elementu systemu zrujnuje bezpieczeństwo, jest to awaria najsłabszego łącza.

POTRZEBA OCHRONY WIELU ZASOBÓW

Trzecim powodem, dla którego zarządzanie bezpieczeństwem jest trudne, jest to, że firmy muszą chronić dużą liczbę zasobów. Niektóre z nich to stosunkowo dobrze zdefiniowane zasoby, takie jak bazy danych i serwery. Inne to szerokie procesy organizacyjne, takie jak sprawozdawczość finansowa i opracowywanie nowych produktów. Wszystkie szybko się zmieniają. Jak omówiono w dalszej części, firmy muszą zidentyfikować wszystkie swoje zasoby i opracować program bezpieczeństwa dla każdego z nich. To jest herkulesowy wysiłek.

TEST XIX

a. Z jakich powodów zarządzanie bezpieczeństwem jest trudne?

b. Co to jest kompleksowe zabezpieczenie i dlaczego jest potrzebne?

c. Jakie są awarie najsłabszego łącza?

POTRZEBA OCHRONY WIELU ZASOBÓW

Trzecim powodem, dla którego zarządzanie bezpieczeństwem jest trudne, jest to, że firmy muszą chronić dużą liczbę zasobów. Niektóre z nich to stosunkowo dobrze zdefiniowane zasoby, takie jak bazy danych i serwery. Inne to szerokie procesy organizacyjne, takie jak sprawozdawczość finansowa i opracowywanie nowych produktów. Wszystkie szybko się zmieniają. Jak omówiono w dalszej części, firmy muszą zidentyfikować wszystkie swoje zasoby i opracować program bezpieczeństwa dla każdego z nich. To jest herkulesowy wysiłek.

TEST XX

a. Z jakich powodów zarządzanie bezpieczeństwem jest trudne?

b. Co to jest kompleksowe zabezpieczenie i dlaczego jest potrzebne?

c. Jakie są awarie najsłabszego łącza?

Potrzeba zdyscyplinowanego procesu zarządzania bezpieczeństwem

Bezpieczeństwo jest zbyt skomplikowane, aby można nim było zarządzać nieformalnie. Firmy muszą opracować i przestrzegać formalnych procesów (zaplanowanych serii działań) w zarządzaniu bezpieczeństwem. Niektóre z tych procesów mogą obejmować proces rocznego planowania

bezpieczeństwa, procesy planowania i opracowywania indywidualnych środków zaradczych oraz proces obsługi incydentów.

Procesy to zaplanowane serie działań.

Stratedzy biznesowi od dawna twierdzą, że poprawa jakości to niekończący się proces, a nie jednorazowy wysiłek. Jeden z trenerów piłkarskich zauważył, że rekrutacja jest jak golenie; zaniedbasz jeden dzień i wyglądasz jak włóczęga. Zarządzanie bezpieczeństwem to również niekończący się proces. Jednym z zewnętrznych czynników motywujących firmy do sformalizowania ich procesów bezpieczeństwa jest rosnąca liczba przepisów i regulacji dotyczących zgodności. Wiele systemów zgodności wymaga od firm przyjęcia określonych formalnych ram zarządzania w celu kierowania planowaniem bezpieczeństwa i zarządzaniem operacyjnym. W dalszej części tego rozdziału przyjrzymy się kilku z tych ram zarządzania.

TEST XXI

a. Dlaczego procesy są niezbędne w zarządzaniu bezpieczeństwem?

b. Co skłania firmy do korzystania z formalnych ram zarządzania w celu kierowania procesami bezpieczeństwa?

Cykl Plan - Chroń – Reaguj

Jeśli procesami bezpieczeństwa trzeba zarządzać kompleksowo, potrzebujemy formalnego procesu zarządzania bezpieczeństwem na najwyższym poziomie. Większość firm chroni obecnie przed zagrożeniami, stosując proces zarządzania bezpieczeństwem na najwyższym poziomie, zwany cyklem plan – ochrona – reakcja

PLANOWANIE

Cykl zaczyna się od planowania. Bez doskonałego planu nigdy nie będziesz mieć kompleksowej ochrony. Oczywiście po wdrożeniu planów wyniki zostaną uwzględnione w planowaniu. Nowe zagrożenia i warunki biznesowe zmuszą również firmy do powrotu do planowania. Wszystkie trzy czynności odbywają się jednocześnie i nieustannie wzajemnie się uzupełniają.

OCHRONA

Ochrona to oparte na planie tworzenie i działanie środków zaradczych. Większość dnia specjalisty ds. Bezpieczeństwa będzie poświęcona na fazę ochrony, nic więc dziwnego, że większość czasu poświęcimy na tworzeniu i obsłudze elementów sterujących.

Ochrona to oparte na planie tworzenie i działanie środków zaradczych

Dla każdego rodzaju ochrony musimy zarządzać cyklem życia systemu (SDLC), który przebiega od wstępnego planowania do wdrożenia. Specjaliści od systemów informacyjnych często koncentrują się na SDLC. Jednak większość życia środka zaradczego składa się z etapu operacyjnego po opracowaniu. Nauczanie studentów bezpieczeństwa skupienia się na SDLC byłoby jak szkolenie lekarzy w zakresie opieki prenatalnej i nie uczenie ich niczego na temat opieki zdrowotnej po urodzeniu. Skupimy się na zarządzaniu kontrolami przez cały cykl życia systemu, a to oznacza skupienie się na bieżącym zarządzaniu po jego stworzeniu.

ODPOWIEDŹ

Nawet przy doskonałym planowaniu i drobiazgowej ochronie, niektóre ataki zakończą się sukcesem. Reakcja jest złożona, ponieważ incydenty mają różną wagę (od prostych fałszywych alarmów po

kompletne katastrofy) oraz ponieważ różne poziomy ciężkości ataku wymagają różnych podejść. Reakcja to powrót do zdrowia zgodnie z planem - definicja, która podkreśla, że jeśli reakcja nie zostanie starannie zaplanowana z wyprzedzeniem, zajmie to zbyt dużo czasu i będzie tylko częściowo skuteczna. Szybkość i dokładność reakcji mają kluczowe znaczenie, a sposobem na osiągnięcie obu tych celów jest częste próby planu reagowania na incydenty, zanim pojawią się kompromisy.

Odpowiedź to powrót do zdrowia zgodnie z planem.

TEST XXII

a. Wymień trzy etapy cyklu plan – ochrona – odpowiedź.

b. Czy między etapami występuje sekwencyjny przepływ?

c. Który etap zajmuje najwięcej czasu?

d. Jak definiujemy ochronę?

e. Jak definiujemy odpowiedź?

Wizja w planowaniu

Wizja bezpieczeństwa IT dotycząca jego roli w odniesieniu do Twojej firmy, jej pracowników i świata zewnętrznego kieruje wszystkim innym.

POGLĄD NA BEZPIECZEŃSTWO JAKO AKTYWATOR

Ze względów bezpieczeństwa istnieją dwa podstawowe elementy widzenia. Pierwszą jest potrzeba postrzegania bezpieczeństwa jako bodźca, a nie jako źródła frustracji. Jeśli firma ma słabe zabezpieczenia, wiele innowacji jest dla niej zamkniętych, ponieważ byłyby zbyt niebezpieczne. Jeśli jednak firma ma silne zabezpieczenia, pozwoli to na wiele rzeczy. Na przykład firma z silnym zabezpieczeniem może angażować się w systemy międzyorganizacyjne z innymi firmami. Może to otworzyć nowe rynki, zapewnić lepszy przepływ informacji i doprowadzić do obniżenia kosztów operacyjnych. Nasza wizja bezpieczeństwa musi koncentrować się na bezpieczeństwie jako czynniku umożliwiającym, a nie zapobieganiu. Aby podać inny przykład, Simple Network Management Protocol (SNMP) daje organizacjom możliwość zarządzania setkami lub tysiącami zdalnych urządzeń sieciowych z jednej konsoli zarządzania. Prawie wszystkie firmy używają polecenia SNMP Get, które prosi zarządzane urządzenie o przesłanie pewnych danych o stanie i działaniu urządzenia. Jest to bardzo przydatne w diagnozowaniu problemów. Z kolei polecenie SNMP Set umożliwia menedżerowi zdalną rekonfigurację urządzeń, na przykład nakazując przełącznikowi wyłączenie określonego portu lub ustawienie portu w tryb testowy. Ten rodzaj zdalnej rekonfiguracji może zaoszczędzić znaczną część kosztów pracy związanej z zarządzaniem siecią, unikając konieczności podróżowania personelu sieciowego do urządzenia zdalnego w celu rozwiązania problemów. Skraca również czas potrzebny do przywrócenia systemów do działania. Jednak wiele firm o słabych zabezpieczeniach wyłącza polecenie Set z powodu zagrożenia spowodowanego przez atakujących, którzy mogą podszywać się pod menedżera SNMP i wysyłać złośliwe polecenia Set, aby wywołać chaos w sieci. Natomiast firmy, które dobrze zarządzają zabezpieczeniami, mogą śmiało korzystać z Set i czerpać korzyści. Jednym z kluczy do uczynienia bezpieczeństwa bodźcem jest włączenie go we wszystkie projekty na wczesnym etapie. Na wczesnym etapie projektu bezpieczeństwo zwykle można dodać stosunkowo niedrogo i bez uczynienia ostatecznego systemu nieelastycznym. Jeśli zabezpieczenia zostaną wprowadzone zbyt późno, modernizacje zabezpieczeń będą prawdopodobnie kosztowne i prawdopodobnie zmniejszą użyteczność systemu. Ponadto, oczywiście, jeśli projektu nie można zrealizować z powodu niedopuszczalnych zagrożeń bezpieczeństwa, lepiej jest to sprawdzić wcześniej niż później.

TWORZENIE POZYTYWNYCH WIZJI UŻYTKOWNIKÓW

Innym kluczowym aspektem wizji jest pozytywne postrzeganie użytkowników. Pewien cyniczny specjalista ds. Bezpieczeństwa powiedział: „są dwa rodzaje użytkowników - ci, którzy robią złe rzeczy, ponieważ są złośliwi, i ci, którzy robią złe rzeczy, ponieważ są głupi". Chociaż można by sympatyzować z tym punktem widzenia, postrzeganie użytkowników jako niszczącego wroga. Zamiast tego powinniśmy postrzegać użytkowników jako zasoby. Na przykład ochrona musi rekrutować i szkolić użytkowników, aby byli na pierwszej linii obrony firmy. Użytkownicy często jako pierwsi widzą problemy z bezpieczeństwem. Jeśli czują, że są częścią zespołu ochrony, mogą wcześniej ostrzec pracowników ochrony. Ponadto użytkownicy muszą zostać przeszkoleni w zakresie samoobrony, aby mogli chronić swoje zasoby przed zagrożeniami. Jeśli „głupi" oznacza „słabo wyszkolony", to jest to wina działu bezpieczeństwa. Podczas podróży samolotem prawdopodobnie zwolniony zostanie steward lub stewardesa, którzy nazywają pasażerów „bydłem". Działy bezpieczeństwa powinny robić to samo wobec specjalistów ds. Bezpieczeństwa, którzy odnoszą się do pracowników w obraźliwy sposób. Nie należy mówić użytkownikom na ich komputerach występują błędy ID10.T (idiota) lub PEBKAC (problem istnieje między klawiaturą a krzesłem). Poniżanie użytkowników może prowadzić do wrogości, wyobcowania i zmniejszonej produktywności. Jednym z problemów w rozwijaniu pozytywnej wizji użytkowników jest częste korzystanie z policji lub zdjęć wojskowych, gdy mowa o użytkownikach. Ma to swoje zalety, ponieważ pomaga specjalistom ds. Bezpieczeństwa zapytać, jak policja lub wojsko poradziłyby sobie w określonych sytuacjach, które wiążą się z umyślnym niewłaściwym zachowaniem. Jednak policja ma tendencję do patrzenia na podejrzanych z żółtawym okiem, a żołnierzy uczy się nienawidzić wroga. W końcu nie są to skuteczne sposoby postrzegania roli bezpieczeństwa IT. Istnieją inne sposoby przeglądania relacji ochrony z pracownikami. Na przykład jeden obraz to bezpieczeństwo matki. Dobre matki wyznaczają granice, spędzają dużo czasu na wyjaśnianiu tych ograniczeń, a co ważniejsze, pomagają swoim dzieciom w dojrzewaniu, aby były bezpieczne w sytuacjach niebezpiecznych. Można również postrzegać pracowników ochrony jako nauczycieli, osobistych trenerów i osoby rozwiązujące problemy. Kiedy szef ochrony odnoszący duże sukcesy został zapytany o trzy najważniejsze kwestie związane z bezpieczeństwem, odpowiedział: „Konsultacje, konsultacje i konsultacje".

TEST XXIII

a. W jaki sposób dobre bezpieczeństwo może być bodźcem?

b. Jaki jest klucz do bycia bodźcem?

c. Dlaczego negatywny pogląd na użytkowników jest zły?

d. Dlaczego postrzeganie funkcji bezpieczeństwa jako siły policyjnej lub organizacji wojskowej to zły pomysł?

Strategiczne planowanie bezpieczeństwa IT

Strategiczne planowanie bezpieczeństwa IT patrzy z szerszej perspektywy. Najpierw ocenia obecne bezpieczeństwo firmy. Następnie bierze pod uwagę czynniki, które będą napędzać zmiany - w tym coraz bardziej złożone i zjadliwe środowisko zagrożeń, rozwój przepisów i regulacji dotyczących zgodności, zmiany w strukturze korporacyjnej, fuzje i wszystko, co zmieni warunki w przyszłości. Następnie musi opracować spis wszystkich swoich zasobów, aby były chronione przez zabezpieczenia IT. Mogą to być korporacyjne bazy danych, serwery internetowe, a nawet arkusze kalkulacyjne. Nie możesz czegoś chronić, jeśli nie wiesz, że to masz. Po wyliczeniu wszystkich zasobów, musisz je klasyfikować według wrażliwości. Po wykonaniu tej wstępnej pracy zidentyfikujesz wiele luk w

zabezpieczeniach. Następnie musi opracować plan naprawczy dla każdego. W szczególności potrzebne będą plany naprawcze dla wszystkich zasobów, chyba że są one już dobrze chronione. Byłoby miło, gdybyś mógł natychmiast zamknąć wszystkie luki w zabezpieczeniach. Jednak prawie na pewno brakuje ci zasobów, aby to zrobić, a nawet jeśli masz zasoby, firmy mogą wchłonąć tylko tyle w danym momencie. Inwestorzy mają portfele inwestycji i oceniają spłaty z tych inwestycji. Ostrożnie inwestują, aby zmaksymalizować swoje zyski przy określonym poziomie ryzyka. Bezpieczeństwo IT musi również nadać priorytet projektom naprawczym, koncentrując się na tych, które przyniosą największe korzyści.

TEST XXIV

a. Co firma powinna najpierw zrobić, opracowując plan bezpieczeństwa IT?

b. Jakie są główne kategorie sił napędowych, które firma musi wziąć pod uwagę na przyszłość?

c. Co firma powinna zrobić dla każdego zasobu?

d. W jakim celu firma powinna opracować plany naprawcze?

e. W jaki sposób pracownicy bezpieczeństwa IT powinni postrzegać listę możliwych planów naprawczych jako portfolio?

PRZEPISY I REGULACJE ZGODNOŚCI

Siły napędowe

Wiele firm ma stosunkowo dobre plany bezpieczeństwa, zabezpieczenia i możliwości reagowania. Jednak aby planować przyszłość, nawet dobrze przygotowane firmy muszą rozumieć siły napędowe, które będą wymagały zmiany planowania bezpieczeństwa, zabezpieczeń i reagowania.

Siły napędowe to rzeczy, które wymagają od firmy zmiany planowania bezpieczeństwa, zabezpieczeń i reagowania

Być może najważniejszym zbiorem sił napędowych dla dzisiejszych firm są przepisy i regulacje dotyczące zgodności, które tworzą wymagania dotyczące bezpieczeństwa korporacyjnego. W wielu przypadkach firmy muszą znacznie poprawić swoje bezpieczeństwo, aby zachować zgodność z tymi przepisami i regulacjami. Jest to szczególnie prawdziwe w obszarach dokumentacji i zarządzania tożsamością. Te ulepszenia mogą być bardzo kosztowne. Innym problemem związanym z bezpieczeństwem korporacyjnym jest tak wiele przepisów i regulacji dotyczących zgodności.

Przepisy i regulacje dotyczące zgodności tworzą wymagania, na które muszą odpowiadać zabezpieczenia korporacyjne.

TEST XXV

a. Jakie są siły napędowe?

b. Co robią przepisy dotyczące zgodności?

c. Dlaczego przepisy i regulacje dotyczące zgodności mogą być drogie dla bezpieczeństwa IT?

Sarbanes-Oxley

Około 2000 roku doszło do kilku masowych oszustw finansowych, które kosztowały miliardy dolarów i spowodowały kryzys na giełdzie. Kongres odpowiedział, tworząc ustawę Sarbanes-Oxley Act z 2002 r. Ustawa ta spowodowała największą zmianę w wymogach sprawozdawczości finansowej od czasu Wielkiego Kryzysu. Zgodnie z ustawą Sarbanes-Oxley firmy muszą zgłaszać, czy mają jakiekolwiek

istotne braki w zakresie kontroli w swoim procesie sprawozdawczości finansowej. Firmy, które zgłaszają istotne niedociągnięcia w zakresie kontroli, prawdopodobnie uderzą w cenę akcji, a większość dyrektorów finansowych tych firm zniknie w ciągu kilku miesięcy. Jeśli dyrektor naczelny (CEO) lub dyrektor finansowy wprowadził w błąd, mogą pójść do więzienia. W przypadku istotnej słabości kontroli występuje „istotna słabość lub połączenie znaczących słabości, które powoduje większe niż znikome prawdopodobieństwo, że istotnemu zniekształceniu rocznego lub śródrocznego sprawozdania finansowego nie uda się zapobiec lub nie zostanie wykryte". Vorhies wskazuje, że 5-procentowy błąd w przychodach to typowy próg oznaczający niedostatek sprawozdawczości finansowej jako istotny. Unikanie słabości kontroli materiałów jest oczywiście bardzo trudne. Pod rządami Sarbanesa – Oxleya firmy musiały szczegółowo przyjrzeć się swoim procesom sprawozdawczości finansowej. W ten sposób odkryli wiele słabych punktów bezpieczeństwa, a w wielu przypadkach zdali sobie sprawę, że te słabości rozciągają się na inne części firmy. Biorąc pod uwagę znaczenie zgodności z ustawą Sarbanes – Oxley, większość firm była zmuszona do zwiększenia wysiłków w zakresie bezpieczeństwa.

TEST XXVI

a. Czym w Sarbanes-Oxley jest brak kontroli materiału?

b. Dlaczego Sarbanes-Oxley był ważny dla bezpieczeństwa IT?

Przepisy dotyczące ochrony prywatności

Kilka innych przepisów wpłynęło na wymagania dotyczące prywatności i ochrony informacji prywatnych. Są to między innymi:

• Dyrektywa Unii Europejskiej (UE) o ochronie danych z 2002 r. To szeroki zbiór przepisów zapewniających prawa do prywatności w Europie. Chociaż unijna dyrektywa o ochronie danych jest najważniejszą międzynarodową zasadą prywatności, wiele innych krajów, z którymi firmy amerykańskie prowadzą interesy, również opracowuje silne przepisy dotyczące prywatności danych handlowych.

• Amerykańska ustawa Gramm – Leach – Bliley Act (GLBA), znana również jako ustawa o modernizacji usług finansowych, z 1999 r. Wymaga silnej ochrony danych osobowych w instytucjach finansowych.

• Amerykańska ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) z 1996 r. Wymaga silnej ochrony danych prywatnych w organizacjach opieki zdrowotnej.

Przepisy te zmusiły firmy do sprawdzenia, w jaki sposób chronią dane osobowe, w tym gdzie te informacje są przechowywane i jak kontrolują dostęp do nich. W wielu przypadkach odkryli, że te informacje są przechowywane w wielu miejscach, w tym w dokumentach tekstowych i arkuszach kalkulacyjnych. Odkryli również, że kontrola dostępu i inne zabezpieczenia często są słabe lub nie istnieją.

TEST XXVII

a. Do czego zmusiły firmy przepisy dotyczące ochrony prywatności?

b. Co znaleźli, kiedy to zrobili?

c. Jakie instytucje podlegają ustawie Gramm – Leach – Bliley?

d. Jakie instytucje podlegają ustawie HIPAA?

Przepisy dotyczące powiadamiania o naruszeniu danych

Począwszy od kalifornijskiego prawa dotyczącego powiadamiania o naruszeniu danych z 2002 r. (SB 1386), pojawiła się rosnąca liczba przepisów, które wymagają od firm powiadamiania osób poszkodowanych w przypadku kradzieży lub nawet utraty poufnych danych osobowych (PII). Biorąc pod uwagę konsekwencje naruszenia bezpieczeństwa danych, firmy ponownie przemyślały swoje zabezpieczenia danych w systemach centralnych i aplikacjach użytkowników końcowych.

TEST XXVIII

a. Czego wymagają przepisy dotyczące powiadamiania o naruszeniu danych?

b. Dlaczego spowodowało to, że firmy zaczęły więcej myśleć o bezpieczeństwie?

Federalna Komisja Handlu

W Stanach Zjednoczonych Federalna Komisja Handlu (FTC) ma uprawnienia do ścigania firm, które nie podejmują rozsądnych środków ostrożności w celu ochrony prywatnych informacji. Chociaż istnieją ograniczenia uprawnień FTC, FTC nałożyła wysokie grzywny na firmy. Ma również prawo wymagać od firm płacenia za coroczne audyty przeprowadzane przez firmę zewnętrzną przez wiele lat i reagowania na te audyty.

TEST XXIX

a. Kiedy Federalna Komisja Handlu może działać przeciwko firmom?

b. Jakie obciążenia finansowe może nałożyć FTC na firmy, które nie podejmują rozsądnych środków ostrożności w celu ochrony prywatnych informacji?

Akredytacja branżowa

Wiele branż ma własne standardy akredytacji dla swoich członków. W wielu przypadkach firmy muszą wykazać określony poziom bezpieczeństwa, aby uzyskać akredytację. Branża szpitalna jest tego godnym uwagi przykładem.

TEST XXX

Jakie zewnętrzne zasady zgodności, poza ustawą HIPAA, muszą wziąć pod uwagę przy planowaniu ochrony?

PCI-DSS

Widzieliśmy, że Sarbanes – Oxley jest ważne dla wszystkich spółek notowanych na giełdzie i że FTC ma również szeroką jurysdykcję. Ponadto większość firm akceptuje płatności kartą kredytową. Wszystkie firmy, które to robią, podlegają zestawowi wymagań zwanych standardem Payment Card Industry - Data Security Standard, który jest prawie zawsze skrócony jako PCI-DSS. Standardy te zostały stworzone przez konsorcjum największych firm obsługujących karty kredytowe. Niestety, w wielu firmach zgodność ze standardem PCI-DSS jest opóźniona. Tak właśnie stało się w przypadku naruszenia danych przez TJX omówionego na początku.

TEST XXXI

Na jakie firmy wpływa PCI-DSS?

FISMA

Federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) z 2002 r. Została uchwalona w celu wzmocnienia bezpieczeństwa komputerów i sieci w rządzie federalnym i podmiotach

stowarzyszonych (takich jak wykonawcy rządowi) poprzez zlecanie corocznych audytów. FISMA narzuca zestaw procesów dla wszystkich systemów informatycznych używanych lub obsługiwanych przez agencję federalną Stanów Zjednoczonych, wykonawcę lub inną organizację w imieniu agencji rządowej USA. Te procesy muszą być zgodne z połączeniem dokumentów Federalnych Standardów Przetwarzania Informacji (FIPS), specjalnych publikacji serii SP-800 wydanych przez National Institute of Standards and Technology (NIST) oraz innych przepisów dotyczących federalnych systemów informacyjnych. FISMA ma dwa etapy. Pierwsza to certyfikacja systemu przez organizację samodzielnie lub przez stronę zewnętrzną. Ta ostatnia jest konieczna, jeśli kategoria ryzyka systemu jest wyższa niż określony próg Po certyfikacji systemu następuje przegląd pakietu dokumentacji bezpieczeństwa przez urzędnika akredytującego. Jeśli urzędnik ten jest zadowolony z certyfikacji, akredytuje system, wydając zezwolenie na prowadzenie działalności (ATO). Wszystkie akredytowane systemy są zobowiązane do monitorowania wybranego zestawu kontroli bezpieczeństwa pod kątem skuteczności, a dokumentacja systemu jest aktualizowana w celu odzwierciedlenia zmian i modyfikacji systemu. Znaczące zmiany w profilu bezpieczeństwa systemu powinny skutkować zaktualizowaną oceną ryzyka, a kontrole, które zostały znacznie zmodyfikowane, mogą wymagać ponownej certyfikacji. FISMA była ostro krytykowana za skupianie się na dokumentacji zamiast na ochronie. W chwili pisania tego tekstu rozważano zmiany w FISMA, aby umożliwić ocenę w czasie rzeczywistym i łatwiejsze raportowanie. Zmiany w FISMA mogą zostać opóźnione ze względu na proponowane dodatki, które pozwolą rządowi federalnemu przejąć kontrolę nad prywatnymi sieciami w przypadku sytuacji awaryjnej.

TEST XXXII

a. Kto podlega FISMA?

b. Rozróżnij certyfikację i akredytację w FISMA.

c. Dlaczego krytykowano FISMA?

ORGANIZACJA

Kompleksowe zabezpieczenie nie jest możliwe, jeśli korporacje nie zorganizują swoich pracowników ochrony, nie umieszczą ich skutecznie w strukturze organizacyjnej i nie sprecyzują swoich relacji z innymi jednostkami organizacyjnymi. W związku z tym planowanie musi rozpocząć się od umieszczenia funkcji ochrony w firmie.

Chief Security Officer

Różne organizacje nadają szefom działów bezpieczeństwa różne tytuły. Zwykły tytuł to szef ochrony (CSO). Innym jest dyrektor ds. bezpieczeństwa informacji (CISO). Będziemy korzystać z CSO.

TEST XXXIII

a. Jak zwykle nazywa się kierownik działu bezpieczeństwa?

b. Jaki jest inny tytuł dla tej osoby?

Czy powinieneś umieścić bezpieczeństwo w IT?

Pierwszym krokiem korporacji w zarządzaniu bezpieczeństwem jest podjęcie decyzji, gdzie funkcja bezpieczeństwa będzie się znajdować na schemacie organizacyjnym firmy. Nie ma magicznych odpowiedzi na pytanie, komu CSO i jego dział bezpieczeństwa powinni się zgłaszać. Jednak częstym problemem jest to, czy umieścić dział bezpieczeństwa wewnątrz, czy na zewnątrz korporacyjnej jednostki IT.

BEZPIECZEŃSTWO WEWNĄTRZ IT

Umieszczenie działu bezpieczeństwa IT w dziale technologii informatycznych (IT) jest atrakcyjne, ponieważ bezpieczeństwo i IT mają wiele wspólnych umiejętności technologicznych. Menedżerowie spoza działu IT mogą nie rozumieć problemów technologicznych na tyle dobrze, aby zarządzać funkcją zabezpieczeń. Inną korzyścią jest to, że bezpieczeństwo IT podlegałoby dyrektorowi ds. informacji w firmie. Jeśli CIO podlega bezpieczeństwu, CIO będzie odpowiedzialny za naruszenia bezpieczeństwa. Dyrektor IT prawdopodobnie poprze wysiłki działu bezpieczeństwa mające na celu stworzenie bezpiecznej infrastruktury IT. To ułatwiłoby również pozyskanie działu IT do wprowadzenia zmian w zakresie bezpieczeństwa.

BEZPIECZEŃSTWO POZA IT

Chociaż umieszczanie bezpieczeństwa w IT ma kilka zalet, ma również jedną poważną negatywną konsekwencję; bezpieczeństwo nie jest niezależne od IT. Wcześniej zauważyliśmy, że duża część wszystkich ataków na bezpieczeństwo korporacyjne pochodzi od samego personelu IT - czasami od starszych menedżerów IT. Jeśli dyrektor ds. informatyki zgłasza kwestie bezpieczeństwa, w jaki sposób może wymusić ochronę działań dyrektora IT? Zgłoszenie szefowi naruszenia bezpieczeństwa korporacyjnego może być „posunięciem ograniczającym karierę". Ponadto, podczas gdy bezpieczeństwo musi w dużym stopniu zajmować się IT, bezpieczeństwo IT jest znacznie szersze niż to. Lokalizowanie bezpieczeństwa IT poza IT może ułatwić radzenie sobie z innymi działami, które mają kluczowe znaczenie dla sukcesu w zakresie bezpieczeństwa. Jednakże, gdy bezpieczeństwo wykracza poza IT, pojawiają się nieuniknione trudności w przekonaniu funkcji IT, w tym dyrektora IT, do przyjęcia „rady" zewnętrznego działu bezpieczeństwa. Nawet jeśli bezpieczeństwo podlega kierownikowi wyższego szczebla, zorganizowanie wsparcia dla bezpieczeństwa w dziale IT może być trudne, zwłaszcza jeśli podległość IT przechodzi przez innego kierownika wyższego szczebla. Podstawowym problemem związanym z uczynieniem bezpieczeństwa IT działem personalnym poza IT jest to, że separacja zmniejsza odpowiedzialność. Dział personelu może tylko polecić. Żadna osoba w dziale liniowym nie jest odpowiedzialna za bezpieczeństwo firmy, z wyjątkiem kierownictwa firmy, którzy mają już szeroki zakres obaw. Aby przekręcić klasyczne stwierdzenie Harry'ego Trumana: „Groszek się nie kończy". Pomimo problemów, które pojawiają się przy umieszczaniu zabezpieczeń poza IT, większość analityków zaleca takie postępowanie. Potrzeba niezależności od IT jest zbyt ważna, aby rozważyć umieszczenie bezpieczeństwa w IT.

ROZWIĄZANIE HYBRYDOWE

Niektóre firmy starają się zrównoważyć bliskość IT i bezpieczeństwa IT z potrzebą niezależności. Robią to poprzez umieszczanie operacyjnych aspektów IT, takich jak utrzymywanie zapór ogniowych w IT, podczas umieszczania funkcji planowania, tworzenia polityki i audytu poza IT.

TEST XXXIV

a. Jakie są zalety umieszczenia zabezpieczeń w IT?

b. Jakie są wady umieszczania zabezpieczeń w IT?

c. Co większość analityków bezpieczeństwa IT zaleca w kwestii umieszczania lub nie umieszczania zabezpieczeń IT w IT?

d. W jaki sposób przydzielane są role zabezpieczeń w rozwiązaniu hybrydowym w celu umieszczenia zabezpieczeń IT wewnątrz lub na zewnątrz działu IT?

Wsparcie najwyższego kierownictwa

Niewiele firm ma raport CSO bezpośrednio do dyrektora generalnego firmy. Jednak wsparcie najwyższego kierownictwa ma kluczowe znaczenie dla powodzenia każdego programu bezpieczeństwa. Niewiele wysiłków tak powszechnych, jak bezpieczeństwo IT, powiedzie się, jeśli najwyższe kierownictwo nie zapewni silnego i spójnego wsparcia. Dowodem wsparcia najwyższego kierownictwa są kolejne działania.

• Jeśli najwyższe kierownictwo nie zapewni odpowiedniego budżetu na ochronę, wszelkie oświadczenia dotyczące polityki będą jedynie deklaracjami.

• Najwyższe kierownictwo musi wspierać bezpieczeństwo, gdy występują konflikty między potrzebami bezpieczeństwa a potrzebami innych funkcji biznesowych - na przykład, gdy w pośpiechu wprowadzany jest nowy system z nieodpowiednimi zabezpieczeniami.

• Subtelnie, ale co ważne, menedżerowie najwyższego szczebla muszą sami przestrzegać procedur bezpieczeństwa, na przykład gdy pracują z domu i zdalnie uzyskują dostęp do zasobów firmy. Wszystko, co robi kierownictwo wyższego szczebla, ma znaczenie symboliczne.

TEST XXXV

a. Dlaczego wsparcie najwyższego kierownictwa jest ważne?

b. Jakie trzy rzeczy musi zrobić najwyższe kierownictwo, aby okazać wsparcie?

Relacje z innymi działami

Aby odnieść sukces, dział bezpieczeństwa IT musi rozwijać produktywne relacje z innymi działami w firmie.

SZCZEGÓLNE RELACJE

Kilka jednostek organizacyjnych firmy ma szczególne znaczenie dla działu bezpieczeństwa IT. Specjaliści ds. Etyki, zgodności i prywatności.

Oprócz CSO większość firm ma dyrektorów ds. Etyki, zgodności i prywatności. Jeśli tych stanowisk nie ma w dziale bezpieczeństwa IT, koordynacja jest oczywiście niezbędna. Wiele firm łączy etykę, zgodność, prywatność i bezpieczeństwo w jeden wspólny dział. Jeśli jest to zrobione, wymaga to od kierownika działu znajomości wszystkich obszarów.

Działy zasobów ludzkich

Działy HR mają bogate i skomplikowane relacje z działami bezpieczeństwa. Za szkolenia, w tym szkolenia z zakresu bezpieczeństwa, odpowiada dział zasobów ludzkich. Ponadto dział zasobów ludzkich zajmuje się krytycznymi procesami zatrudniania i zwalniania pracowników. Bezpieczeństwo IT musi współpracować z zasobami ludzkimi przy procedurach zatrudniania i zwalniania, aby zapewnić uwzględnienie kwestii bezpieczeństwa. HR jest zawsze zaangażowany w sankcje, gdy pracownicy łamią zasady bezpieczeństwa.

Dział prawny

Aby zapewnić, że zasady bezpieczeństwa są zgodne z prawem, dział bezpieczeństwa musi współpracować z działem prawnym. Dział prawny angażuje się również w przypadku poważnych incydentów związanych z bezpieczeństwem.

Działy audytu

Większość korporacji ma już trzy działy audytu. Dział audytu wewnętrznego bada jednostki organizacyjne pod kątem wydajności, skuteczności i adekwatnych kontroli. Audyt finansowy robi to samo dla procesów finansowych. Dział audytu IT bada wydajność, efektywność i kontrolę procesów związanych z technologią informacyjną. Niektóre firmy powierzają audyt bezpieczeństwa IT (ale nie samego bezpieczeństwa) jednemu z tych działów w celu zapewnienia większej niezależności audytowi bezpieczeństwa. Dzięki temu audyt bezpieczeństwa IT może ujawnić dział bezpieczeństwa IT, a nawet CSO, jeśli to konieczne.

Zarządzanie obiektami

Eksploatacja i konserwacja budynków to zadanie zarządzania obiektami. W przypadku kamer bezpieczeństwa, kontroli wejść do budynku i podobnych spraw, ochrona musi ściśle współpracować z zarządem obiektów.

Jednolite bezpieczeństwo

Umundurowani pracownicy ochrony firmy będą oczywiście realizować zasady dotyczące dostępu do budynku. Umundurowani pracownicy ochrony są również potrzebni do przejęcia komputerów, które według bezpieczeństwa IT były zaangażowane w przestępstwa finansowe lub nadużycia. Z drugiej strony, bezpieczeństwo IT może pomóc mundurowym zabezpieczeniom z kamerami monitorującymi i analizą kryminalistyczną sprzętu, który mógł zostać użyty do popełnienia przestępstwa.

WSZYSTKIE DZIAŁY KORPORACYJNE

Poza tymi specjalnymi relacjami dział bezpieczeństwa musi mieć dobre relacje ze wszystkimi innymi funkcjami biznesowymi. Bezpieczeństwo IT nie może po prostu „wyrzucić polityk za mur" i oczekiwać, że będą przestrzegane. Inne działy prawie zawsze nie ufają bezpieczeństwu IT, ponieważ mogą one utrudniać życie. Chociaż personel ds. Bezpieczeństwa IT nie zawsze może współpracować z personelem innych działów, specjaliści ds. Bezpieczeństwa muszą nauczyć się mówić językami innych działów i rozumieć ich sytuację. Bezpieczeństwo powinno towarzyszyć politykom z analizą korzyści finansowych i realistycznymi oświadczeniami o wpływie na biznes. Zrozumienie, w jaki sposób bezpieczeństwo IT może wpływać na firmę i jej cele, jest ważniejsze niż doskonała wiedza technologiczna.

PARTNERZY BIZNESOWI

Planowanie zapór ogniowych i szeregu innych kontroli bezpieczeństwa zwykle zakłada, że istnieje granica między korporacją a światem zewnętrznym. Jednak jednym z największych trendów ostatnich lat była bliska, ale ostrożna integracja między firmami i ich partnerami biznesowymi, w tym organizacjami kupujących, organizacjami klientów, usługami organizacji, a nawet konkurenci. W celu ścisłej współpracy firmy zewnętrzne często potrzebują dostępu do systemów wewnętrznych. Oznacza to przebijanie dziur przez zapory ogniowe, przyznawanie uprawnień dostępu do hostów wewnętrznych i podejmowanie innych potencjalnie ryzykownych działań. Firmy muszą dochować należytej staranności przed kontaktem z firmami zewnętrznymi, co oznacza, że powinny dokładnie zbadać konsekwencje tych partnerstw w zakresie bezpieczeństwa IT przed ich rozpoczęciem

TEST XXXVI

a. Dlaczego dział zasobów ludzkich jest ważny dla bezpieczeństwa IT?

b. Rozróżnij trzy główne typy jednostek audytu korporacyjnego.

c. Jaka jest korzyść z umieszczenia audytu bezpieczeństwa IT w jednym z tych trzech działów audytów?

d. Jakie relacje może mieć ochrona IT z umundurowanymi pracownikami ochrony korporacji?

e. Co mogą zrobić pracownicy ochrony, aby lepiej dogadać się z innymi działami w firmie?

f. Kim są partnerzy biznesowi?

g. Dlaczego są niebezpieczne?

h. Co to jest należyta staranność?

Outsourcing bezpieczeństwa IT

Jedną z opcji jest outsourcing części lub całości zabezpieczeń IT. Całkowity outsourcing jest rzadkością, ponieważ firmy obawiają się utraty kontroli nad swoim bezpieczeństwem. Jednak częściowy outsourcing bezpieczeństwa IT jest powszechny.

OUTSOURCING E-MAIL

Najczęstszym outsourcingiem bezpieczeństwa IT jest poczta elektroniczna. Połączenia e-mail do iz Internetu są kierowane przez firmę zewnętrzną. (W niektórych przypadkach outsourcer internetowy lub e-mailowy umieści swój sprzęt w siedzibie klienta, ale kontroluje sprzęt zdalnie.) Firma zewnętrzna zapewnia zarówno filtrowanie przychodzące, jak i wychodzące. To filtrowanie obejmuje takie rzeczy, jak spam i złośliwe oprogramowanie w załącznikach oraz skrypty w treści wiadomości e-mail. Outsourcing filtrowania poczty e-mail jest atrakcyjny, ponieważ staje się wysoce wyspecjalizowaną dziedziną, która wymaga szybkiego reagowania na nowe zagrożenia. Ciągle pojawia się nowe złośliwe oprogramowanie. Listy niebezpiecznych źródeł wiadomości e-mail są aktualizowane co godzinę lub nawet szybciej.

Strategia i technologia bezpieczeństwa

ZARZĄDZANIE E-MAILEM DLA FIRM

Poczta elektroniczna stała się głównym środkiem komunikacji w środowisku biznesowym i nie ma żadnych oznak spowolnienia w najbliższym czasie. Chociaż niewielki procent wiadomości e-mail służy legalnym biznesom i do użytku osobistego, przeważający procent to spam. Spam to niechciana lub niechciana wiadomość e-mail wysyłana przez jednego użytkownika do wielu użytkowników bez rozróżnienia. Dla firm korzystanie z filtrowania spamu i wirusów jest jedyną realną alternatywą dla ręcznego codziennego sortowania spamu.

Pobieranie odcisków palców

Analiza odcisków palców w wiadomościach e-mail to nowe, gorące rozwiązanie do filtrowania wiadomości e-mail. Jego skuteczność i jakość sprawiają, że jest to jedno z najlepszych rozwiązań aby zarządzać pocztą elektroniczną dla korporacji. Analiza odcisków palców składa się z kilku elementów. Rozwiązanie do pobierania odcisków palców poczty e-mail bada cechy charakterystyczne lub odcisk palca lub każdą wiadomość e-mail wcześniej zidentyfikowaną jako spam i wykorzystuje te informacje do identyfikowania podobnych wiadomości. Kontrola odcisków palców w czasie rzeczywistym zapewnia ciągłe aktualizacje bazy danych na żywo, umożliwiając najdokładniejsze filtrowanie i prawie zero procent wskaźnika fałszywie pozytywnych Analiza odcisków palców to nie tylko analiza wiadomości e-mail i jej zawartości, ale także analiza pochodzenia wiadomości e-mail. Proces filtrowania sprawdza adresy URL zawarte w wiadomości e-mail i porównuje je z domenami wcześniej zidentyfikowanymi jako rozprzestrzeniające wiadomości e-mail zawierające spam. Jeśli odebrana wiadomość zawiera znany adres URL będący spamem, jest ona automatycznie identyfikowana jako spam i usuwana. Wielu dostawców usług i urządzeń do analizy odcisków palców utrzymuje duże bazy danych znanych adresów spamowych i treści e-mail, które są dostępne na całym świecie. Odciski

palców to inteligentne rozwiązanie do zwalczania spamu i wirusów w wiadomościach e-mail. Ten typ filtrowania opiera się na twierdzeniu Baye'a, zasadzie, że większość zdarzeń jest warunkowa lub zależna, a prawdopodobieństwo wystąpienia zdarzenia w przyszłości można wywnioskować z poprzednich wystąpień tego zdarzenia. Te filtry i bazy danych są nieustannie szkolone w zakresie odróżniania spamu od legalnej poczty e-mail.

Czarne listy i kontrola stawek

Kolejnym elementem filtrowania spamu i wirusów są czarne listy. Czarne listy to listy znanych adresów IP naruszających spam. Czarne listy są wykorzystywane w analizie odcisków palców w celu porównania adresu IP możliwego spamu z listą znanych adresów IP spamu. Czarne listy są publicznie dostępne i są również przechowywane w bazach danych podobnych do adresów URL naruszających spam. Kontrola prędkości zapobiega wykorzystywaniu przez spamerów i phisherów niczego niepodejrzewających sieci do wysyłania spamu i wirusów. Hakerzy i inni złośliwi napastnicy przejmują kontrolę nad komputerami w innych sieciach i używają tych komputerów do wysyłania dużych ilości spamu i wirusów w krótkim czasie. Kontrola szybkości pozwala na dokładną kontrolę wychodzących wiadomości e-mail, na przykład liczby wiadomości e-mail wysłanych w danym okresie i innego wychodzącego ruchu sieciowego. Takie kontrole kursów chronią korporacje i dostawców usług internetowych przed potencjalnymi stratami finansowymi i niedogodnościami takiego ataku. Kontrola stawek obejmuje weryfikację nadawcy i odbiorcy. Weryfikacja nadawcy i odbiorcy wykorzystuje wsteczne wpisy DNS w celu sprawdzenia, czy domeny nadawcy i odbiorcy są prawidłowe i nie są związane z rozprzestrzenianiem spamu. Ten rodzaj weryfikacji zapewnia również, że domeny mają uprawnienia do wysyłania i odbierania wiadomości e-mail od siebie nawzajem.

DOSTAWCA ZARZĄDZANYCH USŁUG BEZPIECZEŃSTWA

Inną alternatywą outsourcingu jest przekazanie jeszcze większej liczby kontroli zewnętrznej firmie zwanej zarządzanym dostawcą usług bezpieczeństwa (MSSP). Jak pokazano na rysunku 2-12, nad Twoją firmą czuwa MSSP. Umieszcza centralny serwer logowania w sieci. Ten serwer przesyła dane z dziennika zdarzeń firmy do witryny MSSP. Tam programy skanujące i eksperci ds. Bezpieczeństwa przeglądają dane dziennika, klasyfikują zdarzenia według poziomu istotności i odrzucają fałszywe alarmy. Jeśli MSSP wykonuje swoją pracę, każdego dnia będzie badać kilkaset podejrzanych zdarzeń. Szybko zidentyfikuje większość jako oczywiste fałszywe alarmy. Jeszcze inni zostaną sklasyfikowani jako zagrożenia, ale nieistotne, takie jak drobne ataki skanujące. W typowym dniu tylko jedno lub dwa pozornie poważne zagrożenia mogą zostać zgłoszone klientowi za pośrednictwem pagera lub alertów e-mail, w zależności od ich potencjalnej wagi. Przekształcając powódź podejrzanych incydentów na kilka ważnych wydarzeń wymagających codziennego działania ze strony klienta, MSSP uwalniają pracowników ochrony do pracy nad innymi sprawami. Dlaczego firma powinna używać MSSP? Jak powiedział Bruce Schneier czasami outsourcing ochrony odbywa się z tych samych powodów, dla których firmy „zlecają" gaszenie pożarów rządowi. Wewnętrzne straże pożarne byłyby prawie cały czas bezczynne. To uczyniłoby je niezwykle kosztownymi w przeliczeniu na ogień. Co gorsza, gdyby wezwano tę wewnętrzną siłę gaśniczą, byłaby niedoświadczona, ponieważ nie miałaby codziennego doświadczenia gaszenia pożarów , jakie mają miejscy strażacy. Kolejną zaletą korzystania z MSSP jest niezależność. Jeśli pracownicy MSSP zauważą, że dyrektor ds. Informatyki lub CSO firmy klienta robi coś, co wydaje się być sprzeczne z polityką firmy klienta, MSSP powiadomi o tym urzędnika wyższego szczebla w firmie. MSSP mogą działać jako kontrola przed członkami personelu IT, a nawet pracownikami bezpieczeństwa IT, o których zakłada się, że działają w najlepszym interesie firmy. MSSP może również przeprowadzać testy podatności. Zwykle firmy nie zlecają wszystkich kontroli podmiotom MSSP. Polityka i planowanie są zbyt ważne, aby zlecać je MSSP, chociaż MSSP musi znać zasady i procedury stworzone przez firmę. Chociaż MSSP mogą być bardzo pomocne, czasami

wykonują kiepską pracę. Jeśli w umowie określono, że MSSP będzie przeglądać dzienniki, ale nie jest to bardziej szczegółowe, firma outsourcingowa może po prostu skanować pliki dziennika w pobieżny sposób mniej więcej co tydzień. Jedna firma poinformowała, że w ciągu pierwszych sześciu miesięcy świadczenia usług MSSP nie wysłał do niej ani jednego ostrzeżenia. Firma uważała, że świadczy to o całkowitym zaniedbaniu ze strony firmy outsourcingowej.

TEST XXXVII

a. Co to jest MSSP?

b. Jakie są dwie główne zalety korzystania z MSSP?

c. Dlaczego dostawcy usług MSSP wykonują lepszą pracę niż pracownicy działu bezpieczeństwa IT?

d. Jakie funkcje bezpieczeństwa są zazwyczaj zlecane na zewnątrz?

e Jakie funkcje bezpieczeństwa zazwyczaj nie są zlecane na zewnątrz?

f. Na co powinna zwrócić uwagę firma przy wyborze MSSP?

ANALIZA RYZYKA

Planowanie bezpieczeństwa IT zawsze koncentruje się na ryzyku. Większość ludzi uważa, że specjaliści od bezpieczeństwa IT próbują wyeliminować ryzyko. Jednak w biznesie nigdy nie jest możliwe całkowite wyeliminowanie ryzyka. Celem jest zarządzanie ryzykiem. Ten pogląd jest nawet ujęty w pojęciu zapewniania informacji lub zarządzania ryzykiem związanym z systemami informatycznymi, które przetwarzają, przechowują i wykorzystują informacje. Wymaga to sposobu myślenia o ryzyku zwanego analizą ryzyka. Analiza ryzyka porównuje prawdopodobne straty z kosztami ochrony. Nie ma sensu płacić miliona dolarów za ochronę laptopa o wartości 2000 dolarów, który nie zawiera poufnych informacji. Ten przykład jest oczywiście uproszczony. Oczywiście w rzeczywistych zabezpieczeniach porównywanie kosztów i korzyści jest znacznie bardziej złożone.

Rozsądne ryzyko

Termin „zapewnienie informacji" jest nieco mylący, sugerując, że firma może zagwarantować poufność, integralność i dostępność swoich informacji. To bzdury. Przecież rabunek istnieje od zarania dziejów i żadne społeczeństwo go nie wyeliminowało. Całkowite bezpieczeństwo IT jest równie niemożliwe. Firmy muszą raczej myśleć w kategoriach rozsądnego ryzyka opartego na analizie ryzyka. Chociaż bezpieczeństwo może zmniejszyć ryzyko ataków, ma negatywne skutki uboczne. Najwyraźniej zabezpieczenia mają tendencję do ograniczania funkcjonalności. Życie w środowisku o wysokim poziomie bezpieczeństwa może być nieprzyjemne i zwykle nieefektywne. Jeśli mieszkasz w cichym i bezpiecznym miejscu sąsiedztwa, umieszczenie krat w oknach spowodowałoby nieprzyjemne uczucie zamknięcia. Wymaganie zapamiętania długiego hasła, aby dostać się do domu, spowolniłoby cię za każdym razem, gdy wchodzisz do domu. Oprócz tych kosztów psychologicznych i związanych z produktywnością, bezpieczeństwo nigdy nie jest darmowe i rzadko kiedy jest tanie. Urządzenia zabezpieczające są drogie, a praca przy ich wdrażaniu i obsłudze może być jeszcze droższa.

TEST XXXVIII

a. Dlaczego zapewnianie informacji to kiepska nazwa dla bezpieczeństwa IT?

b. Dlaczego uzasadnione ryzyko jest celem bezpieczeństwa IT?

c. Jakie są negatywne konsekwencje bezpieczeństwa IT?

Obliczenia klasycznej analizy ryzyka

Niektóre egzaminy certyfikujące bezpieczeństwo IT sprawdzają prosty proces (1) obliczania prawdopodobnych strat, (2) obliczania, w jaki sposób środki zaradcze zmienią prawdopodobieństwo strat oraz (3) decydowania, czy te środki zaradcze przynoszą korzyści przewyższające ich koszty.

	Base Case	Countermeasure	
		A	B
Asset Value (AV)	$100,000	$100,000	$100,000
Exposure Factor (EF)	80%	20%	80%
Single Loss Expectancy (SLE): = AV*EF	$80,000	$20,000	$80,000
Annualized Rate of Occurrence (ARO)	50%	50%	25%
Annualized Loss Expectancy (ALE): = SLE*ARO	$40,000	$10,000	$20,000
ALE Reduction for Countermeasure	NA	$30,000	$20,000
Annualized Countermeasure Cost	NA	$17,000	$4,000
Annualized Net Countermeasure Value	NA	$13,000	$16,000

WARTOŚĆ AKTYWÓW

Pierwsza linia podaje wartość chronionego zasobu. Na rysunku wartość aktywów to 100 000 USD.

CZYNNIK EKSPOZYCJI

Współczynnik ekspozycji to procent wartości aktywów, który zostałby utracony w przypadku naruszenia. Na rysunku współczynnik ekspozycji wynosi 80 procent. Oznacza to, że kompromis spowodowałby utratę 80% wartości aktywów.

OCZEKIWANIE POJEDYNCZEJ STRATY

Oczekiwana wartość pojedynczej straty to wielkość szkód, które zostałyby poniesione w przypadku pojedynczego naruszenia. Oczekiwana pojedyncza strata to iloczyn wartości aktywów i współczynnika ekspozycji. Na rysunku jest to 80 000 USD (100 000 razy 80%).

ROCZNE PRAWDOPODOBIEŃSTWO (LUB WARTOŚĆ) WYSTĘPOWANIA

Teraz, gdy wiemy, ile szkód spowodowałoby jedno naruszenie, następnym problemem jest częstotliwość występowania naruszeń. Zwykle odbywa się to w ujęciu rocznym. Oznacza to, że w tym , na przykład atak powinien się udać mniej więcej raz na dwa lata.

ROCZNE OCZEKIWANIE STRAT

Roczne prawdopodobieństwo wystąpienia pomnożone przez oczekiwaną pojedynczą stratę daje zannualizowaną oczekiwaną stratę - średnią roczną stratę oczekiwaną z tego rodzaju kompromisu dla tego składnika aktywów. Na rysunku ALE wynosi 40 000 USD (80 000 USD razy 50%).

ŚRODKI ZARADCZE

Następnym krokiem jest ocena korzyści wynikających ze środka zaradczego. Zmniejszyłoby to roczne oczekiwane straty z 40 000 USD do 10 000 USD. To byłaby oszczędność w wysokości 30 000 dolarów. Przeciwdziałanie B ma inny efekt. Zmniejsza roczne prawdopodobieństwo wystąpienia z raz na dwa

lata do raz na cztery lata. Ten środek zaradczy zmniejszy ALE z 40 000 USD do 20 000 USD. To oszczędność 20 000 dolarów

ROCZNY KOSZT ŚRODKÓW ŚRODKOWYCH I WARTOŚĆ NETTO

Jak dotąd Przeciwdziałanie A wygląda lepiej niż Przeciwdziałanie B, oszczędzając dodatkowe 10 000 USD rocznie. Jednak środki zaradcze nigdy nie są darmowe. Aby porównać ten koszt ze zannualizowaną wartością środka zaradczego, koszt ten musi być rocznym kosztem środka zaradczego. Aby obliczyć roczny koszt środka zaradczego, ważne jest, aby wziąć pod uwagę zarówno koszty zakupu, jak i koszty operacyjne. Środek zaradczy B tylko przynosi roczne korzyści w wysokości 20 000 USD, ale jest niedrogi i kosztuje tylko 4 000 USD rocznie. Zatem roczna wartość netto środka zaradczego Countermeasure B wynosi 16 000 USD rocznie. Ogólnie rzecz biorąc, chociaż środek zaradczy B nie zmniejsza oczekiwanej straty w ujęciu rocznym tak bardzo, jak środek zaradczy A, niższy koszt środka zaradczego B sprawia, że jest to opcja preferowana. Ważne jest, aby wziąć pod uwagę wszystkie koszty środków zaradczych, w tym koszty niezwiązane z bezpieczeństwem. Jeśli środek zaradczy ogranicza funkcjonalność systemu na tyle, aby mieć poważny wpływ na produktywność użytkowników, koszt ten należy traktować jako część całkowitych kosztów środków zaradczych.

TEST XXXIX

a. Dlaczego w obliczeniach analizy ryzyka dokonujemy annualizacji kosztów i korzyści?

b. Jak obliczyć ALE?

Aktywa mają wartość 1 000 000 USD. Oczekuje się, że podczas ataku straci 60 procent swojej wartości. Przeciwdziałanie X zmniejszy straty o dwie trzecie. Przeciwdziałanie Y zmniejszy straty o połowę. Oba środki zaradcze będą kosztować 20 000 USD rocznie. Atak może zakończyć się sukcesem raz na dziesięć lat. Oba środki zaradcze mogą zmniejszyć częstotliwość występowania o połowę. Przeanalizuj te środki zaradcze, a następnie przekaż swoje zalecenia.

Problemy z obliczeniami klasycznej analizy ryzyka

Chociaż klasyczne obliczenia analizy ryzyka są powszechnie nauczane, są one trudne lub niemożliwe do zastosowania w praktyce.

NIERÓWNE WIELOLETNIE PRZEPŁYWY PIENIĘŻNE

Problem z klasyczną analizą ryzyka polega na tym, że zakłada ona, że korzyści i koszty środków zaradczych będą co roku takie same. W praktyce koszt środka zaradczego jest często najwyższy w pierwszym roku, a następnie spada do niższego poziomu. Z kolei korzyści często rosną w czasie, gdy środek zaradczy staje się bardziej znany, a zatem prawdopodobnie będzie skuteczniej stosowany. Później, gdy środek zaradczy się starzeje, koszt może wzrosnąć, a korzyści mogą spaść. Kiedy przez kilka lat występują nierówne przepływy pieniężne, decydenci zwracają się do analizy zdyskontowanych przepływów pieniężnych, która jest również nazywana analizą zwrotu z inwestycji (ROI). Wymaga to obliczenia wartości bieżącej netto (NPV) lub wewnętrzna stopa zwrotu (IRR).

CAŁKOWITY KOSZT SZKODY

Poważnym, ale łatwym do rozwiązania problemem w klasycznej analizie ryzyka jest jej miara szkody - utraty wartości aktywów. To absurd, ponieważ szkody mogą wystąpić na wiele sposobów. Na przykład, jeśli dane klienta zostaną skradzione w celu kradzieży tożsamości, wartość aktywów w ogóle nie zostanie zmniejszona. Jednak koszt naruszenia może być ogromny. Prostym sposobem rozwiązania tego problemu bez silnego zakłócania klasycznych obliczeń analizy ryzyka jest zastąpienie obliczenia

przewidywanej pojedynczej straty wartością całkowitego kosztu incydentu (TCI), która daje szacunki całkowitego kosztu kompromisu, w tym kosztów napraw, procesów i wiele innych czynników.

WIELE DO WIELU RELACJI MIĘDZY ŚRODKAMI I ZASOBAMI

Trudniejszym problemem jest to, że klasyczne podejście zakłada relację jeden do jednego między środkami zaradczymi a zasobami. To rzadko się zdarza. Na przykład zapora graniczna chroni wszystkie serwery i klientów za nią. Innymi słowy, jeden środek zaradczy może chronić wiele aktywów, a jeden składnik aktywów może być chroniony wieloma różnymi środkami zaradczymi. W takich przypadkach proste klasyczne obliczenia całkowicie się psują.

NIEMOŻLIWOŚĆ OBLICZENIA ROCZNIONYCH WSPÓŁCZYNNIKÓW WYSTĘPOWANIA

Najgorszym problemem z klasyczną analizą ryzyka jest to, że rzadko jest możliwe oszacowanie rocznego wskaźnika występowania zagrożeń. Gdzie planista może znaleźć takie prawdopodobieństwa? Prosty fakt jest taki, że nie ma nawet przeciętnego źródła dobrej informacji o częstotliwości ataków różnego typu, a tym bardziej procentu takich ataków, które się powiodą. Po prostu niemożliwe jest dokładne obliczenie rocznego prawdopodobieństwa wystąpienia, a zatem nie można porównać kosztów środków zaradczych z ich korzyściami. Nie ma źródła danych dotyczących możliwości ataku, więc nie można obliczyć rocznej oczekiwanej straty. Alternatywą jest przeprowadzenie analizy uszkodzeń na bardziej zgrubnym poziomie. Na przykład może istnieć możliwość sklasyfikowania zagrożeń dla zasobów za pomocą szerokich kategorii, takich jak krytyczne, znaczące lub drugorzędne. Umożliwi to firmie ustalenie priorytetów ryzyk i skupienie się na tych o najwyższym priorytecie. Następnie pracownicy ochrony mogą zaplanować środki zaradcze dla tych głównych zagrożeń.

PROBLEM Z „TWARDYM MYŚLENIEM"

Chociaż twarde liczby są uspokajające i powinny być używane w miarę możliwości, badacze operacyjni ostrzegają również, że „liczby wypędzają myślenie". Krytyczne względy, które nie są tak łatwe do określenia ilościowego, można zignorować lub mocno bagatelizować. Poniższy przykład ilustruje ten punkt. Kiedy Maria Lopez przejęła linię meksykańskiej żywności Papa Lopez swojego ojca, spotkała się z dyrektorem ds. Informacji firmy, aby omówić plany firmy dotyczące aplikacji do zarządzania relacjami z klientami, propozycji sieci bezprzewodowej i propozycji bezpieczeństwa8. z Wharton School of Business Maria zażądała analizy zwrotu z inwestycji (ROI) trzech propozycji. Analizy zwrotu z inwestycji wyraźnie wykazały duże pozytywne korzyści netto dla aplikacji do zarządzania relacjami z klientami i sieci bezprzewodowej. Z drugiej strony korzyści z projektu bezpieczeństwa były niemożliwe do oszacowania. Firma minimalnie zainwestowała w bezpieczeństwo. Wkrótce do bazy danych firmy włamano się, a poufne dane osobowe klientów zostały skradzione. Nie istniał żaden plan reagowania, więc naprawienie luki w zabezpieczeniach, która umożliwiła włamanie, zajęło tygodnie. Ponadto rodzinny przepis na salsę został skradziony, a szantażysta zażądał pieniędzy, aby uniknąć jego wydania. Co gorsza, Biuro Prokuratora Generalnego Kalifornii powiadomiło firmę, że może zostać pociągnięta do odpowiedzialności karnej za zaniedbanie w zakresie ochrony informacji o klientach. Aby podkreślić problem, sprzedaż szybko spadła o 50 procent. ROI to świetne narzędzie, w którym można go używać, ale liczby nigdy nie powinny zniechęcać do myślenia. Ten przypadek nie jest wyjątkowy. W przypadku inwestycji w bezpieczeństwo zmierzenie zwrotu z inwestycji jest trudne, jeśli nie niemożliwe. Fakt ten stwarza duże problemy dla firm, które ślepo wykorzystują zwrot z inwestycji.

Inwestycje w bezpieczeństwo IT często zapobiegają dużym stratom, zamiast zwracać dodatkowe korzyści finansowe. Dodajmy do tego trudność oszacowania prawdopodobieństwa straty, a uzasadnienie inicjatyw związanych z bezpieczeństwem IT kierownikom biznesowym staje się trudne.

PERSPEKTYWICZNY

Paradoksalnie, chociaż klasyczna analiza ryzyka jest niemożliwa, firmy muszą spróbować zrobić to lub coś podobnego. Nakłada ogólną dyscyplinę w myśleniu o zagrożeniach i środkach zaradczych. Określa kluczowe kwestie, nawet jeśli nie można ich dokładnie określić ilościowo. Ponadto, gdy wartość środka zaradczego znacznie przekracza koszt środka zaradczego (lub gdy występuje odwrotnie), problemy z kwantyfikacją niektórych wartości są nieistotne. W każdym razie firmy nigdy nie powinny przeprowadzać klasycznych obliczeń analizy ryzyka według wartości nominalnej.

TEST XL

a. Dlaczego jest to problem, jeśli korzyści i koszty pojawiają się przez kilka lat?

b. Dlaczego całkowity koszt incydentu (TCI) powinien być używany zamiast czynników ekspozycji i wartości aktywów?

c. Dlaczego nie można zastosować klasycznych obliczeń analizy ryzyka dla zapór?

d. Jaki jest najgorszy problem z klasycznym podejściem?

e Dlaczego beztroskie myślenie o zwrocie z inwestycji w bezpieczeństwo jest niebezpieczne?

Reagowanie na ryzyko

Do tej pory omawialiśmy odpowiedzi na zagrożenia w jeden sposób, instalując środki zaradcze. Istnieją jednak cztery logiczne możliwe reakcje na ryzyko.

REDUKCJA RYZYKA

Najbardziej oczywistą reakcją na ryzyko jest redukcja ryzyka - zastosowanie aktywnych środków zaradczych, takich jak instalacja zapór ogniowych. Będzie to naszym celem w całej książce. Jednak nie zawsze jest to najlepsze podejście.

AKCEPTACJA RYZYKA

Jeśli jednak wpływ szkody byłby niewielki, a koszt środków zaradczych przewyższałby prawdopodobną szkodę naruszenia, sensowne jest podjęcie decyzji o akceptacji ryzyka - bez podejmowania środków zaradczych i absorbowaniu ewentualnych szkód. Brak opancerzenia dachu przed uderzeniami meteorytów jest przykładem osobistej akceptacji ryzyka.

PRZENIESIENIE RYZYKA (UBEZPIECZENIE)

Trzecią możliwością jest przeniesienie ryzyka - ktoś inny wchłania ryzyko. Najczęstszym przykładem przeniesienia ryzyka jest ubezpieczenie, w którym towarzystwo ubezpieczeniowe pobiera roczną składkę, w zamian za którą zapłaci w przypadku wystąpienia szkody. Ubezpieczenie (i ogólnie przenoszenie ryzyka) jest szczególnie dobre w przypadku ataków, które są rzadkie, ale niezwykle niszczące. Dlatego właściciele domów kupują ogniowe i ubezpieczenie powodziowe. Firmy ubezpieczeniowe często wymagają, aby klienci zainstalowali rozsądne środki zaradcze, zanim zapewnią ochronę, więc ubezpieczenie nie może być wykorzystywane jako sposób całkowitego zaniedbania bezpieczeństwa. Ponadto ubezpieczenie będzie miało znacznie wyższe odliczenia, jeśli ochrona firmy nie będzie tak silna, jak powinna. Jedną konkretną kwestią jest to, jakie zagrożenia obejmuje polisa ubezpieczeniowa, a jakie nie. Szkody spowodowane klęskami żywiołowymi, cyberterrorem i cyberwojną często są wyraźnie wyłączone z zakresu ochrony.

UNIKANIE RYZYKA

Ostatnim wyborem jest unikanie ryzyka, czyli niepodejmowanie zbyt ryzykownych działań. Na przykład, jeśli korzystanie z usług outsourcera do przechowywania prywatnych danych klientów lub pracowników jest zbyt ryzykowne, firma po prostu tego nie zrobi. Chociaż unikanie ryzyka jest dobre z punktu widzenia ryzyka, oznacza to, że firma musi zrezygnować z innowacji, która byłaby atrakcyjna, gdyby problemy z bezpieczeństwem jej nie „zabiły". Nie podoba się to reszcie firmy bezpieczeństwa IT.

Unikanie ryzyka oznacza niepodejmowanie ryzykownych działań.

TEST XLI

a. Jakie są cztery sposoby reagowania na ryzyko?

b. Co oznacza nic nie robienie?

c. Co obejmuje ubezpieczenie?

d. Dlaczego ubezpieczenie nie jest sposobem na uniknięcie bezpieczeństwa?

e. Co to jest unikanie ryzyka?

f. Dlaczego unikanie ryzyka nie traktuje bezpieczeństwa IT dla reszty firmy?

ARCHITEKTURA ZABEZPIECZENIA TECHNICZNEGO

Nigdy nie zbudowałbyś domu, gdyby architekt nie stworzył najpierw szerokiego projektu pomieszczeń w domu i sposobów ich interakcji, aby zapewnić pełne wrażenia z życia. Ten szeroki projekt nazywa się architekturą.

Architektury bezpieczeństwa technicznego

W ten sam sposób firmy nie powinny instalować technicznych środków zaradczych bez ogólnego planu. Ten plan jest techniczną architekturą zabezpieczeń firmy, która obejmuje wszystkie techniczne środki zaradcze firmy - w tym zapory ogniowe, wzmocnione hosty, systemy wykrywania włamań i inne narzędzia - oraz sposób zorganizowania tych środków w kompletny system ochrony.

Architektura zabezpieczeń technicznych firmy obejmuje wszystkie techniczne środki zaradcze firmy oraz sposób ich zorganizowania w kompletny system ochrony.

DECYZJE ARCHITEKTONICZNE

Termin architektura wskazuje, że systemy bezpieczeństwa firmy nie powinny po prostu ewoluować w nieskoordynowanej serii indywidualnych decyzji inwestycyjnych w zakresie bezpieczeństwa. Powinien raczej istnieć spójny plan architektoniczny, który pozwoli firmie wiedzieć, że techniczne zabezpieczenia są dobrze dopasowane do potrzeb w zakresie ochrony aktywów przedsiębiorstwa i zagrożenia zewnętrzne. Głównym celem jest stworzenie wszechstronnej ściany bez dziur, przez które mogliby przejść napastnicy.

POSTĘPOWANIE ZE STARSZĄ TECHNOLOGIĄ BEZPIECZEŃSTWA

Architektury bezpieczeństwa zwykle muszą uwzględniać starsze technologie bezpieczeństwa firmy, które są technologiami bezpieczeństwa, które firma wdrożyła w przeszłości, ale obecnie są przynajmniej nieco nieskuteczne. Żadna firma nie może sobie pozwolić na jednoczesną wymianę wszystkich starszych technologii bezpieczeństwa. Jeśli starsza technologia poważnie osłabia zabezpieczenia, należy ją wymienić. Jednak o ile korzyści z aktualizacji nie przewyższają kosztów aktualizacji, firmy muszą obejść starsze technologie zabezpieczeń, dodając mocne strony w innych obszarach, aby zrekompensować ograniczenia dotychczasowej technologii zabezpieczeń.

Starsze technologie bezpieczeństwa to technologie bezpieczeństwa, które firma wdrożyła w przeszłości, a obecnie są co najmniej nieco nieskuteczne

TEST XLII

a. Jaka jest techniczna architektura zabezpieczeń firmy?

b. Dlaczego potrzebna jest techniczna architektura zabezpieczeń?

c. Kiedy najlepiej je założyć?

d. Dlaczego firmy nie zastępują natychmiast swoich starszych technologii zabezpieczeń?

Zasady

Chociaż tworzenie architektury bezpieczeństwa wymaga podejmowania wielu decyzji na podstawie złożonych informacji sytuacyjnych, przy projektowaniu architektury bezpieczeństwa należy kierować się pewnymi ogólnymi zasadami.

OBRONA W GŁĘBI

Pierwsza zasada to głęboka obrona. Z głęboką obroną atakujący musi przebić się przez wiele środków zaradczych, aby odnieść sukces. Na przykład, aby zaatakować serwer, osoba atakująca może być zmuszona do przebicia się przez graniczną zaporę ogniową, przez wewnętrzną zaporę ogniową, a na końcu przez zabezpieczenia aplikacji wzmocnionej na wzmocnionym serwerze. Powód głębokiej obrony jest prosty. Zgłaszający luki w zabezpieczeniach znajdują problemy w prawie każdym środku ochrony raz lub częściej w roku. Podczas gdy luka w jednym elemencie obronnym jest naprawiana, inne na linii obrony pozostaną skuteczne, udaremniając atakującego.

OBRONA W GŁĘBI A NAJSŁABSZE LINKI

Możesz być zdezorientowany różnicą między głęboką obroną a najsłabszymi ogniwami. W głębokiej obronie istnieje szereg niezależnych środków zaradczych. Jeśli jeden środek zaradczy zawodzi, inne pozostają na miejscu. Natomiast w przypadku awarii najsłabszego łącza istnieje jeden środek zaradczy złożony z wielu współzależnych komponentów. Współzależność oznacza, że jeśli ktoś zawodzi, wszystkie zawodzą.

POJEDYNCZE PUNKTY WRAŻLIWOŚCI

Na przeciwległym krańcu obrony w głębi znajduje się pojedynczy punkt podatności - element architektury, w którym atakujący może wyrządzić ogromne szkody, narażając pojedynczy system. Na przykład podczas ataków terrorystycznych z 11 września 2001 r. odkryto, że większość operatorów telekomunikacyjnych w Nowym Jorku połączyła swoje linie przesyłowe pod World Trade Center. Zawalenie się wież nie rzuciło internetu na kolana, ale znacznie obniżyło ruch internetowy. Pojedyncze punkty podatności często występują na serwerze DNS firmy (chyba że ma ich kilka), który jest centralnym menedżerem programu zarządzania siecią firmy oraz indywidualne zapory. Nie wszystkie pojedyncze punkty awarii można wyeliminować. Każda architektura bezpieczeństwa, której urządzenia nie są kontrolowane centralnie, może implementować niespójne zasady, a wiele działań podejmowanych w celu udaremnienia trwającego ataku wymaga systemowej odpowiedzi, która może działać tylko przez centralny punkt kontroli. Wraz z rozwojem centralnego zarządzania zasobami bezpieczeństwa coraz ważniejsze będzie zabezpieczenie konsol centralnego zarządzania bezpieczeństwem i ich komunikacji z urządzeniami zabezpieczającymi firmy.

MINIMALIZACJA OBCIĄŻEŃ BEZPIECZEŃSTWA

Kolejną podstawową zasadą jest minimalizowanie obciążeń bezpieczeństwa w działach funkcjonalnych. Do pewnego stopnia bezpieczeństwo nieuchronnie zmniejsza produktywność i może spowolnić tempo innowacji, wymagając, aby kwestie bezpieczeństwa zostały rozwiązane przed wprowadzeniem innowacji. Ważne jest, aby wybrać architektury i elementy zabezpieczeń, które minimalizują utratę produktywności i spowolnienie innowacji. W rzeczywistości w firmach, które są wysoce innowacyjne, bezpieczeństwo może być jedynym czynnikiem hamującym wzrost. Częstym zarzutem menedżerów funkcjonalnych jest „Nie rozumiesz". Wartość wzrostu w porównaniu z wartością ochrony bezpieczeństwa należy dokładnie rozważyć. Jednak wiele działań może znacznie zmniejszyć obciążenia użytkowników, na przykład przejście na uwierzytelnianie jednokrotnego logowania, tak że każda osoba będzie musiała pamiętać tylko jedno hasło, aby korzystać ze wszystkich systemów wewnętrznych.

REALISTYCZNE CELE

Chociaż byłoby miło móc usunąć wszystkie luki z dnia na dzień, ważne jest, aby mieć realistyczne cele dotyczące ulepszeń. Na przykład w 1999 roku NASA opracowała listę swoich najpoważniejszych luk w zabezpieczeniach - listę, którą stale aktualizuje. Od 2000 roku wszystkie systemy podłączone do sieci były testowane pod kątem tych wad. NASA postawiła sobie za cel zmniejszenie stosunku podatności na komputery z 1: 1 do 1: 4. W 2002 roku stosunek spadł do 1: 0. Tworząc ducha rywalizacji, NASA była w stanie osiągnąć znaczne zyski, wydając zaledwie 2-3 mln USD rocznie (30 USD na komputer).

TEST XLIII

a. Dlaczego obrona głęboka jest ważna?

b. Rozróżnij między obroną w głębi a problemami z najsłabszym ogniwem.

c. Dlaczego konsole centralnego zarządzania bezpieczeństwem są niebezpieczne?

d. Dlaczego są pożądane?

e. Dlaczego ważne jest, aby minimalizować obciążenia, jakie bezpieczeństwo nakłada na jednostki funkcjonalne w firmie?

f. Jak myślisz, dlaczego ważne jest, aby mieć realistyczne cele dotyczące zmniejszenia podatności?

Elementy architektury bezpieczeństwa technicznego

Przyjrzymy się szczegółowo wielu kontrolom technicznym firmy oraz sposobowi organizacji tych kontroli. W tym miejscu wymienimy jedynie kilka klas technicznych środków zaradczych stosowanych przez firmy.

ZARZĄDZANIE GRANICAMI

Tradycyjnie firmy utrzymywały granicę między swoimi (względnie zaufanymi) sieciami wewnętrznymi a niezaufanymi sieciami zewnętrznymi, najczęściej Internetem. Zapory ogniowe były podstawą zarządzania granicami i powinny pozostać nimi.

ZARZĄDZANIE BEZPIECZEŃSTWEM MIEJSCA WEWNĘTRZNEGO

Istotne jest również wewnętrzne zarządzanie zaufaną siecią wewnętrzną. W celu zapobiegania należy stosować wewnętrzne zapory ogniowe, zabezpieczonych klientów i serwery, systemy wykrywania włamań i inne narzędzia.

ZARZĄDZANIE ZDALNYMI POŁĄCZENIAMI

Poza granicami potrzebne są zdalne połączenia między lokacjami korporacyjnymi, poszczególnymi pracownikami zdalnymi i partnerami biznesowymi. Technologie wirtualnych sieci prywatnych odgrywają kluczową rolę w zarządzaniu komunikacją między zaufanymi użytkownikami a witrynami w niezaufanych sieciach, takich jak Internet. Indywidualni pracownicy pracujący z domu i pokoju hotelowego stanowią szczególny problem, zwłaszcza gdy pracownicy umieszczają osobiste oprogramowanie na swoich zdalnych komputerach. W rzeczywistości często używają własnych komputerów domowych do uzyskiwania dostępu do witryn firmowych. Ogólny brak dyscypliny bezpieczeństwa wśród użytkowników domowych można złagodzić dzięki zarządzaniu technologią zdalnego dostępu.

SYSTEMY INTERORGANIZACYJNE

W systemach międzyorganizacyjnych dwie firmy łączą niektóre ze swoich zasobów IT i żadna z nich nie może bezpośrednio wymusić bezpieczeństwa w drugiej. W rzeczywistości często nie potrafią nawet poznać szczegółów bezpieczeństwa w innej firmie.

W systemach międzyorganizacyjnych dwie firmy łączą niektóre ze swoich zasobów IT.

CENTRALNE ZARZĄDZANIE BEZPIECZEŃSTWEM

Ważnym celem w architekturach bezpieczeństwa jest scentralizowane zarządzanie bezpieczeństwem - możliwość zarządzania technologiami bezpieczeństwa z pojedynczej konsoli zarządzania bezpieczeństwem lub przynajmniej z kilku stosunkowo niewielu konsol zarządzania bezpieczeństwem, z których każda zarządza klastrem technologii bezpieczeństwa. Scentralizowane zarządzanie bezpieczeństwem wymusza zasady bezpośrednio na urządzeniach firmy, zapewniając spójność zabezpieczeń. Obniża również koszt zarządzania bezpieczeństwem poprzez redukcję podróży i umożliwia natychmiastowe oddziaływanie działań związanych z zarządzaniem bezpieczeństwem na urządzenia.

TEST XLIV

a. Dlaczego zarządzanie granicami jest ważne?

b. Dlaczego nie jest to kompletne rozwiązanie zabezpieczające?

c. Dlaczego połączenia zdalne z domu są szczególnie niebezpieczne?

d. Dlaczego systemy międzyorganizacyjne są niebezpieczne?

e. Dlaczego centralne zarządzanie bezpieczeństwem jest atrakcyjne?

WDRAŻANIE Z MYŚLĄ O ZASADACH

Ważna jest dobra technologia i dobry plan. Następnym krokiem jest wdrożenie kontroli i utrzymanie środków zaradczych przez cały okres ich użytkowania. Aby to osiągnąć, firmy polegają na tworzeniu, wdrażaniu i nadzorowaniu zasad.

Zasady

CZYM SĄ ZASADY?

Zasady to stwierdzenia, co należy zrobić w określonych okolicznościach. Na przykład polityka może wymagać dokładnego sprawdzenia przeszłości każdego nowego pracownika.

CO, NIE JAK

Zwróć uwagę, że zasady określają, co należy zrobić, a nie jak należy to zrobić. Z biegiem czasu wrażliwość na różne stanowiska w firmie będzie się zmieniać. Zmieni się również to, co stanowi dokładne sprawdzenie przeszłości. Polityki wyznaczają cele i wizję, ale nie ograniczają błędnie przyszłych zmian we wdrażaniu, gdy zmienią się warunki.

Polityki to stwierdzenia, co należy zrobić, a nie jak należy to zrobić.

PRZEJRZYSTOŚĆ

Skoncentrowanie się na tym, co należy zrobić, a nie na tym, jak należy to zrobić, nie oznacza, że zasady są nieistotne dla wdrażających. Wręcz przeciwnie, podejmując decyzje projektowe, wdrażający nieustannie zwracają się o wytyczne do polityk. Kontynuując nasz przykład, jeśli istnieją dwie alternatywy przeprowadzania kontroli przeszłości, wdrażający zadają sobie pytanie, czy odpowiadają one intencjom polityki. Koncentrując się na celach politycznych (a czasem na uzasadnieniach tych celów), polityki zapewniają jasność co do tego, co należy zrobić. Realizatorzy nie gubią się w szczegółach.

TEST XLV

a. Jakie są zasady?

b. Rozróżnij zasady i wdrażanie.

c. Dlaczego zasady nie powinny szczegółowo określać implementacji?

Kategorie polityk bezpieczeństwa

POLITYKA BEZPIECZEŃSTWA FIRMY

Firma potrzebuje kilku kategorii zasad bezpieczeństwa. Na górze znajduje się polityka bezpieczeństwa firmy. Jak właśnie zauważyliśmy, jego celem jest podkreślenie zaangażowania firmy w zapewnienie silnego bezpieczeństwa. To jest krótkie i na temat.

Celem korporacyjnej polityki bezpieczeństwa jest podkreślenie zaangażowania firmy w zapewnienie silnego bezpieczeństwa.

GŁÓWNE POLITYKI

W ramach krótkiej korporacyjnej polityki bezpieczeństwa firmy potrzebują konkretnych zasad dotyczących głównych problemów. Te główne zasady są znacznie bardziej szczegółowe niż korporacyjne zasady bezpieczeństwa.

• Zasady dotyczące poczty elektronicznej istnieją w prawie wszystkich firmach. Zasady dotyczące poczty e-mail określają, co personel IT powinien zrobić w przypadku problemów związanych z bezpieczeństwem poczty e-mail. Powinny również określać, co użytkownicy poczty e-mail powinni robić, a czego nie robić z pocztą e-mail.

• Zasady zatrudniania i wypowiadania są potrzebne, ponieważ zatrudnianie i wypowiedzenie to niebezpieczne okresy. Firma potrzebuje rygorystycznych zasad dotyczących sprawdzania przeszłości i innych spraw w momencie zatrudniania, a także zasad dotyczących wypowiedzeń dla różnych rodzajów wypowiedzeń (dobrowolne, zwolnienia, wypowiedzenie z przyczyn, itp.).

• Zasady dotyczące danych osobowych (PII) określają ochronę poufnych danych osobowych. Zasady te muszą określać kontrolę dostępu, szyfrowanie i inne kwestie, które mogą zmniejszyć ryzyko ujawnienia wrażliwych danych osobowych.

PRZYJĘTE ZASADY UŻYTKOWANIA

Nie można oczekiwać, że użytkownicy przeczytają wiele szczegółowych zasad. Dla użytkowników korporacje tworzą zasady dopuszczalnego użytkowania (AUP), które podsumowują kluczowe punkty o szczególnym znaczeniu dla użytkowników. Na przykład AUP zauważy, że (1) zasoby są własnością firmy i nie są przeznaczone do użytku osobistego, (2) nie powinno istnieć domniemane prawo do prywatności w przypadku poczty elektronicznej lub innych zastosowań oraz (3) określone typy zachowania nie będzie tolerowany. Zwykle firmy wymagają od użytkowników przeczytania i podpisania AUP. Zapewnia to ochronę prawną, dzięki czemu użytkownik nie może powiedzieć, że nigdy nie znał zasad firmy. Co równie ważne, podpisywanie stwarza poczucie ceremonii, która jest niezapomniana. Wymagane podpisywanie podkreśla również zaangażowanie firmy w bezpieczeństwo IT.

POLITYKI DOTYCZĄCE OKREŚLONYCH ŚRODKÓW PRZECIWŚRODKOWYCH LUB ZASOBÓW

Na najbardziej szczegółowym poziomie główne zasady nie są wystarczająco szczegółowe dla określonych środków zaradczych, takich jak pojedynczy firewall lub dla określonych zasobów, takich jak baza danych listy płac. Tę dodatkową specyfikę zapewniają środki zaradcze i zasady dotyczące zasobów. Ponownie, celem jest oddzielenie celów bezpieczeństwa od implementacji.

TEST XLVI

a. Rozróżnij korporacyjną politykę bezpieczeństwa i główne zasady bezpieczeństwa.

b. Rozróżnij główne zasady bezpieczeństwa i zasady dopuszczalnego użytkowania.

c. Jakie są cele wymagania od użytkowników podpisania umowy AUP?

d. Dlaczego potrzebne są zasady dotyczące indywidualnych środków zaradczych i zasobów?

Zespoły opracowujące zasady

Szerokie zasady nie mogą być opracowywane w odosobnieniu przez pracowników bezpieczeństwa IT. W przypadku każdej polisy firma powinna utworzyć zespół, który utworzy polisę. Chociaż bezpieczeństwo IT będzie ważnym członkiem zespołu, może nawet nie przewodniczyć zespołowi. Na przykład rozważ zasady zwalniania pracowników z powodu oszustwa lub kradzieży własności intelektualnej. Oczywiście w zespole powinien być dział prawny. Więc jeśli jakikolwiek dział, na który ma to wpływ, taki jak dział zasobów ludzkich, który musiałby wdrożyć tę politykę. Zasady opracowane przez zespół mają znacznie większe znaczenie dla pracowników niż zasady opracowane wyłącznie przez dział bezpieczeństwa IT. Są też bardziej skuteczne, ponieważ one nie są oparte na ograniczonym punkcie widzenia bezpieczeństwa IT.

TEST XLVII

Dlaczego ważne jest, aby zespoły korporacyjne tworzyły zasady?

Wskazówki dotyczące wdrażania

Chociaż polityki są i powinny być szerokimi deklaracjami wizji i celów. Firmy często opracowują wytyczne dotyczące wdrażania polityk. Wytyczne wdrożeniowe ograniczają swobodę realizatorów w celu uproszczenia decyzji wdrożeniowych, uniknięcia złych wyborów w interpretacji polityk i zapewnienia spójności we wdrażaniu.

Wytyczne wdrożeniowe ograniczają swobodę realizatorów w celu uproszczenia decyzji wdrożeniowych i uniknięcia złych wyborów w interpretacji polityk.

Wskazówki dotyczące wdrażania różnią się od polityki, której dotyczą. Polityka państwowa cele bezpieczeństwa i wizja napędzająca wdrażanie. Wskazówki wdrożeniowe w odpowiednim stopniu ograniczają wybór wdrożenia. Polityki rzadko się zmieniają. Wytyczne wdrożeniowe, choć ogólnie stabilne, prawdopodobnie będą się zmieniać szybciej niż polityki. Mamy teraz trzy poziomy. Zasady regulują co, a implementacja określa jak. W międzyczasie wytyczne dotyczące wdrażania stanowią opcjonalny pośredni etap kontroli.

BRAK WYTYCZNYCH

Jeśli firma może zaufać realizatorom, że będą działać mądrze, nie powinna tworzyć wskazówek dotyczących wdrażania. Brak wytycznych dotyczących implementacji zwalnia realizatorów z rozwijania tego, co uważają za najlepszą możliwą implementację polityki. Pozwala również uniknąć uczucia blokady. Często jest to dobry kompromis ze zwiększonym ryzykiem, jakie stwarza brak wskazówek dotyczących wdrożenia.

NORMY I WYTYCZNE

Powszechne jest dzielenie wskazówek dotyczących wdrażania na standardy i wytyczne. Normy są obowiązkowymi wytycznymi dotyczącymi wdrażania, co oznacza, że podlegający im pracownicy – w tym menedżerowie – nie mają możliwości ich nieprzestrzegania. Ważne jest, aby kontrolować przestrzeganie standardów. Dzięki obowiązkowemu charakterowi standardów, audytorzy powinni stosunkowo łatwo zdecydować, czy dany standard jest przestrzegany w konkretnej sytuacji. W przeciwieństwie do norm, które są obowiązkowe, wytyczne mają charakter uznaniowy. Na przykład, aby kontynuować wcześniejszy przykład, firma może mieć wskazówkę, że każdy nowy pracownik powinien mieć sprawdzenie przeszłości. Chociaż decydent jest zobowiązany do rozważenia wytycznych, nie jest obowiązkowe przestrzeganie wytycznych, jeśli istnieją uzasadnione powody, aby tego nie robić. Załóżmy na przykład, że wytyczne określają skanowanie odcisków palców w celu kontroli dostępu. Załóżmy dalej, że odciski palców robotnika budowlanego są zbyt zniszczone, by je odczytać. W takim przypadku osoba odpowiedzialna za uwierzytelnienie może zatwierdzić inny sposób uwierzytelnienia. Wytyczne są odpowiednie w złożonych i niepewnych sytuacjach, dla których nie można określić sztywnych norm.

TEST XLVIII

a. Rozróżnij normy i wytyczne.

b. Co jest obowiązkowe w przypadku wytycznych?

c. Kiedy wytyczne są odpowiednie?

Rodzaje wytycznych dotyczących wdrażania

Istnieje kilka rodzajów standardów i wytycznych dotyczących wdrażania polityk. Firmy powinny używać każdego z nich w odpowiedni sposób.

PROCEDURY

Na najbardziej szczegółowym poziomie procedury określają szczegółowe działania, jakie muszą podjąć poszczególni pracownicy. Słowo operacyjne jest tutaj szczegółowe. Na przykład w kinie jeden pracownik sprzedaje bilety, a drugi bierze bilet, aby wpuścić klienta do kina. Jeśli sprzedawca biletów również wpuścił klienta, sprzedawca biletów może zabrać pieniądze i wpuścić klienta bez dzwonienia do sprzedaży, a następnie zgarnąć pieniądze. Bilet należy wydrukować dopiero po odnotowaniu

sprzedaży. O ile nie ma zmowy między sprzedawcą biletu a przyjmującym bilet, ta procedura bezpieczeństwa jest skuteczna.

Procedury określają szczegółowe działania, które muszą podjąć poszczególni pracownicy.

Ten przykład teatralny ilustruje jedną z najważniejszych zasad projektowania procedur. W przypadku podziału obowiązków kompletny akt powinien wymagać wykonania przez dwie lub więcej osób. Uniemożliwia to jednej osobie działanie w pojedynkę, aby wyrządzić krzywdę. Jak zauważono w przykładzie, zmowa może pokonać podział obowiązków, ale przynajmniej podział obowiązków zmniejsza prawdopodobieństwo szkodliwego zachowania. Inny przykład podziału obowiązków pojawia się, gdy musi istnieć zezwolenie na coś, co jest potencjalnie ryzykowne. W takim przypadku ważne jest ograniczenie liczby osób, które mogą wystąpić o zatwierdzenie, a liczba osób zdolnych do autoryzacji wniosku musi być jeszcze mniejsza. Co najważniejsze, osoba autoryzująca wniosek nigdy nie może być tą samą osobą, która złożyła wniosek. Nazywa się to kontrolą żądania/autoryzacji. Powinny również istnieć zasady dotyczące urlopów i rotacji pracy. Jeśli ktoś wdraża niezatwierdzoną praktykę, często musi być stale obecny, aby to zadziałało. Urlopy powinny być obowiązkowe, aby stworzyć okres, w którym dana osoba nie może podjąć działań. Rotacja stanowisk, do innej roli lub obszaru odpowiedzialności, pełni tę samą funkcję, jeśli jest to możliwe. Obowiązkowe urlopy lub rotacje stanowisk również zmniejszają możliwość zmowy między pracownikami.

PROCESY

W przypadku pracy biurowej i innej ściśle określonej pracy odpowiednie mogą być procedury. Jednak w przypadku pracy kierowniczej i zawodowej wytyczne muszą być luźniejsze, ponieważ sytuacje zazwyczaj nie są tak proste i suche. Jednak nawet w przypadku pracy menedżerskiej i zawodowej firmy kierują się procesami, które są wysokopoziomowymi opisami tego, co należy zrobić. Na przykład rozwój nowych produktów wymaga szerokiego procesu, aby dobrze funkcjonować. Proces określałby, w jaki sposób nominować nowe pomysły na produkty, kto powinien przeprowadzić wstępną analizę wykonalności, a kto powinien otrzymać obiecujące nowe produkty różnych typów. W pracy menedżerskiej i zawodowej rzadko udaje się zredukować każdy etap procesu – w tym analizę wykonalności – do procedur niskopoziomowych. Jednak procesy muszą być wystarczająco jasne, aby zmniejszyć ryzyko. Procesy to szerokie opisy tego, co należy zrobić.

LINIE BAZOWE

Procedury i procesy opisują etapy wdrażania. W przeciwieństwie do tego, linie bazowe są jak listy kontrolne samolotów. Linie bazowe opisują szczegóły tego, co należy osiągnąć, nie opisując szczegółowo, jak to zrobić. Na przykład, jeśli administrator systemu musi zabezpieczyć serwer WWW przed zagrożeniami, zwróci się do korporacyjnej linii bazowej, która określa takie rzeczy, jak stosowanie silnych haseł w celu zastąpienia określonych haseł domyślnych. Linia bazowa nie opisuje jednak, jak to zrobić, jak to miało miejsce w przypadku procedury lub procesu.

Linie bazowe opisują szczegóły tego, co należy osiągnąć, nie opisując szczegółowo, jak to zrobić.

Linie bazowe muszą być dostosowane do konkretnych sytuacji. Na przykład firma potrzebowałaby różnych linii bazowych do wzmocnienia systemu Windows Server 2003, Windows Server 2008, Red Hat LINUX i tak dalej. Bez linii bazowych administrator systemu może łatwo zapomnieć o zmianie określonego hasła domyślnego lub włączeniu rejestrowania zdarzeń.

NAJLEPSZE PRAKTYKI I ZALECANE PRAKTYKI

Chociaż firmy ciężko pracują nad swoją polityką i wskazówkami wdrożeniowymi, często chcą wyjść poza siebie. Najlepsze praktyki to opisy tego, co najlepsze firmy w branży robią w zakresie bezpieczeństwa. Najlepsze praktyki są zwykle opracowywane przez firmy konsultingowe, ale stowarzyszenia handlowe, a nawet rządy zaczynają je opracowywać.

Najlepsze praktyki to opisy tego, co najlepsze firmy w branży robią w zakresie bezpieczeństwa.

Najlepsze praktyki różnią się od zalecanych praktyk, które stanowią nakazowe stwierdzenia dotyczące tego, co firmy powinny robić. Zalecane praktyki są zwykle opracowywane przez stowarzyszenia branżowe i agencje rządowe. Być może najbardziej znanym zestawem zalecanych praktyk jest rodzina norm ISO 27000 omówiona później.

Zalecane praktyki to nakazowe stwierdzenia dotyczące tego, co firmy powinny robić.

ODPOWIEDZIALNOŚĆ

Ostateczną kontrolą, która w przybliżeniu mieści się w obszarze wytycznych wdrożeniowych, jest przypisanie odpowiedzialności, co oznacza, że odpowiedzialność za sankcje związane z wdrożeniem nie jest wykonywana prawidłowo. Właścicielem każdego zasobu i kontroli powinna być jedna osoba. Jeśli coś pójdzie nie tak, właściciel zostanie pociągnięty do odpowiedzialności. Jeśli dana osoba wie, że zostanie pociągnięta do odpowiedzialności, jest to silna zachęta do wiernego wdrażania polityki. Często właściciel deleguje zadanie wdrożenia polityki komuś innemu, powiernikowi. Zazwyczaj powiernik ma więcej umiejętności technicznych lub lepiej rozumie szczegółową sytuację niż właściciel. Jednak o ile prace nad wdrożeniem można delegować na powiernika, odpowiedzialności nie można delegować.

ETYKA

W skomplikowanych sytuacjach twarde i szybkie prowadzenie jest niemożliwe. Decyzje muszą być podejmowane na podstawie etyki, która jest systemem wartości danej osoby. Trudną częścią etycznego podejmowania decyzji jest to, że jednostki mogą mieć różne systemy wartości. W konsekwencji różni ludzie dobrej woli mogą podejmować różne decyzje etyczne w tej samej sytuacji. Aby podejmowanie etycznych decyzji było bardziej przewidywalne, większość korporacji posiada kodeksy etyczne, które zawierają pewne konkretne wytyczne. Te kodeksy etyczne zawierają zwykle stwierdzenia dotyczące następujących kwestii (między innymi):

• Kodeks etyki obowiązuje wszystkich, w tym pracowników zatrudnionych w niepełnym wymiarze godzin i kadrę kierowniczą wyższego szczebla. (W rzeczywistości większość firm ma dodatkowe kodeksy etyczne dla zarządów i urzędników korporacyjnych.)

• Zachowanie etyczne nie jest opcjonalne; niewłaściwe zachowanie etyczne może prowadzić do rozwiązania umowy lub mniejszej dyscypliny.

• Jeśli pracownik zauważy nieetyczne zachowanie, musi zgłosić to korporacyjnemu dyrektorowi ds. etyki lub komitetowi audytu firmy.

• Pracownik musi unikać konfliktów interesów, co oznacza, że nigdy nie może wykorzystywać swojej pozycji dla osobistych korzyści. Obejmuje to preferencyjne kontakty z krewnymi, inwestowanie w konkurencję i konkurowanie z firmą, gdy nadal jest przez nią zatrudniony.

• Pracownikowi nie wolno brać łapówek ani nielegalnych prowizji, w tym wszelkich nietrywialnych „prezentów". Łapówki to prezenty pieniężne mające na celu nakłonienie pracownika do faworyzowania dostawcy lub innej strony. Prowizja to w szczególności płatność dokonywana przez dostawcę na rzecz kupującego korporacyjnego po dokonaniu zakupu.

• Pracownicy muszą wykorzystywać aktywa biznesowe wyłącznie do celów biznesowych, a nie do użytku osobistego.

• Pracownikowi nie wolno nigdy ujawniać informacji poufnych, prywatnych ani tajemnic handlowych.

TEST XLIX

a. Rozróżnij procedury i procesy

b. Kiedy będą używane?

c. Czym jest podział obowiązków i jaki jest jego cel?

d. Kiedy ktoś prosi o podjęcie działania, które jest potencjalnie niebezpieczne, jakie zabezpieczenia należy zastosować?

e. Dlaczego tak ważne jest egzekwowanie obowiązkowych urlopów lub rotacji pracy?

f. Czym różnią się wytyczne od procedur i procesów?

g. Rozróżnij najlepsze praktyki i zalecane praktyki.

h. Rozróżnij właścicieli zasobów i powierników pod względem odpowiedzialności.

i. Co właściciel może przekazać powiernikowi?

j. Czego właściciel nie może przekazać powiernikowi?

a. Dlaczego etyka jest nieprzewidywalna?

b. Dlaczego firmy tworzą kodeksy etyczne?

c. Dlaczego dobra etyka jest ważna w firmie?

d. Kogo obowiązują kodeksy etyczne?

e. Czy wyżsi funkcjonariusze często otrzymują dodatkowy kodeks etyczny?

f. Jeśli pracownik ma wątpliwości etyczne, co musi zrobić?

g. Co musi zrobić pracownik, jeśli zauważy nieetyczne zachowanie?

h. Jakie zostały podane przykłady konfliktów interesów?

i. Dlaczego łapówki i prowizje są złe?

j. Rozróżnij łapówki i prowizje.

k. Jakich informacji pracownik nie powinien ujawniać?

Obsługa wyjątków

Byłoby dobrze, gdyby implementacja nigdy nie wymagała wyjątków od polityk lub wskazówek dotyczących implementacji, ale czasami wyjątki są konieczne. Wymaga to specyfikacji wskazówek dotyczących implementacji, aby zawierały wskazówki dotyczące obsługi wyjątków. Wytyczne mają kluczowe znaczenie, ponieważ wyjątki są niebezpieczne, więc muszą być ściśle kontrolowane i udokumentowane. Poniżej znajdują się ogólne wskazówki dotyczące obsługi wyjątków.

• Tylko niektóre osoby powinny mieć prawo prosić o wyjątki.

• Jeszcze mniej osób powinno mieć możliwość autoryzacji wyjątków.

• Osoba, która wnioskuje o wyjątek, nigdy nie może być tą samą osobą, która autoryzuje wyjątek.

• Każdy wyjątek musi być dokładnie udokumentowany pod kątem tego, co zostało zrobione i kto wykonał każde działanie.

• Szczególną uwagę należy zwrócić na wyjątki w okresowych audytach.

• Na wyjątki powyżej określonego poziomu zagrożenia należy zwrócić uwagę działu bezpieczeństwa IT i bezpośredniego przełożonego autoryzującego.

TEST L

a. Dlaczego wyjątki nie powinny być absolutnie zabronione?

b. Dlaczego potrzebne są wskazówki dotyczące implementacji obsługi wyjątków?

c. Jakie są pierwsze trzy zasady dotyczące wyjątków?

d. Dlaczego dokumentacja i okresowe audyty byłyby ważne?

e. Jaki jest przykład niebezpiecznego wyjątku, który należy zgłosić kierownikowi?

Przeoczenie

Idealnie, polityki byłyby wdrażane wiernie pod ograniczeniami odpowiednich wytycznych wdrożeniowych. Niestety nie zawsze tak jest. Pod koniec 2007 roku Instytut Ponemon przeprowadził ankietę wśród 890 specjalistów IT. Ponad połowa stwierdziła, że osobiście skopiowała dane osobowe na pamięć USB, chociaż 87 procent przyznało, że zna zasady zakazujące im tego. Raport był wypełniony podobnymi przyznaniami się do naruszeń zasad przez tych specjalistów IT. Ponadto wiele osób zgłosiło, że ich firmy nie posiadały zasad dotyczących niektórych wrażliwych kwestii związanych z bezpieczeństwem IT – lub przynajmniej stwierdziło, że nie znają takich zasad. Dlaczego te naruszenia były tak powszechne? Respondenci przypisywali swoje naruszenia bezpieczeństwa wygodzie i brakowi egzekwowania zasad. Nadzór to proces, funkcja lub grupa narzędzi, które służą do usprawnienia wdrażania i egzekwowania zasad. Istnieje wiele rodzajów nadzoru.

Nadzór to proces, funkcja lub grupa narzędzi, które służą do usprawnienia wdrażania i egzekwowania zasad.

POLITYKI I NADZÓR

Polityka i nadzór są ze sobą powiązane. Tak jak polityka napędza wdrożenie, ta sama polityka napędza nadzór. Pracownicy zaangażowani w nadzór muszą opracować plany nadzoru odpowiednie dla określonej polityki.

OPUBLIKOWANIE

Pierwszym zadaniem zarządzania bezpieczeństwem po utworzeniu polityk jest uświadomienie ich użytkownikom. Formalne ogłaszanie, publikowanie lub informowanie użytkowników o nowej polityce nazywa się promulgacją. Jeśli użytkownicy nie znają lub nie rozumieją zasad, nie mogą ich przestrzegać. Ważne jest, aby aktywnie wprowadzać politykę na rynek i podkreślać wizję poszczególnych polityk. Potrzebę promulgacji do najniższych dotkniętych poziomów w organizacji zilustrowano przykładem tego, co się dzieje, gdy nie jest to zrobione. W latach 70. młody podporucznik piechoty morskiej został

wysadzony na brzeg ze swoim plutonem w pewnym kraju. Powiedziano mu, że trwa rewolucja, ale niewiele więcej. Niemal natychmiast jego pluton został ostrzelany z obu stron. Nagle przyszło mu do głowy, że nie powiedziano mu, po której stronie ma stanąć. Jak wspomniano wcześniej, przydatne jest, aby użytkownicy, których dotyczy problem, podpisywali polityki. Daje to poczucie bezpieczeństwa, które zwiększa świadomość. Jednym z kontrowersyjnych sposobów nagłaśniania polityki jest prowadzenie żądło pracowników. W takich przypadkach pracownicy są proszeni o zrobienie czegoś wbrew polityce. Na przykład stan Karolina Południowa wysłał e-maile phishingowe do 100 pracowników stanowych. W ciągu 20 minut 30 odpowiedziało. Wynik ten został szeroko nagłośniony w stanowym biuletynie pracowniczym. Prowadzenie użądleń jest dobre dla podniesienia świadomości. Użądlenia mogą być również użyte jako sztuczka w celu zwiększenia środków na szkolenia w zakresie świadomości bezpieczeństwa IT. Jeśli określone użądlenia powtarzane są corocznie, można je również wykorzystać do wskazania pozytywnych trendów. Użądlenia są kontrowersyjne, ponieważ wywołają urazę, jeśli nie zostaną odpowiednio potraktowane. Aby uniknąć problemów, nigdy nie należy ujawniać tożsamości urażonych pracowników. Ponadto powinny być używane wyłącznie jako sytuacje dydaktyczne, a nigdy jako kary.

MONITOROWANIE ELEKTRONICZNE

W wielu przypadkach możliwe jest automatyczne elektroniczne monitorowanie zachowania zgodności. Na przykład w 2007 roku badanie American Management Association wykazało, że 66 procent ankietowanych firm stwierdziło, że monitoruje połączenia internetowe. Ponadto ponad połowa stwierdziła, że zwolniła pracowników za nadużycie poczty elektronicznej lub inne nadużycia w sieci. Jeśli firma zamierza korzystać z monitoringu elektronicznego, ważne jest, aby poinformować o tym pracowników z wyprzedzeniem i wyjaśnić, dlaczego to robi.

MIERNIKI BEZPIECZEŃSTWA

Monitoring podaje szczegóły. Innym sposobem mierzenia zgodności jest tworzenie metryk bezpieczeństwa, które są kilkoma dobrze dobranymi, mierzalnymi wskaźnikami sukcesu lub niepowodzenia zabezpieczeń, które są mierzone okresowo. Przykłady obejmują odsetek komputerów użytkowników pozostawionych w nocy, odsetek możliwych do złamania haseł na serwerze oraz odsetek krytycznych poprawek zastosowanych na serwerach internetowych. Okresowe mierzenie tych wskaźników wskazuje, czy firma radzi sobie lepiej, czy gorzej we wdrażaniu swoich zasad.

Metryki bezpieczeństwa są mierzalnymi wskaźnikami powodzenia lub niepowodzenia bezpieczeństwa.

AUDYT

Wszystkie spółki notowane na giełdzie muszą poddać się badaniu sprawozdań finansowych. Firmy audytorskie nie analizują wszystkich informacji, które znajdują się w sprawozdaniach finansowych. Raczej celowo próbkują określone fragmenty danych finansowych. Na podstawie wyrywkowych danych wypracowują opinię na temat kontroli procesu sprawozdawczości finansowej. Celem audytu jest opracowanie opinii na temat stanu kontroli, a nie wykrycie karalnych przypadków niezgodności.

Celem audytu jest opracowanie opinii na temat stanu kontroli, a nie wykrycie karalnych przypadków niezgodności.

Audyt jest możliwy tylko wtedy, gdy informacje są rejestrowane. W związku z tym większość przepisów i regulacji dotyczących zgodności wymaga obszernego rejestrowania informacji. Jeśli informacje są zapisane w bazie danych, nazywane są informacjami rejestrowanymi. Jeżeli informacje są zapisane na formularzach lub notatkach, nazywa się je dokumentacją. Audyt pobiera próbkę zarejestrowanych i udokumentowanych informacji. W niektórych przypadkach audyt będzie mierzył, ile razy wystąpiły

niezgodności, na przykład, czy wyjątek nie został autoryzowany. W innych przypadkach audytor opracowuje wskaźniki, takie jak odsetek działań w określonej kategorii, które naruszały zasady. Jedną z kluczowych zasad jest staranne mierzenie zdarzeń niezgodności, ale intensywne koncentrowanie się na każdym przypadku, w którym występuje aktywne unikanie zgodności. Unikanie zgodności wskazuje na celowe obchodzenie zabezpieczeń i zawsze wymaga przeprowadzenia dochodzenia. Audyty wewnętrzne są wykonywane przez samą organizację. Audyty zewnętrzne są wykonywane przez firmę zewnętrzną. W audycie finansowym firmy są zobowiązane do przeprowadzania zarówno audytu wewnętrznego, jak i zewnętrznego. To samo jest wskazane w przypadku audytu bezpieczeństwa IT. Audyty należy planować wystarczająco często, aby ostrzec o rosnących zagrożeniach. Wiele firm przeprowadza kwartalne audyty bezpieczeństwa IT, a bardziej rygorystyczne audyty odbywają się raz w roku. Regularnie rozmieszczone audyty są atrakcyjne, ponieważ pozwalają firmie porównywać wyniki w czasie. Jednak regularnie zaplanowane audyty mogą działać na korzyść osób, które unikają bezpieczeństwa. Dlatego też pożądane są również nieplanowane audyty.

ANONIMOWA ZABEZPIECZONA INFOLINIA

Firmy od dawna wiedzą, że najlepszym sposobem wykrywania oszustw i innych poważnych nadużyć jest stworzenie anonimowej, chronionej infolinii. Często to współpracownik jako pierwszy odkrywa naruszenie bezpieczeństwa. Na przykład po huraganie Katrina 22 osoby pracujące dla wykonawcy Czerwonego Krzyża w Bakersfield zostały oskarżone o składanie fałszywych roszczeń. Skorzystali ze słabych kontroli, które miały miejsce ze względu na pilną potrzebę udzielenia pomocy ludziom. Zostali złapani tylko wtedy, gdy menedżer Western Union zobaczył, jak ta sama osoba trzy razy przychodziła po pieniądze. Zamówiła urzędy, a to złamało oszustwo. Pracownicy, którzy widzą niewłaściwe zachowanie, mogą niechętnie mówić z obawy przed odwetem. Za pomocą posiadania anonimowej infolinii, do której można dzwonić, oraz zagwarantowanie ochrony przed represjami, firmy mogą zmaksymalizować udział pracowników. Niektóre firmy wymagają nawet od pracowników, którzy wykryją poważne uchybienia, korzystania z infolinii. Wszystkie spółki notowane na giełdzie muszą mieć gorącą linię dla zgodności Sarbanes-Oxley. Mogą poszerzyć jego zakres, aby uwzględnić wszystkie poważne zachowania. Jedną z opcji jest oferowanie zapłaty za informacje jako zachętę. Jest to wbudowane w szereg przepisów dotyczących zgodności, w tym HIPAA. Niewiele firm oferuje płatności, ale rozsądne może być zrobienie tego, jeśli istnieje ryzyko dużych oszustw i innych bardzo szkodliwych działań.

ŚWIADOMOŚĆ BEHAWIORALNA

Jedną z kontroli nadzorczych jest bycie świadomym ludzkiego zachowania. Wszelkie poważne nadużycia pracowników powinny być traktowane jako sygnał ostrzegawczy, ponieważ w wielu przypadkach poważnych naruszeń bezpieczeństwa sprawca miał w przeszłości przemoc, groźby lub inne niedopuszczalne jawne zachowania. Nie zwracanie uwagi na takie zachowania jest poważnym zaniedbaniem.

OSZUSTWO

W przypadku oszustw pisarze od dawna dyskutują o trójkącie oszustw, który służy do zrozumienia nieuczciwych zachowań. Wydaje się, że ma to również zastosowanie do ogólnych niewłaściwych zachowań w zakresie bezpieczeństwa. W związku z tym będziemy go nazywać trójkątem oszustw i nadużyć. Trójkąt uwzględnia trzy aspekty ludzkiej motywacji, które zwykle występują przed wystąpieniem niewłaściwego zachowania. Będąc wrażliwym na te aspekty motywacji, firma może być w stanie wykryć problem, zanim się pojawi, lub przynajmniej mieć realistyczne zrozumienie, dlaczego robią to osoby nadużywające bezpieczeństwa.

Możliwość. Pierwszy wierzchołek trójkąta to okazja. Oczywiście, jeśli istnieje niewielka możliwość popełnienia nadużycia lub jeśli sprawca prawdopodobnie zostanie złapany, nadużycie raczej nie nastąpi. Ograniczenie szans na sukces i zwiększenie wykrywalności to normalne drogi do osiągnięcia bezpieczeństwa.

Nacisk. Równie ważna jest jednak psychologia sprawcy. Oczywiście niewiele osób, które mają okazję popełnić poważne nadużycia w zakresie bezpieczeństwa, faktycznie to robi. Szansa to za mało. Kolejnym czynnikiem jest presja. Ta presja popycha osobę do popełnienia nadużycia. Przykładami presji są m.in. osobiste problemy finansowe, chciwość lub chęć ukrycia słabych wyników, które zagrażałyby pracy pracownika. Być może najczęstszą formą presji są nieuzasadnione oczekiwania dotyczące wydajności.

Racjonalizacja. Nawet pod presją i możliwościami pracownicy prawdopodobnie nie będą działać, jeśli nie potrafią zracjonalizować swoich działań we własnych głowach. Na przykład mogą wmawiać sobie, że czyn jest uzasadniony, ponieważ firma ma nierealistyczne oczekiwania dotyczące wydajności lub że zwrócą zdefraudowane pieniądze. Celem racjonalizacji jest umożliwienie sprawcom myślenia o sobie jako o dobrych ludziach. Firmy i menedżerowie muszą się nauczyć, że nadmierne oczekiwania dotyczące wydajności mogą przynieść odwrotny skutek, ułatwiając racjonalizację. Ważne jest, aby nie lekceważyć racjonalizacji lub odrzucać możliwości ataków dobrych ludzi.

Testy podatności. Jednym ze sposobów sprawdzenia, czy polityka bezpieczeństwa jest skuteczna, jest samodzielne zaatakowanie systemu w celu sprawdzenia, czy uda Ci się znaleźć luki, zanim zrobią to atakujący. Nazywa się to testowaniem podatności.

Testowanie luk polega na samodzielnym atakowaniu systemu w celu sprawdzenia, czy uda się znaleźć luki, zanim zrobią to atakujący.

Istnieje wiele programów do testowania podatności. Oprogramowanie hakerskie jest zwykle dostępne za darmo, podczas gdy komercyjne programy testujące luki w zabezpieczeniach są mniej podatne na wyrządzanie szkód jako efekt uboczny. Wewnętrzne testy podatności. Jeśli testy podatności mają być wykonywane wewnętrznie, pracownik wykonujący test podatności powinien nalegać na podpisanie umowy upoważniającej do przeprowadzenia testu podatności od swojego przełożonego. Testy podatności wyglądają dokładnie tak, jak rzeczywiste ataki. Przeprowadzenie testu podatności bez podpisanej umowy, nawet jeśli testowanie podatności znajduje się na liście pisemnych obowiązków danej osoby, może łatwo doprowadzić do zwolnienia specjalisty ds. bezpieczeństwa IT lub gorzej. Zewnętrzne testy podatności. Umowa na testowanie podatności powinna szczegółowo określać, co zostanie zrobione i kiedy. Podczas testu nie powinno być żadnych odchyleń od umowy. Ponadto testy podatności czasami powodują awarię systemów lub powodują inne szkody. Umowa musi uniewinniać wewnętrznego testera podatności, jeśli takie uszkodzenie wystąpi. Zewnętrzne firmy testujące podatności zapewniają większą niezależność oraz prawdopodobnie większą wiedzę i doświadczenie. Ważne są również konkretne plany testów, a firma testująca powinna mieć ubezpieczenie od ewentualnych uszkodzeń. Co najważniejsze, firma testująca nie powinna zatrudniać obecnych lub byłych hakerów, ponieważ testerzy zdobędą bardzo szczegółową wiedzę na temat Twoich systemów. Po badaniu testów podatności tester powinien stworzyć konkretną listę zalecanych poprawek, którą powinien podpisać przełożony testera. Powinna również nastąpić późniejsza obserwacja, aby potwierdzić, że poprawki zostały wprowadzone.

SANKCJE

Jest stare powiedzenie o sankcjach - dostajesz to, co egzekwujesz. Jeśli pracownicy łamią protokoły bezpieczeństwa, powinni zostać odpowiednio ukarani (zdyscyplinowani). Jeśli tak się nie stanie, szybko

staje się powszechnie znany brak intencji firmy w zakresie monitorowania bezpieczeństwa. Często firmy bardzo niechętnie nakładają sankcje na personel wyższego szczebla. W jednym przypadku stażysta Departamentu Usług Administracyjnych Ohio zabrał do domu urządzenie taśmowe z taśmą do tworzenia kopii zapasowych. Ten stażysta za 10 dolarów za godzinę otrzymał polecenie od bardziej doświadczonego stażysty. Przełożony nigdy nie omawiał procedur bezpiecznego przechowywania taśm z kopiami zapasowymi na noc. Pewnego razu włamano się do samochodu stażysty i skradziono urządzenie. Taśma zawierała dane wszystkich 64 467 pracowników stanu, 19 388 byłych pracowników i 47 245 podatników Ohio. Oczekiwano, że naruszenie danych będzie kosztować stan ponad 3 miliony dolarów. Stażystę surowo przesłuchano i zmuszono do rezygnacji. Jego przełożony otrzymał znacznie mniejszą sankcję – jeden tydzień straconego urlopu.

TEST LI

a. Co to jest nadzór?

b. Jak nadzór jest powiązany z polityką?

c. Co to jest promulgacja?

d. Czym są kłujący pracownicy?

e. Jakie są jego koszty i korzyści?

f. Czy monitoring elektroniczny jest szeroko stosowany?

g. Co powinieneś powiedzieć pracownikom przed rozpoczęciem monitorowania?

h. Czym są metryki bezpieczeństwa?

RAMY ZARZĄDZANIA

Wcześniej widzieliśmy wytyczne, które są listami kontrolnymi do wdrażania polityki. Wiele firm zmagających się z planowaniem bezpieczeństwa chciałoby czegoś takiego jak punkt odniesienia, który by nimi kierował. W rzeczywistości, Rysunek 2-25 pokazuje, że istnieje kilka struktur zarządzania, które określają sposób planowania i wdrażania zabezpieczeń. Jednak fakt, że istnieje kilka, oznacza dokonanie wyboru jednej lub większej liczby ram zarządzania w celu podjęcia złożonej decyzji. Te ramy zarządzania koncentrują się na nieco innych obszarach. Na przykład COSO koncentruje się w dużej mierze na korporacyjnych kontrolach wewnętrznych i finansowych, podczas gdy CobiT koncentruje się bardziej konkretnie na kontrolowaniu całej funkcji IT. Rodzina norm ISO/IEC 27000 dotyczy w szczególności bezpieczeństwa IT.

Ramy zarządzania określają sposób planowania i wdrażania zabezpieczeń.

TEST LII

a. Czym są ramy zarządzania?

b. Porównaj koncentrację COSO z koncentracją CobiT.

c. Porównaj koncentrację CobiT z serią norm ISO/IEC 27000.

d. Dlaczego pomiary okresowe są korzystne?

a. Jaki jest cel audytu?

b. Rozróżnij pliki dziennika i dokumentację.

c. Dlaczego unikanie zgodności jest poważnym sygnałem ostrzegawczym?

d. Rozróżnij audyt wewnętrzny i zewnętrzny.

e. Dlaczego regularnie zaplanowane audyty są dobre?

f. Dlaczego przeprowadzane są nieplanowane audyty?

a. Dlaczego firmy powinny instalować anonimowe chronione infolinie?

b. Dlaczego anonimowość i ochrona przed represjami są ważne w przypadku korzystania z infolinii?

c. Dlaczego ogólne złe zachowanie pracowników powinno być problemem?

d. Jakie są trzy elementy trójkąta oszustwa i nadużycia?

e. Podaj przykład nacisku, który nie został omówiony w tekście.

f. Dlaczego racjonalizacje są ważne?

g. Podaj dwa przykłady racjonalizacji nie podane w tekście.

a. Co to jest test podatności?

b. Dlaczego nigdy nie powinieneś angażować się w test podatności bez podpisanej umowy?

c. Co powinno znaleźć się w umowie?

d. Czego należy szukać w zewnętrznej firmie testującej podatności?

e. Dlaczego potrzebne są dalsze działania dotyczące zalecanych poprawek?

Dlaczego ważne jest nakładanie sankcji na osoby naruszające przepisy?

COSO

Implementacja Sarbanes-Oxley wyraźnie wymaga od korporacji korzystania z dobrze opracowanego, kompleksowego systemu kontroli. Chociaż to wymaganie dotyczące implementacji nie nakazuje korporacjom korzystania z określonego frameworka, wyszczególniono tylko jeden framework jako akceptowalny, a większość firm używa tego frameworka do implementacji Sarbanes-Oxley. To są ramy COSO.

RAMY COSO

Chociaż COSO jest powszechnie znany pod swoim akronimem, struktura COSO jest w rzeczywistości dokumentem o nazwie Internal Control-Internal Framework (COSO, 1994). Skrót COSO pochodzi od organizacji, która stworzyła dokument, Komitetu Organizacji Sponsorujących Komisji Treadway (http://www.coso.org). W 2004 r. COSO wydało nową, rozszerzoną strukturę, Enterprise Risk Management-Integrated Framework, która koncentruje się bardziej na zarządzaniu ryzykiem korporacyjnym.

CELE

Ramy kontroli wymagają celów. W ramach COSO istnieją cztery cele.

• Strategiczne - cele wysokiego poziomu, zgodne z misją i wspierające tę misję

• Operacje - efektywne i wydajne wykorzystanie jej zasobów

• Raportowanie – wiarygodność raportowania

• Zgodność - zgodność z obowiązującymi przepisami i regulacjami

ROZSĄDNE ZABEZPIECZENIE

Dobre kontrole nie mogą całkowicie zagwarantować, że cele zostaną osiągnięte. Jednak efektywne środowisko kontroli da wystarczającą pewność, że cele zostaną osiągnięte.

KOMPONENTY RAMOWE COSO

Ramy COSO składają się z ośmiu komponentów. Są to raczej komponenty niż fazy, ponieważ nie ma między nimi porządkowania czasowego. Wszystko musi zachodzić jednocześnie, a każde nieustannie karmi się innymi.

• Środowisko wewnętrzne - środowisko wewnętrzne obejmuje ton organizacji i stanowi podstawę postrzegania ryzyka i zajmowania się nim przez pracowników jednostki, w tym filozofię zarządzania ryzykiem i apetyt na ryzyko, uczciwość i wartości etyczne oraz środowisko, w którym działają .

• Wyznaczanie celów - cele muszą istnieć, zanim kierownictwo będzie mogło zidentyfikować potencjalne zdarzenia mające wpływ na ich osiągnięcie. Zarządzanie ryzykiem korporacyjnym zapewnia, że kierownictwo wdrożyło proces ustalania celów, a wybrane cele wspierają i są zgodne z misją jednostki oraz są spójne z jej apetytem na ryzyko.

• Identyfikacja zdarzeń - wewnętrzne i zewnętrzne zdarzenia mające wpływ na osiągnięcie celów jednostki muszą być zidentyfikowane, z rozróżnieniem między ryzykami a szansami. Szanse są kierowane z powrotem do strategii kierownictwa lub procesów ustalania celów.

• Ocena ryzyka – ryzyko jest analizowane z uwzględnieniem prawdopodobieństwa i wpływu, jako podstawy do określenia, w jaki sposób należy nimi zarządzać. Ryzyka są oceniane na zasadzie nieodłącznej i rezydualnej.

• Reakcja na ryzyko - Kierownictwo wybiera reakcje na ryzyko - unikanie, akceptowanie, ograniczanie lub dzielenie ryzyka - opracowując zestaw działań w celu dostosowania ryzyka do tolerancji na ryzyko i apetytu na ryzyko jednostki.

• Czynności kontrolne - Zasady i procedury są ustanawiane i wdrażane w celu zapewnienia skutecznej realizacji reakcji na ryzyko.

• Informacja i komunikacja - istotne informacje są identyfikowane, przechwytywane i przekazywane w formie i ramach czasowych, które umożliwiają ludziom wykonywanie ich obowiązków. Skuteczna komunikacja występuje również w szerszym sensie, spływając w dół, w poprzek i w górę całości.

• Monitorowanie - Całość zarządzania ryzykiem korporacyjnym jest monitorowana iw razie potrzeby wprowadzane są modyfikacje. Monitorowanie odbywa się poprzez bieżące działania zarządcze, oddzielne oceny lub jedno i drugie.

TEST LIII

a. Jakie są cztery cele COSO?

b. Wymień osiem komponentów COSO.

c. Czym jest czynność kontrolna i dlaczego jest ważna?

CobiT

COSO to ogólne narzędzie do planowania i oceny kontroli dla korporacji. W przypadku kontroli IT istnieje bardziej szczegółowe ramy, CobiT (Cele kontroli w zakresie informacji i technologii pokrewnych). Oprócz stworzenia szerokich ram celów kontrolnych, IT Governance Institute opracował również szczegółowe wytyczne dotyczące wdrażania ram CobiT. Rysunek 2-28 ilustruje strukturę CobiT. Ramy te składają się z czterech głównych domen, które podążają za ogólnym cyklem rozwoju systemów:

• Planuj i organizuj - domena planowania i organizowania obejmuje 10 celów kontroli wysokiego poziomu, które obejmują wszystko, od strategicznego planowania IT i tworzenia korporacyjnej architektury informacji po zarządzanie określonymi projektami.

• Zakup i wdrożenie - po zaplanowaniu firmy muszą nabyć i wdrożyć systemy informatyczne. Ta domena ma siedem celów kontroli wysokiego poziomu.

• Dostarczanie i wsparcie - większość życia projektu IT ma miejsce po jego wdrożeniu. W związku z tym struktura CobiT ma 13 celów kontroli wysokiego poziomu w zakresie realizacji i wsparcia. To więcej niż jakakolwiek inna domena.

• Monitoruj i oceniaj - wreszcie firmy muszą monitorować swoje procesy, oceniać adekwatność kontroli wewnętrznych, uzyskiwać niezależną pewność i zapewniać niezależne audyty. Są to cztery cele kontrolne.

Poniżej czterech głównych domen CobiT znajdują się 34 cele kontroli wysokiego poziomu. Poniżej znajduje się ponad 300 szczegółowych celów kontrolnych. CobiT zawiera również wiele dokumentów, które pomagają organizacjom zrozumieć, jak wdrożyć ramy.

DOMINACJA W STANACH ZJEDNOCZONYCH

IT Governance Institute został utworzony przez Stowarzyszenie Audytu i Kontroli Systemów Informacyjnych (ISACA). Z kolei ISACA jest głównym stowarzyszeniem zawodowym zrzeszającym specjalistów audytu IT w Stanach Zjednoczonych. Certyfikacja certyfikowanego audytora systemów informatycznych Stowarzyszenia (CISA) jest dominującą certyfikacją dla amerykańskich audytorów IT, nic więc dziwnego, że CobiT stał się dominującą strukturą audytu kontroli IT w Stanach Zjednoczonych.

TEST LIV

a. Rozróżnij obszary zainteresowania COSO i CobiT.

b. Wymień cztery domeny CobiT.

c. Ile celów kontroli wysokiego poziomu ma CobiT?

d. Która domena ma najwięcej celów kontrolnych?

e. Ile szczegółowych celów kontrolnych ma CobiT?

f. Dlaczego CobiT jest zdecydowanie preferowany przez amerykańskich audytorów IT?

Rodzina ISO/IEC 27000

Podczas gdy CobiT koncentruje się na zarządzaniu funkcjami IT w szerokim zakresie, rodzina norm ISO/IEC 27000 koncentruje się szczególnie i szczegółowo na bezpieczeństwie IT.

ISO/IEC 27002

Pierwszy standard z tej serii nosił początkowo nazwę ISO/IEC 17799. Kiedy zdecydowano, że wszystkie standardy bezpieczeństwa zaczynają się od 27000, zmieniono jego nazwę na ISO/IEC 27002. Norma ta dzieli bezpieczeństwo na 11 szerokich obszarów, które są podzielone na wiele bardziej szczegółowe elementy:

• Polityka bezpieczeństwa

• Organizacja bezpieczeństwa informacji

• Zarządzanie aktywami

• Bezpieczeństwo zasobów ludzkich

• Bezpieczeństwo fizyczne i środowiskowe

• Zarządzanie komunikacją i operacjami

• Kontrola dostępu

• Pozyskiwanie, rozwój i utrzymanie systemów informatycznych

• Zarządzanie incydentami związanymi z bezpieczeństwem informacji

• Ciągłości działania

• Zgodność

ISO/IEC 27001

W 2005 r. ISO i IEC wydały ISO/IEC 27001. Norma ta określa sposób certyfikacji organizacji jako zgodnych z normą ISO/IEC 27002. Jest to ważne, ponieważ wykazując zgodność, firmy mogą zapewnić partnerów biznesowych (i ich kierownictwo), że firma bezpieczeństwo jest dobrze zarządzane. W innych ramach, w tym COSO i CobiT, firmy certyfikują się same, czasami za zgodą audytora zewnętrznego. Brakuje im procesu certyfikacji stron trzecich ISO/IEC 27001, który strony zewnętrzne mogą wysoko cenić. Jednak certyfikacja niekoniecznie zapewnia doskonałe bezpieczeństwo – tylko to, że funkcja zarządzania bezpieczeństwem IT jest zgodna z normą ISO/IEC 27002. Bezpieczeństwo IT, jak wspomniano na początku tego rozdziału, nie może zagwarantować, że nie nastąpią żadne naruszenia bezpieczeństwa.

INNE 27000 STANDARDÓW

ISO i IEC pracują nad wieloma innymi normami dla rodziny 27000. Norma ISO/IEC 27004 określi sposób mierzenia metryk bezpieczeństwa, ISO/IEC 27005 będzie proponowanym standardem zarządzania ryzykiem, a ISO/IEC 27007 będzie koncentrować się na audycie.

TEST LV

a. Jaka jest funkcja ISO/IEC 27001 w rodzinie norm 27000?

b. Jaka jest funkcja ISO/IEC 27002 w rodzinie norm 27000?

c. Wymień 11 szerokich obszarów w 27002.

d. Dlaczego certyfikacja ISO/IEC 27000 jest dla firm bardziej atrakcyjna niż certyfikacja COSO czy CobiT?

WNIOSEK

Zaczęliśmy od cytatu podkreślającego znaczenie zarządzania bezpieczeństwem w porównaniu z technologią bezpieczeństwa. Przyjrzeliśmy się cyklowi planu-zabezpiecz-odpowiedz oraz niektórym z wielu zawiłości zarządzania bezpieczeństwem IT. W dalszej części książki będziemy przyglądać się aspektom zarządzania bezpieczeństwem IT w kontekście różnych zabezpieczeń. Następnie przyjrzeliśmy się kilku prawom i przepisom dotyczącym zgodności, które działają jako siły napędowe w zarządzaniu bezpieczeństwem IT - Sarbanes–Oxley, przepisom dotyczącym prywatności, przepisom dotyczącym powiadamiania o naruszeniu danych, PCI-DSS i FISMA. Omówiono funkcjonowanie, umiejscowienie, ogólny charakter interakcji między działem bezpieczeństwa IT a innymi działami organizacyjnymi oraz outsourcing do dostawców usług zarządzania bezpieczeństwem. Rozdział następnie przyjrzał się klasycznej analizie ryzyka, jej problemom i sposobom reagowania na ryzyko. Doprowadziło nas to do dyskusji na temat architektury bezpieczeństwa, polityk, standardów, procedur i najlepszych praktyk w branży. Dostrzegliśmy potrzebę nadzoru nad istniejącymi zasadami, audytami i sankcjami w celu zapobiegania oszustwom wewnętrznym. Rozdział zakończył się omówieniem kilku dobrze znanych ram zarządzania, w tym COSO, CobiT i ISO 27002. Ramy pomagają firmom, zapewniając systematyczny sposób podejścia do planowania, wdrażania, monitorowania i stopniowego doskonalenia bezpieczeństwa IT.

Przemyślane pytania

1. Wymień 12 celów kontrolnych PCI-DSS. Będziesz musiał to sprawdzić w Internecie.

2. Omówiono trzy sposoby postrzegania funkcji bezpieczeństwa IT – jako siły policyjnej, organizacji wojskowej i kochającej matki. Nazwij inny pogląd i opisz, dlaczego jest dobry.

3. Firma posiada zasób XYZ. W przypadku naruszenia bezpieczeństwa firma może zostać ukarana grzywną w wysokości 100 000 USD i zapłacić kolejne 20 000 USD w celu usunięcia naruszenia. Firma uważa, że atak może się powieść mniej więcej raz na pięć lat. Proponowany środek zaradczy powinien zmniejszyć częstotliwość występowania o połowę. Ile firma powinna być skłonna zapłacić za środek zaradczy?

CO TO JEST KRYPTOGRAFIA?

Większość ludzi myśli o bezpieczeństwie informacji jako o nowym problemie. Jednak potrzeba bezpiecznego przesyłania informacji istnieje od tysięcy lat. Wcześni dowódcy wojskowi musieli bezpiecznie wysyłać rozkazy, a renesansowi książęta handlowi musieli utrzymywać w tajemnicy swoje wiadomości handlowe. Dziś przedsiębiorstwa i rządy mają taką samą potrzebę zachowania tajemnicy. W tym celu zwracają się do kryptografii, która polega na wykorzystaniu operacji matematycznych do ochrony wiadomości przesyłanych między stronami lub przechowywanych na komputerze.

Kryptografia to wykorzystanie operacji matematycznych do ochrony wiadomości przesyłanych między stronami lub przechowywanych na komputerze.

W latach 60. wielu wierzyło, że kryptografia będzie głównym środkiem zaradczym dla ataków. Chociaż pogląd ten okazał się zbyt ograniczony, kryptografia pozostaje bardzo ważnym środkiem zaradczym w zakresie bezpieczeństwa. Dodatkowo kryptografia jest częścią wielu innych środków zaradczych, dlatego w tym i następnym rozdziale rozpoczniemy omawianie technologii środków zaradczych od kryptografii.

W wiadomościach

Brazylijskie władze skonfiskowały pięć dysków twardych brazylijskiemu bankierowi Danielowi Dantasowi, podejrzanemu o przestępstwa finansowe. Brazylijski Narodowy Instytut Kryminologii (NIC) przez pięć miesięcy bezskutecznie próbował złamać szyfrowanie na dyskach twardych. NIC poprosił o pomoc FBI. FBI również nie odniosło sukcesu po 12-miesięcznym wysiłku przy użyciu różnych ataków słownikowych. Dantas użył 256-bitowego algorytmu szyfrowania AES do zaszyfrowania dysków. Algorytm został zaimplementowany przy użyciu popularnego oprogramowania szyfrującego innej firmy o nazwie TrueCrypt. Gdyby Dantas użył słabszego hasła opartego na powszechnym słowie ze słownika, dane mogłyby zostać odszyfrowane.

Szyfrowanie w celu zachowania poufności

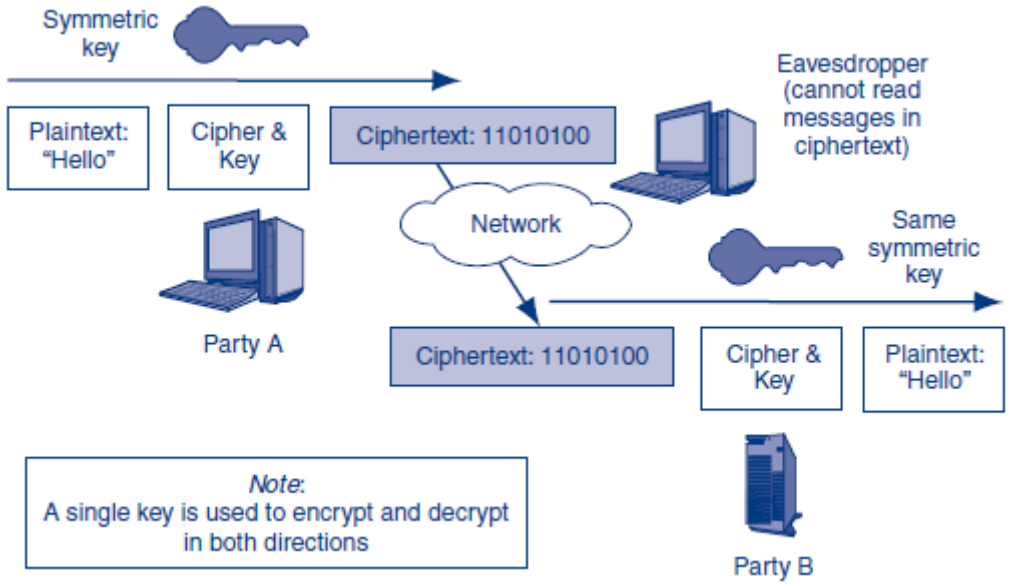
Wspólnym celem bezpieczeństwa jest poufność, co oznacza, że osoby przechwytujące wiadomości nie mogą ich odczytać. Rysunek pokazuje, że poufność wymaga pewnego rodzaju kryptografii zwanego szyfrowaniem. Szyfrowanie w celu zachowania poufności było pierwotnym celem kryptografii.

Poufność oznacza, że osoby, które przechwytują wiadomości, nie mogą ich czytać.

Terminologia

TEKST ZWYKŁY

Rysunek pokazuje, że oryginalna wiadomość nazywana jest tekstem jawnym.



Ta nazwa wydaje się sugerować, że kryptografia działa tylko w przypadku wiadomości tekstowych. Tak było, gdy ukuto termin „tekst jawny". Obecnie jednak wiadomości tekstowe mogą być obrazami, dźwiękami, filmami lub kombinacją kilku formatów danych. Oryginalna nazwa utknęła jednak, więc każda oryginalna wiadomość jest nazywana zwykłym tekstem.

SZYFROWANIE I DESZYFROWANIE

Szyfrowanie to proces kryptograficzny, który zamienia tekst jawny w pozornie losowy strumień bitów zwany tekstem zaszyfrowanym. Nadawca wysyła ten zaszyfrowany tekst do odbiorcy.

Podsłuchujący nie będą w stanie zrozumieć zaszyfrowanego tekstu, jeśli go przechwycą. Jednak odbiorca będzie mógł odszyfrować zaszyfrowany tekst, zamieniając go z powrotem w oryginalny tekst jawny.

SZYFR

Rysunek pokazuje, że szyfrowanie i deszyfrowanie wymagają dwóch rzeczy. Pierwszy to szyfr, który jest specyficznym procesem matematycznym używanym do szyfrowania i deszyfrowania. Istnieje wiele szyfrów i wszystkie działają inaczej. Obie strony muszą użyć tego samego szyfru, aby odbiorca mógł odszyfrować wiadomość.

Szyfr to specyficzny proces matematyczny używany do szyfrowania i deszyfrowania

KLUCZ

Drugą rzeczą, której wymaga szyfrowanie i deszyfrowanie, jest klucz, który jest losowym ciągiem od 40 do 4000 bitów (jedynek i zer). (Dłuższe klucze są trudniejsze do odgadnięcia, co zapewnia większą poufność). Dla danego szyfru różne klucze generują różne szyfrogramy z tego samego tekstu jawnego.

Klucz to losowy ciąg bitów (jedynek i zer).

ZACHOWANIE TAJEMNICY KLUCZA

Matematyk Auguste Kerckhoffs przekonywał, że w praktyce nie da się utrzymać szyfru w tajemnicy. Jest tylko kilka dobrze przetestowanych szyfrów i zazwyczaj łatwo jest określić, który z nich jest używany. Na szczęście Kerckhoffs udowodnił, że dopóki klucz będzie utrzymywany w tajemnicy, obie

strony zachowają poufność. Prawo Kerckhoffsa mówi, że utrzymywanie kluczy w tajemnicy jest receptą na bezpieczne szyfrowanie.

Prawo Kerckhoffsa mówi, że aby zachować poufność, partnerzy komunikacji muszą jedynie zachować w tajemnicy klucz, a nie szyfr.

Prosty szyfr

Rysunek ilustruje prosty szyfr. Ten szyfr działa na literach alfabetu. Rysunek ma trzy kolumny.

• Pierwsza kolumna ma dość banalny tekst jawny, jak na razie. Aby uprościć przykład, usunięto wielkie litery i spacje.

• Druga kolumna zawiera klucz. Ten klucz to seria liczb od 1 do 26.

• Trzecia kolumna to zaszyfrowany tekst do przesłania.

Plaintext	Key	Ciphertext
n	4	r
o	8	w
w	15	l
i	16	...
s	23	...
t	16	...
h	3	...
e	9	...
t	12	...
i	20	...
m	6	...
e	25	...

W tym szyfrze tekst jawny jest zamieniany na tekst zaszyfrowany, przesuwając każdą literę w dół alfabetu. Litera tekstu jawnego jest przesunięta o N miejsc dalej w alfabecie, gdzie N jest liczbą w kluczu dla tej litery. Na przykład, jeśli literą tekstu jawnego jest b, a wartość klucza to 2, symbolem zaszyfrowanego tekstu jest d.

• Pierwsza litera w tekście jawnym przykładu to n, a wartość klucza to 4. Cztery miejsca poza n w alfabecie to r, więc r jest symbolem tekstu zaszyfrowanego dla pierwszego znaku.

• Następna litera tekstu jawnego to o. Kluczową wartością jest tym razem 8. W konsekwencji zaszyfrowany tekst to w.

• Trzecia litera w tekście jawnym to w, a wartość klucza to 15. Piętnaście kroków wykracza poza koniec alfabetu i zaczyna się ponownie od a. Ostatnim symbolem szyfrogramu jest l. Jak dotąd mamy zaszyfrowany tekst rwl. Jeśli oglądałeś teleturniej Koło fortuny, wiesz, że częstą literą alfabetu jest e. Ta litera pojawia się dwukrotnie w tej prostej wiadomości. Jednak ma on różne wartości klucza za każdym razem - 9 i 25. Używając losowego klucza, szyfr ten może uniemożliwić analizę tekstu według częstotliwości liter. W tym przykładzie użyto liter alfabetu jako tekstu jawnego. Jednak prawie wszystkie informacje komputerowe są zakodowane jako zestaw bitów. Klucze to także ciągi jedynek i zer. Ponadto prawdziwe szyfry wykorzystują wiele rund obliczeń. Po zakończeniu szyfrowania zaszyfrowany tekst przypomina czysto losowy ciąg jedynek i zer.

Kryptoanaliza

Kryptoanalityk to ktoś, kto łamie szyfrowanie. Ten najprostszy rodzaj kryptoanalizy to brutalne łamanie klucza - próba wszystkich możliwych kluczy, dopóki kryptoanalityk nie znajdzie właściwego klucza. Jednak, jak zobaczymy w dalszej części, jeśli klawisze są długie, łamanie klawiszy metodą brute force będzie trwało zbyt długo, aby było użyteczne. W niektórych przypadkach kryptoanalitycy mogą odgadnąć przynajmniej część wiadomości. Na przykład podczas II wojny światowej japońskie raporty morskie często zaczynały się od tego samego standardowego powitania początkowego. Gdy takie prawidłowości wystąpią, kryptoanalityk może dość szybko nauczyć się przynajmniej części klucza. Ponadto implementacja szyfru może być słaba, pozwalając aby część klucza „wyciekała" z każdą wiadomością. Standard transmisji bezprzewodowej sieci LAN 802.11 początkowo wykorzystywał metodę zabezpieczeń o nazwie Wired Equivalent Privacy (WEP). WEP wykorzystał implementację szyfru RC4, który ujawnił informacje. Obecnie klucze WEP można złamać w dwie lub trzy minuty.

TEST LVI

a. Zdefiniuj kryptografię.

b. Czym jest poufność?

c. Rozróżnij tekst jawny i tekst zaszyfrowany.

d. Co jest przesyłane przez sieć - tekst jawny czy tekst zaszyfrowany?

e. Czym jest szyfr?

f. Czym jest klucz?

g. Co należy zachować w tajemnicy w szyfrowaniu, aby zachować poufność?

h. Kim jest kryptoanalityk?

Dokończ szyfrowanie na rysunku 2.

Szyfry podstawieniowe i transpozycyjne

Specyficzne procesy matematyczne w dzisiejszych szyfrach są niezwykle złożone. Jednak większość wykorzystuje warianty dwóch podstawowych procesów matematycznych — podstawienia i transpozycji.

Szyfry podstawieniowe

W szyfrach podstawieniowych jeden znak jest zastępowany innym, ale kolejność znaków nie ulega zmianie. Przykładowy szyfr jest bardzo prostym szyfrem podstawieniowym. Każda litera jest zastępowana inną literą alfabetu. Jednak pozycja każdej litery jest taka sama. Więc n-o-w staje się r-w-l.

W szyfrach podstawieniowych jeden znak jest zastępowany innym.

Szyfry transpozycji

Z kolei w szyfrach transpozycyjnych litery są przemieszczane w obrębie wiadomości na podstawie ich początkowej pozycji w wiadomości. Same litery nie są zmieniane, jak w przypadku szyfrów zastępczych, ale zmienia się ich pozycja w komunikacie.

Szyfry transpozycyjne przenoszą litery w wiadomości, ale znaki nie są zastępowane.

Rysunek 3 przedstawia prosty szyfr transpozycji. Po pierwsze, tekst jawny (nowistthet) jest zapisany w macierzy trzy na trzy — lub tyle wiadomości, ile zmieści się w macierzy. Klucz ma sześć cyfr (132231). Pierwsza część klucza (132) składa się z liczby w każdej kolumnie, a druga część (231) liczby w każdym rzędzie.

	Key (Part 1)		
Key (Part 2)	1	3	2
2	n	o	w
3	i	s	t
1	h	e	t

Szyfr określa sposób wyjmowania liter z pola transpozycji. Pierwsza litera będzie miała wartość klucza kolumny 1 i wartość klucza wiersza 1. To jest pierwsza kolumna i trzeci wiersz. Litera tam jest h. Więc h jest pierwszym znakiem szyfrogramu. Druga litera będzie miała wartość klucza kolumny 1 i wartość klucza wiersza 2. To jest pierwsza kolumna i pierwszy wiersz. Litera tam jest n. Więc n jest drugim znakiem szyfrogramu. Mamy teraz hn na początku szyfrogramu. Resztę zaszyfrowanego tekstu można określić, pobierając litery z pola transpozycji w podobnej kolejności kolumna-wiersz.

Szyfrowanie w świecie rzeczywistym

W szyfrach podstawieniowych litery są zmieniane, ale ich pozycja nie. W szyfrach transpozycyjnych litery nie są zmieniane, ale zmienia się ich pozycja w szyfrogramie. Prawdziwe szyfry są znacznie bardziej złożone niż wskazywały na to nasze przykłady. Po pierwsze, szyfrowanie odbywa się na bitach, a nie na literach alfabetu. Ponadto szyfry w świecie rzeczywistym mieszają kilka rund transpozycji i podstawienia, aby zapewnić dobrą losowość. Na szczęście specjaliści ds. bezpieczeństwa w organizacjach nie muszą rozumieć specyfiki działania prawdziwych szyfrów szyfrujących.

TEST LVII

a. Co pozostawia litery bez zmian – szyfry transpozycyjne lub podstawieniowe?

b. Co pozostawia litery w ich pierwotnych pozycjach — szyfry transpozycyjne lub podstawieniowe?

Dokończ szyfrowanie na rysunku 3.

Szyfry i kody

Czytając tą część, być może spodziewałeś się, że zamiast szyfru zobaczysz termin kod. Jednak szyfr to ogólny sposób szyfrowania informacji, podczas gdy kody są ograniczone. W szyfrze pojedyncza litera jest zastępowana inną literą lub ciąg bitów o stałej długości jest zastępowany innym ciągiem bitów o stałej długości. Obie strony muszą tylko znać klucz. Jeśli to zrobią, mogą przekazać wszystko, co zechcą. Kompromis polega na tym, że szyfrowanie może podlegać kryptoanalizie. Podczas gdy szyfry działają na pojedynczych znakach, kody używają symboli kodu, które reprezentują całe słowa lub frazy. Rysunek 4 pokazuje uproszczoną wersję japońskiego kodu operacyjnego marynarki wojennej JN-25 używanego podczas II wojny światowej. Dla każdego słowa lub symbolu interpunkcyjnego istnieje pięciocyfrowe słowo kodowe. To słowo kodowe jest wysyłane zamiast słowa lub innego symbolu. Aby zakodować wiadomość, nadawca wyszukuje słowo lub symbol i zapisuje pięciocyfrowy kod. Następnie przechodzi do następnego słowa lub symbolu. Na początek sprawdza „od” i widzi, że kod to 17434. Nadawca rozpoczyna szyfrogram od 17434.

Message	Code
From	17434
Akagi	63717
To	83971
Truk	11131
STOP	**34058**
ETA	53764
6 PM	73104
STOP	**26733**
Require	29798
B	72135
N	54678
STOP	**61552**

W przypadku powszechnych słów lub symboli książka kodów miałaby kilka numerów kodów. Na przykład w komunikacie trzykrotnie pojawia się STOP. Za pierwszym razem jest kodowany jako 34058. Następnym razem jest kodowany jako 26733. Za trzecim razem jest kodowany jako 61552. Posiadanie wielu kodów dla popularnych słów i symboli utrudnia kryptoanalitykom złamanie kodu. Kody są atrakcyjne, ponieważ ludzie mogą kodować i dekodować ręcznie, bez komputera. Minusem jest to, że książki kodów muszą być dystrybuowane z wyprzedzeniem, a jeśli jedna książka kodów zostanie przechwycona, cała poufność zostaje utracona. Ponadto nawet popularne terminy mają tylko ograniczoną liczbę możliwych kodów. W związku z tym kryptoanalitycy, którzy przechwycili duży ruch, mogą stosunkowo łatwo nauczyć się książki kodów. W przeciwieństwie do tego, szyfry mogą zaszyfrować wszystko, a jeśli klucz szyfru jest wystarczająco długi (i jeśli zostaną podjęte odpowiednie kroki, aby zapewnić, że ludzie nie zrobią czegoś, co zmniejszy ochronę), szyfry są niezwykle silne. Fakt, że szyfry są złożone obliczeniowo, nie jest już przeszkodą w ich użyciu, dzięki szybkiemu przetwarzaniu dostępnemu nawet w telefonach komórkowych.

TEST LVIII

a. Co oznaczają symbole kodu w kodach?

b. Jaka jest zaleta kodów?

c. Jakie są wady?

Zakończ kodowanie wiadomości na rysunku 4.

Szyfrowanie kluczem symetrycznym

Szyfr, o którym mówiliśmy, nazywa się szyfrem z kluczem symetrycznym, ponieważ obie strony szyfrują i deszyfrują za pomocą tego samego klucza. W komunikacji dwukierunkowej z szyfrowaniem kluczem symetrycznym obie strony używają tylko jednego klucza do szyfrowania i deszyfrowania w obu kierunkach.

W szyfrowaniu z kluczem symetrycznym do szyfrowania i deszyfrowania w obu kierunkach używany jest jeden klucz.

Szyfrowanie kluczem symetrycznym jest bardzo szybkie, co powoduje niewielkie obciążenie obliczeniowe komputerów. W rezultacie nawet komputery osobiste i urządzenia przenośne mają wystarczającą moc obliczeniową do szyfrowania za pomocą szyfrowania z kluczem symetrycznym. Ze względu na niskie obciążenie przetwarzania przesyłanie plików, wiadomości błyskawiczne i inne

popularne aplikacje wykorzystują szyfrowanie kluczem symetrycznym w celu zachowania poufności. W rzeczywistości prawie tylko niewielka część szyfrowania w celu zachowania poufności wykorzystuje szyfrowanie z kluczem symetrycznym.

Prawie każde szyfrowanie w celu zachowania poufności wykorzystuje szyfrowanie z kluczem symetrycznym.

DŁUGOŚĆ KLUCZA

Widzieliśmy, że tylko klucz musi być utrzymywany w tajemnicy, aby zapewnić poufność. Jednym ze sposobów, w jaki atakujący może nauczyć się klucza, jest przeprowadzenie wyczerpującego wyszukiwania i wypróbowanie wszystkich możliwych kluczy, aż znajdzie właściwy. Najprostszym sposobem na udaremnienie wyczerpujących poszukiwań jest po prostu sprawienie, aby klucz był tak długi, że czas potrzebny na złamanie klucza przez atakujących jest zbyt długi, aby był praktyczny. Jeśli długość klucza wynosi N bitów, istnieje 2N możliwych kluczy. Przeciętnie kryptograf będzie musiał wypróbować połowę wszystkich kluczy, zanim się powiedzie, więc złamanie klucza powinno zająć około ($2^N/2$). Na przykład, jeśli klucz ma długość 8 bitów, jest tylko 256 możliwych kluczy (2^8 = 256). Znalezienie prawidłowego klucza zajmie kryptoanalitykowi średnio tylko 128 prób. Jak pokazano na rysunku 3-5, każdy dodatkowy bit w kluczu podwaja czas potrzebny na złamanie klucza.

Key Length in Bits	Number of Possible Keys
1	2
2	4
4	16
8	256
16	65,536
40	1,099,511,627,776
56	72,057,594,037,927,900
112	5,192,296,858,534,830,000,000,000,000,000
112	5.1923E+33
168	3.74144E+50
256	1.15792E+77
512	1.3408E+154

Zwiększenie długości klucza z 8 do 9 bitów będzie wymagało od kryptoanalityka wypróbowania połowy 512 kluczy (2^9 = 512) zamiast połowy 256. Podwoiłoby to czas potrzebny do złamania klucza.

Każdy dodatkowy bit w kluczu podwaja czas potrzebny na złamanie klucza.

Podwojenie długości klucza wielokrotnie zwiększa liczbę możliwych kluczy. Na przykład zwiększenie długości klucza z 8 do 16 bitów zwiększa liczbę możliwych kluczy 256 razy (65 536/256 = 256). W bardziej imponującym przykładzie zwiększenie długości klucza z 56 do 112 bitów zwiększa wyczerpujący czas wyszukiwania 72 biliardy razy! Niektóre kraje ograniczyły długość klucza symetrycznego w eksportowanych produktach do 40 bitów, aby zachować zdolność agencji rządowych do złamania kluczy, gdy zajdzie taka potrzeba. Dziś klucze 40-bitowe można złamać bardzo szybko. W Wielkiej Brytanii rozporządzenie o uprawnieniach dochodzeniowych (RIPA) może być wykorzystywane do zmuszania osób do ujawnienia kluczy szyfrowania. Kilka osób trafiło do więzienia za nieoddanie kluczy. W latach 70. silne klucze symetryczne (tj. klucze, których złamanie jest zbyt czasochłonne) musiały mieć tylko około 56 bitów, aby szyfrować kluczem symetrycznym. Obecnie klucze symetryczne muszą mieć co najmniej 100 bitów, aby można je było uznać za silne. Ponieważ moc komputerów

kryptoanalityków stale rośnie, do silnego szyfrowania potrzebne będą jeszcze dłuższe klucze symetryczne.

Obecnie klucz symetryczny o długości 100 bitów lub dłuższy jest uważany za silny klucz symetryczny.

TEST LIX

a. Dlaczego słowo symetryczne jest używane w szyfrowaniu z kluczem symetrycznym?

b. Kiedy dwie strony komunikują się ze sobą za pomocą szyfrowania kluczem symetrycznym, ile kluczy jest używanych łącznie?

c. Jaki rodzaj szyfru jest prawie zawsze używany w szyfrowaniu w celu zachowania poufności?

a. Jaki jest najlepszy sposób na udaremnienie wyczerpujących poszukiwań przez kryptoanalityków?

b. Jeśli klucz ma 43 bity, ile czasu zajmie złamanie go przez wyczerpujące wyszukiwanie, jeśli zostanie rozszerzony do 45 bitów?

c. Jeśli zostanie rozszerzony do 50 bitów?

d. Jeśli klucz ma długość 40 bitów, ile kluczy trzeba średnio wypróbować, aby go złamać?

e. Jak długo musi być dzisiaj klucz szyfrowania symetrycznego, aby był uważany za silny?

Problemy ludzkie w kryptografii

Przy wystarczająco długich kluczach i dobrze przetestowanym szyfrze szyfrowanie kluczem symetrycznym w celu zachowania poufności jest niepraktyczne do złamania z technicznego punktu widzenia. Jeśli jednak nadawca lub odbiorca nie utrzyma klucza w tajemnicy, podsłuchujący może poznać klucz i przeczytać każdą wiadomość. Mówiąc szerzej, ogólnie słaba dyscyplina komunikacji może pokonać najsilniejszy szyfr i najdłuższy klucz. Na przykład podczas II wojny światowej japońska marynarka wojenna często wysyłała wiadomości, gdy nie było takiej potrzeby. Dało to alianckim kryptologom dużą bazę wiadomości do zbadania. To znacznie ułatwiło pracę kryptoanalitykom, niż gdyby Japończycy stosowali lepszą dyscyplinę komunikacyjną. Ponadto, jak wspomniano wcześniej, raporty japońskiej marynarki często zaczynały się od standardowego, kwiecistego wstępu, który miał kilka zdań. Ta sytuacja ze „znanym tekstem jawnym" była nieoceniona przy łamaniu japońskich książek kodowych. Pomocny był również fakt, że transmisje często odbywały się zgodnie z ustalonym formatem dla typowych sytuacji, takich jak raportowanie prędkości statku i namiaru kompasu.

W wiadomościach

W grudniu 2009 r. Google (Gmail) doświadczył wysoce skoordynowanego ataku hakerów z Chin, którzy skupili się na zbieraniu informacji o obrońcach praw człowieka. Miesiąc później, w styczniu 2010 r., Google ogłosił, że będzie zabezpieczać całą pocztę za pomocą protokołu SSL (Secure Sockets Layer).Wcześniej poczta e-mail była wysyłana w sposób jawny i była podatna na ataki typu man-in-the-middle. Wysyłanie zaszyfrowanej wiadomości e-mail przy użyciu protokołu HTTPS powoduje nieco mniejszą ogólną szybkość połączenia w porównaniu z tradycyjnym połączeniem HTTP. Jednak użycie SSL do szyfrowania wiadomości e-mail zapewniłoby całkowitą poufność i powstrzymałoby ataki typu man-in-the-middle. Korzystanie z protokołu HTTPS jest teraz domyślne na wszystkich kontach Gmail.

Komunikujący się partnerzy mogą nawet mieć fałszywe poczucie bezpieczeństwa, ponieważ będą myśleć, że złamana metoda szyfrowania nadal ich chroni. W czasie II wojny światowej Niemcy mieli

bardzo zaawansowaną technicznie maszynę szyfrującą o nazwie Enigma. Jednak polskie wojsko zdobyło kopię maszyny i poddało ją inżynierii wstecznej, aby ujawnić, jak działa. Po upadku Polski w ręce Niemiec Polacy przekazali swoje wyniki Anglikom, którzy kontynuowali pracę. W końcu Anglicy mogli odczytać duży procent niemieckich wiadomości zaszyfrowanych Enigmą. Nadmiernie pewni siebie Niemcy wysyłali ogromne ilości bardzo wrażliwych kierowców, myśląc, że są całkowicie bezpieczni. Rzeczywistość kryptografii jest taka, że nie jest to automatyczna ochrona. Działa tylko wtedy, gdy firmy mają i wymuszają procesy organizacyjne, które nie naruszają technicznych zalet kryptografii.

TEST LX

Dlaczego kryptografia nie jest automatyczną ochroną?

SZYFROWANIE KLUCZY SYMETRYCZNYCH

Podczas korzystania z szyfrowania kluczem symetrycznym możesz wybierać spośród różnych szyfrów. Wszyscy osiągają ostateczny cel, jakim jest stworzenie zaszyfrowanej wiadomości. Jednak działają one bardzo różnie i różnią się siłą, szybkością i wymaganiami obliczeniowymi. Partnerzy komunikacji muszą wybrać określony szyfr szyfrowania kluczem symetrycznym, jeśli chcą komunikować się bezpiecznie. Tylko kilka popularnych szyfrów szyfrowania z kluczem symetrycznym zostało dobrze przetestowanych i ważne jest, aby wybrać spośród tych kilku. Przyjrzymy się najpopularniejszym, dobrze przetestowanym szyfrom: RC4, DES, 3DES i AES.

RC4

Najsłabszym powszechnie obecnie używanym szyfrem jest RC4, który jest zwykle wymawiany jako „ARKA CZWARTA". RC4 ma dwie zalety w stosunku do innych popularnych algorytmów szyfrowania. Po pierwsze, RC4 jest niezwykle szybki i wykorzystuje tylko niewielką ilość pamięci RAM. Oznacza to, że idealnie nadaje się do małych urządzeń przenośnych i sprawdza się nawet w przypadku najwcześniejszych bezprzewodowych punktów dostępowych 802.11. W konsekwencji RC4 stał się podstawą cieszącego się złą sławą systemu szyfrowania WEP dla bezprzewodowych sieci LAN, który zobaczymy w rozdziale 4. Po drugie, RC4 może używać szerokiego zakresu długości kluczy. W przypadku większości szyfrów dłuższa długość klucza jest lepsza. Jednak RC4 był szeroko stosowany przede wszystkim dlatego, że jego najkrótsza opcjonalny klucz to 40 bitów. Jak wspomniano wcześniej w tym rozdziale, krajowe ograniczenia eksportowe w wielu krajach ograniczały kiedyś produkty komercyjne do szyfrowania 40-bitowego. W konsekwencji 40-bitowy RC4 stał się standardową długością klucza WEP. Niestety, RC4 jest niebezpiecznym szyfrem. Jeśli nie jest poprawnie zaimplementowany, jego ochrona jest minimalna. Słaba implementacja RC4 sprawiła, że WEP jest tak słabym systemem ochrony bezprzewodowych sieci LAN.

TEST LXI

a. Jakie są dwie zalety RC4?

b. Dlaczego powszechnie używany jest klucz RC4 o długości 40 bitów?

c. Czy to mocny klucz?

Standard szyfrowania danych (DES)

W 1977 r. amerykańskie Krajowe Biuro Standardów, które obecnie jest Narodowym Instytutem Standardów i Technologii (NIST), stworzyło standard szyfrowania danych (DES). DES szybko stał się najczęściej stosowaną metodą szyfrowania kluczem symetrycznym. DES jest nadal powszechnie

używany, ponieważ przetrwał wszystko oprócz wyczerpujących ataków wyszukiwania metodą brute-force, ponieważ jest powszechnie dostępny i jest obsługiwany przez akceleratory sprzętowe.

56-BITOWY ROZMIAR KLUCZY

Klucz DES ma długość 56 bitów. Występuje w bloku 64 bitów, z których 56 bitów reprezentuje klucz. Pozostałe 8 bitów jest nadmiarowych w tym sensie, że możesz je obliczyć, jeśli znasz pozostałe 56 bitów. Ta nadmiarowość umożliwia stronom wykrywanie nieprawidłowych kluczy. Obecnie 56-bitowy rozmiar klucza jest zbyt krótki dla dużych transakcji biznesowych i wysoce wrażliwych tajemnic handlowych.13 Jest jednak wystarczający dla większości domowych zastosowań konsumenckich i, jak zobaczymy dalej, kryptografowie rozszerzyli DES na 3DES dla celów przemysłowych. siła bezpieczeństwa. Nawet 56-bitowy DES zużywa umiarkowaną ilość pamięci RAM i jest tylko umiarkowanie szybki.

SZYFROWANIE BLOKOWE

Rysunek poniżej pokazuje, że DES jest standardem szyfrowania blokowego. DES szyfruje wiadomości 64 bity na raz. Dane wejściowe do szyfrowania to klucz i 64-bitowy blok zwykłego tekstu. Dane wyjściowe to 64-bitowy blok zaszyfrowanego tekstu

TEST LXII

a. Jak długi jest klucz DES?

b. Czy to mocna długość?

c. Opisz szyfrowanie blokowe za pomocą DES.

Tam, gdzie firmy potrzebują silniejszego szyfrowania niż zapewnia DES, mogą skorzystać z potrójnego DES (3DES), które rozszerza efektywny rozmiar klucza DES w prosty, ale boleśnie powolny sposób, który wykorzystuje umiarkowaną ilość pamięci RAM.

168-BITOWA OBSŁUGA 3DES

Algorytm 3DES po prostu stosuje DES trzy razy z rzędu dla dodatkowej siły. Zwykle odbywa się to za pomocą trzech różnych kluczy DES. Daje to efektywną długość klucza 168 bitów (3 razy 56). To jest bardzo mocne.

112-BITOWY 3DES

Wariant 3DES wykorzystuje tylko dwa klucze. W tym podejściu trzecią operacją nadawcy jest zaszyfrowanie danych wyjściowych drugiego etapu za pomocą pierwszego klucza – klucza, którego użył w pierwszym kroku. To skutecznie zapewnia szyfrowanie 112-bit16, które jest silne i wymaga jedynie bezpiecznej dystrybucji dwóch kluczy DES.

PERSPEKTYWA NA 3DES

Z punktu widzenia bezpieczeństwa 3DES zapewnia silne szyfrowanie kluczem symetrycznym. Jednak z praktycznego punktu widzenia DES jest powolny, a konieczność trzykrotnego zastosowania DES jest bardzo powolna, a zatem kosztowna pod względem kosztów przetwarzania.

TEST LXIII

a. Jak działa 3DES?

b. Jakie są dwie wspólne efektywne długości kluczy w 3DES?

c. Czy te długości są wystarczające do komunikacji w korporacjach?

d. Jaka jest wada 3DES?

Zaawansowany standard szyfrowania (AES)

W odpowiedzi na słabą długość klucza DES i przetwarzanie obciążeniem 3DES, NIST wydał w 2001 r. Advanced Encryption Standard (AES). AES jest wystarczająco wydajny pod względem mocy obliczeniowej i wymagań pamięci RAM, aby można go było używać na szerokiej gamie urządzeń – nawet telefonach komórkowych i osobistych asystentach cyfrowych (PDA). AES oferuje trzy alternatywne długości kluczy: 128 bitów, 192 bity i 256 bitów. Nawet 128-bitowa długość klucza jest silna. System gwałtownego łamania kodu, który mógłby pokonać 56-bitowy DES w sekundę, zajęłby ponad 100 bilionów lat, aby złamać 128-bitowy AES. Dłuższe klucze są wystarczająco mocne nawet dla materiału, który musi być trzymany w tajemnicy przez wiele lat. Wiele systemów kryptograficznych obsługuje teraz AES, a AES powinien zdominować szyfrowanie w celu zapewnienia poufności w najbliższej przyszłości.

TEST LXIV

a. Jaka jest duża przewaga AES nad 3DES?

b. Jakie są trzy długości kluczy oferowane przez AES?

c. Jakiego silnego szyfru z kluczem symetrycznym można używać z małymi urządzeniami mobilnymi?

d. Który szyfr szyfrowania kluczem symetrycznym prawdopodobnie zdominuje szyfrowanie kluczem symetrycznym w najbliższej przyszłości?

Inne szyfry z kluczem symetrycznym

Istnieje wiele innych szyfrów szyfrujących kluczem symetrycznym. Jednak tylko kilka z tych innych szyfrów przetrwało lata szeroko zakrojonej kryptoanalizy. Wśród tych, które to zrobiły i które widzą znaczące zastosowanie, są IDEA (zwłaszcza w Europie), SEED (w Korei Południowej), GOST (w Rosji) i Camellia (w Japonii). Niestety, wiele firm z dumą reklamuje „nowe i zastrzeżone" szyfry szyfrujące. Twierdzą, że ponieważ atakujący nie znają algorytmu szyfru, nie będą w stanie złamać szyfrowania. Jednak specjaliści ds. Bezpieczeństwa wyśmiewają to jako zabezpieczenie przez ukrywanie, ponieważ opiera się na tajności lub niemożności uzyskania przez atakującego informacji o szyfrze, a nie na odporności samego szyfru. Jeśli szczegóły niesprawdzonego szyfru zostaną ujawnione, może to spowodować katastrofalną utratę bezpieczeństwa.

Bezpieczeństwo poprzez ukrywanie to zasada polegania na tajności w celu stworzenia bezpieczeństwa poprzez ukrywanie potencjalnych luk w zabezpieczeniach.

W praktyce szyfrogram zaszyfrowany zastrzeżonymi algorytmami zazwyczaj jest łamany szybko, nawet jeśli atakujący nie zna szczegółowego szyfru. Stworzenie pozbawionego luk szyfru szyfrującego jest niezwykle trudne, nawet dla profesjonalistów w tej dziedzinie. Dlatego w organizacjach powinny być używane tylko bardzo dobrze przetestowane szyfry. Na zajęciach z bezpieczeństwa na wydziałach informatyki studenci zazwyczaj uczą się, jak projektować nowe szyfry szyfrujące. Natomiast zajęcia z bezpieczeństwa systemów informatycznych uczą studentów, aby nigdy nie tworzyć własnych algorytmów szyfrowania.

Na zajęciach z bezpieczeństwa na wydziałach informatyki studenci zazwyczaj uczą się, jak projektować nowe szyfry szyfrujące. Natomiast zajęcia z bezpieczeństwa systemów informatycznych uczą studentów, aby nigdy nie tworzyć własnych algorytmów szyfrowania.

TEST LXV

a. Twierdzi się, że nowe i zastrzeżone szyfry szyfrujące są dobre, ponieważ kryptoanalitycy ich nie znają. Skomentuj to.

b. Czym jest bezpieczeństwo przez ukrycie i dlaczego jest złe?

STANDARDY SYSTEMU KRYPTOGRAFICZNEGO

Systemy kryptograficzne

Do niedawna głównym celem kryptografii była poufność. Jednak kryptografia dojrzała do tego stopnia, że organizacje wojskowe i biznesowe wiedzą, że szyfrowanie zapewniające poufność jest tylko jedną z kilku zabezpieczeń kryptograficznych potrzebnych w wymianie wiadomości. W praktyce zabezpieczenia te zapewnia system kryptograficzny, który jest pakietem kryptograficznych środków zaradczych do ochrony dialogów.

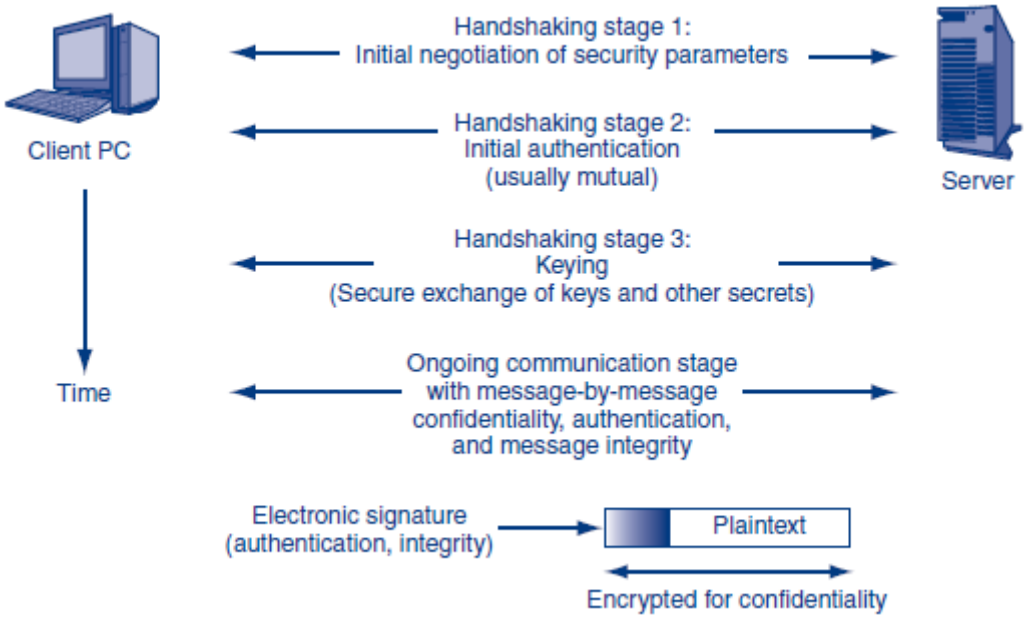
System kryptograficzny to pakiet kryptograficznych środków zaradczych do ochrony dialogów.

Gdy dwie strony komunikują się za pomocą systemu kryptograficznego, muszą użyć określonego standardu systemu kryptograficznego. Norma ta określa zarówno zabezpieczenia, które mają być zastosowane, jak i procesy matematyczne, które zostaną użyte do zapewnienia ochrony.

Popularne standardy systemów kryptograficznych obejmują SSL/TLS i IPsec.

Początkowe etapy uzgadniania

Kiedy dwie strony (urządzenia lub programy) zaczynają komunikować się za pośrednictwem standardu systemu kryptograficznego, przechodzą przez trzy etapy uzgadniania, jak pokazano na rysunku 3-8.



NEGOCJACJA

Prawie wszystkie standardy systemów kryptograficznych oferują wiele metod kryptograficznych do wykorzystania w komunikacji, a prawie wszystkie metody kryptograficzne mają wiele opcji. W związku z tym pierwszym etapem uzgadniania jest negocjowanie metod i opcji kryptograficznych do

wykorzystania w komunikacji. Określony zestaw opcji w SSL/TLS nazywa się zestawem szyfrów. Zanim dwie strony w połączeniu SSL/TLS zrobią cokolwiek innego, muszą wynegocjować określony zestaw szyfrów dla sesji komunikacyjnej. (Inne standardy systemów kryptograficznych używają różnych nazw dla kombinacji metod i opcji).

Zestaw szyfrów to określony zestaw opcji dla określonego standardu systemu kryptograficznego.

WSTĘPNE UWIERZYTELNIANIE

Drugim etapem uzgadniania jest wstępne uwierzytelnianie. Wiadomości mogą być wysyłane przez oszustów, więc zanim dwie strony rozpoczną komunikację, muszą się wzajemnie uwierzytelnić, czyli przetestować tożsamość partnera komunikacyjnego. Nazywa się to uwierzytelnianiem początkowym, ponieważ odbywa się przed rozpoczęciem komunikacji. Jak zauważono w dalszej części tej sekcji, może również następować kolejne uwierzytelnianie wiadomość po wiadomości dla każdej wiadomości wysyłanej przez dwie strony. Gdy obie strony uwierzytelniają się, jest to uwierzytelnianie wzajemne. Czasami jednak uwierzytelnianie jest wykonywane tylko przez jedną stronę. Na przykład, gdy logujesz się do serwera, musisz uwierzytelnić się na serwerze, ale serwer zazwyczaj nie uwierzytelnia się przed Tobą. Podczas uwierzytelniania partnerzy komunikacji udowadniają sobie nawzajem swoją tożsamość. Zwróć uwagę, że wstępne uwierzytelnianie odbywa się po etapie negocjacji. Powód tego jest bardzo prosty. Dopóki obie strony nie wynegocjują metod i opcji uwierzytelniania w ramach tych metod, nie mogą rozpocząć uwierzytelniania.

KLUCZ

Trzeci etap to kluczowanie. Jak wspomniano wcześniej, szyfry poufne wymagają kluczy. Jak zobaczymy później, uwierzytelnianie wymaga sekretów. Zarówno klucze, jak i sekrety są po prostu długimi ciągami bitów, które muszą być utrzymywane w tajemnicy między dwiema stronami. W większości przypadków klucze i klucze tajne muszą być przesyłane w bezpieczny sposób. Bezpieczne wysyłanie kluczy lub wpisów tajnych jest ogólnie nazywane kluczowaniem. W dalszej części tego rozdziału zobaczymy dwie metody kluczowania. Pamiętaj, że kluczowanie następuje po uwierzytelnieniu. Jest to konieczne, ponieważ wiele metod kluczowania jest podatnych na kradzież klucza przez osoby trzecie, chyba że najpierw zostanie przeprowadzone uwierzytelnienie.

Ciągła komunikacja

Po uwierzytelnieniu się obu stron i wymianie kluczy etapy uzgadniania dobiegają końca. Rozpoczyna się ciągła komunikacja i obie strony przesyłają wiele wiadomości tam i z powrotem. Obie strony zwykle stosują kilka kryptograficznych zabezpieczeń podczas bieżącej komunikacji na zasadzie komunikat po komunikacie.

• Najpierw nadawca dodaje podpis elektroniczny do każdej wiadomości. Dzięki temu odbiorca może uwierzytelnić każdą wiadomość. Uwierzytelnianie wiadomość po wiadomości udaremnia wysiłki oszustów, aby wstawić wiadomości do strumienia dialogów.

• Po drugie, wszystkie dobre technologie podpisu elektronicznego zapewniają również integralność wiadomości, co oznacza, że jeśli atakujący przechwyci i zmodyfikuje wiadomość (np. zmieniając saldo banku klienta), proces uwierzytelniania odrzuci wiadomość.

• Po trzecie, nadawca szyfruje połączoną wiadomość i podpis elektroniczny w celu zachowania poufności.

TEST LXVI

a. Rozróżnij systemy kryptograficzne i kryptograficzne.

b. Rozróżnij systemy kryptograficzne i standardy systemów kryptograficznych.

c. Dlaczego pierwszym etapem uścisku dłoni jest negocjowanie metod i opcji zabezpieczeń?

d. Kim jest oszust?

e. Co to jest uwierzytelnianie?

f. Co to jest uwierzytelnianie wzajemne?

g. Dlaczego potrzebna jest bezpieczna faza kluczowania?

a. Jakie trzy zabezpieczenia zapewniają systemy kryptograficzne dla poszczególnych wiadomości?

b. Co to jest podpis elektroniczny?

c. Jakie dwa zabezpieczenia zwykle zapewniają podpisy elektroniczne?

d. Rozróżnij etapy uścisku dłoni i bieżącą komunikację.

ETAP NEGOCJACJI

Przeszliśmy dość szybko przez cztery etapy związane z systemami kryptograficznymi. Teraz przejdziemy przez każdy z tych etapów bardziej szczegółowo, zaczynając od etapu negocjacji.

Opcje pakietu szyfrów

Jak omówiono wcześniej, zestaw szyfrów to określony zestaw metod i opcji zabezpieczeń dla określonego standardu systemu kryptograficznego (np. SSL/TLS). Zestaw szyfrów zawiera określony zestaw metod i opcji początkowego uwierzytelniania, wymiany kluczy oraz ciągłej poufności, uwierzytelniania i integralności wiadomości. Rysunek 3-9 przedstawia mały podzbiór opcjonalnych zestawów szyfrowania oferowanych przez popularne standardy SSL/TLS omówione w dalszej części.

Cipher Suite	Key Negotiation	Digital Signature Method	Symmetric Key Encryption Method	Hashing Method for HMAC	Strength
NULL_WITH_NULL_NULL	None	None	None	None	None
RSA_EXPORT_WITH_RC4_40_MD5	RSA export strength (40 bits)	RSA export strength (40 bits)	RC4 (40-bit key)	MD5	Weak
RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	SHA-1	Stronger but not very strong
DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie–Hellman	Digital signature standard	3DES_EDE_CBC	SHA-1	Strong
RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES 256 bits	SHA-256	Very strong

Są one pokazane w kolejności rosnącej siły kryptograficznej. Zobaczymy większość konkretnych metod kryptograficznych pokazanych na rysunku w dalszej części tego rozdziału oraz w innych rozdziałach.

Zasady pakietu szyfrów

Najsłabsze zestawy szyfrów w standardzie systemu kryptograficznego często zapewniają bardzo małą ochronę lub wcale. Na przykład pierwszy zestaw szyfrów na rysunku 9 nie zapewnia żadnego zabezpieczenia. Drugi używa tylko szyfrowania klasy eksportowej, więc chociaż jest silniejszy, nadal jest dość słaby. Ostatni zestaw szyfrów jest bardzo silny. Ze względu na duże zróżnicowanie siły zestawów szyfrowania SSL/TLS, firmy muszą opracować oparte na ryzyku zasady wyboru zestawów szyfrowania, zezwalając tylko na zestawy szyfrowania o odpowiedniej sile dla zagrożeń, przed którymi stoi aplikacja. Standard systemu kryptograficznego IPsec (omówiony w dalszej części tego rozdziału) umożliwia centralne ustalanie zasad dla metod i opcji zabezpieczeń oraz narzucanie tych zasad wszystkim partnerom komunikującym się.

TEST LXVII

a. Co to jest zestaw szyfrów w SSL/TLS?

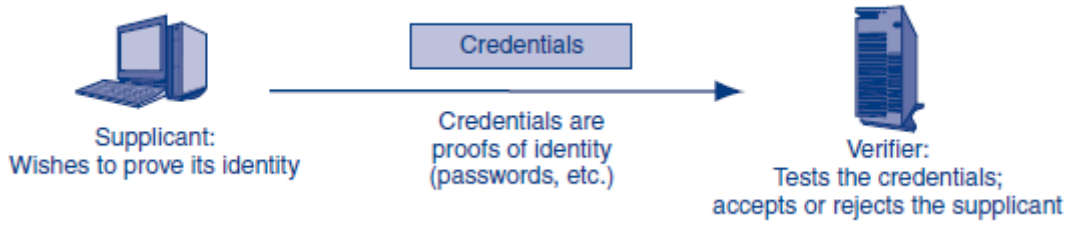
b. Dlaczego firmy chcą tworzyć zasady, które definiują metody i opcje zabezpieczeń dla określonej aplikacji, która jest używana między partnerami korporacyjnymi?

WSTĘPNY ETAP UWIERZYTELNIANIA

Po zakończeniu etapu negocjacji zabezpieczeń kolejnym etapem uzgadniania w nawiązywaniu dialogu systemu kryptograficznego jest uwierzytelnianie. Istnieje kilka początkowych metod uwierzytelniania. Przyjrzymy się tylko jednemu, MS-CHAP, który opiera się na uwierzytelnianiu hasłem na serwerach.

Terminologia uwierzytelniania

W uwierzytelnianiu strona próbująca udowodnić swoją tożsamość nazywana jest suplikantem. Drugą stroną jest weryfikator. Suplikant wysyła poświadczenia (dowody tożsamości) do weryfikatora.



We wzajemnym uwierzytelnianiu obie strony na zmianę są petentami i weryfikatorami.

TEST LXVIII

a. W uwierzytelnianiu rozróżnij suplikanta i weryfikatora.

b. Co to są poświadczenia?

c. Ilu petentów i weryfikatorów jest we wzajemnym uwierzytelnianiu między dwiema stronami? Wyjaśnij

Haszowanie

Kiedy większość ludzi myśli o kryptografii, skupiają się na szyfrowaniu. Jednak haszowanie jest również ważną częścią działania systemów kryptograficznych. Zanim rozważymy wstępne uwierzytelnianie MS-CHAP, musimy przyjrzeć się, jak działa haszowanie. Uproszczonym sposobem myślenia o haszowaniu jest traktowanie bitów wiadomości jako bardzo dużej liczby binarnej i podzielenie jej przez mniejszą liczbę. Reszta może być haszem. Na przykład, jeśli wiadomość ma numer 6457, a numer skrótu to 236, wartość skrótu zostanie umieszczona w wiadomości o numerze 27 razy z resztą 85. Ta reszta, 85, to skrót. Prawdziwe haszowanie jest bardziej złożone, ale ten przykład daje posmak haszowania. Po zastosowaniu mieszania do wiadomości binarnej wynik (nazywany skrótem) jest znacznie krótszy niż oryginalna wiadomość - zwykle ma długość od 128 do 512 bitów. W przeciwieństwie do tego, szyfrowanie tworzy tekst zaszyfrowany, który jest mniej więcej tak długi, jak tekst jawny. W przeciwieństwie do szyfrowania, które można odwrócić przez odszyfrowanie, haszowanie jest nieodwracalne. Nie ma algorytmu „dehashowania". Nie możesz zacząć od wiadomości składającej się z kilku tysięcy bitów, utworzyć hash kilkuset bitów i oczekiwać, że będziesz w stanie odzyskać całą oryginalną wiadomość. W poprzednim przykładzie, jeśli ktoś powie, że hash to 87, nie ma możliwości obliczenia, że oryginalna wartość wynosiła 6457. Innym sposobem na zapamiętanie nieodwracalności jest to, że nie można zamienić hamburgera z powrotem w krowę. Haszowanie jest również powtarzalne. Jeśli dwie różne osoby zastosują ten sam algorytm mieszający do tego samego ciągu bitów, zawsze otrzymają dokładnie ten sam skrót. Najpowszechniej obecnie stosowaną metodą haszowania jest prawdopodobnie MD5, która generuje skróty 128-bitowe. Ponadto istnieje rodzina wariantów Secure Hash Algorithm (SHA) o rosnącej sile, w tym SHA-1, SHA-224, SHA-256, SHA-384 i SHA-512. SHA-1 tworzy skrót o długości 160 bitów, podczas gdy inne wersje SHA mają w swoich nazwach długość skrótu (w bitach). Niestety, kryptoanalitycy odkryli ostatnio słabości zarówno w MD5, jak i SHA-1. Obecnie powinny być używane tylko silniejsze wersje SHA, a MD5 nie powinno być w ogóle używane.

TEST LXIX

a. W haszowaniu, czym jest hasz?

b. Czy szyfrowanie jest odwracalne?

c. Czy haszowanie jest odwracalne?

d. Czy haszowanie jest powtarzalne?

e. Czy po zastosowaniu algorytmu haszującego hash ma stałą czy zmienną długość?

f. Jaki jest rozmiar skrótu MD5?

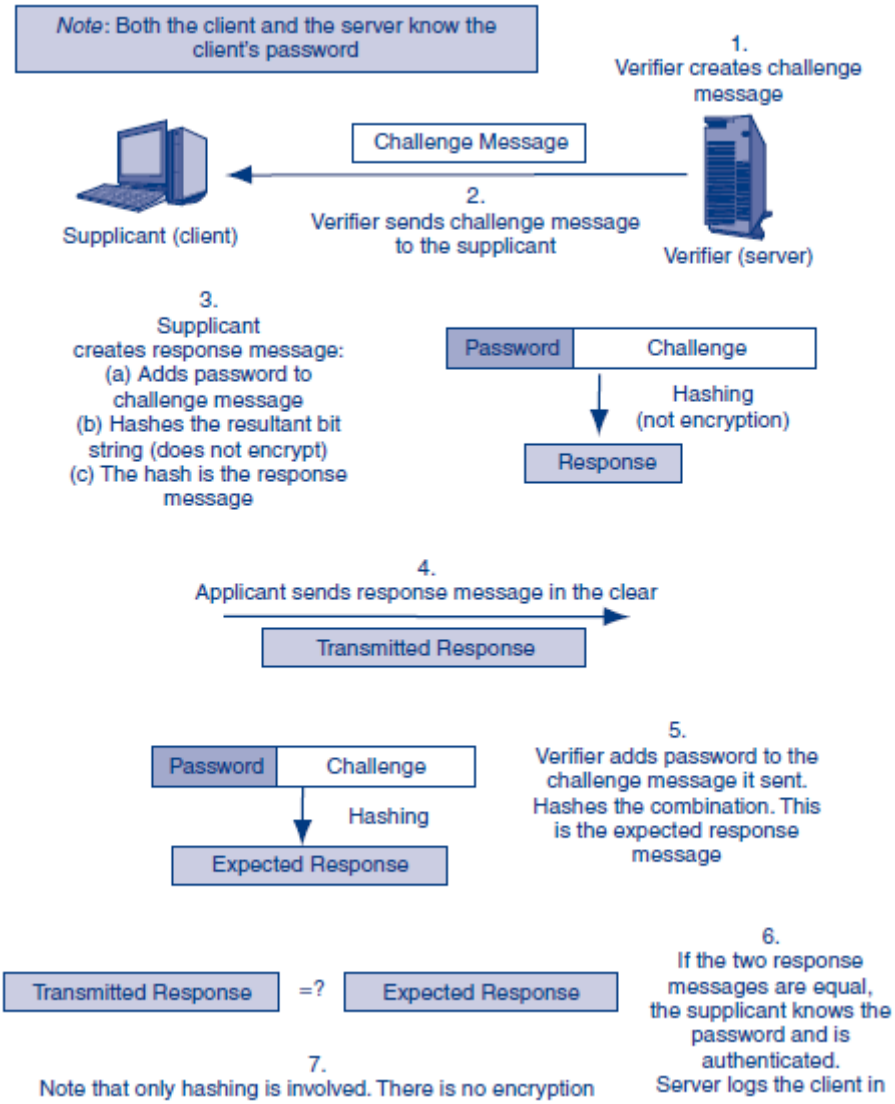
g. Jaki jest rozmiar skrótu SHA-1?

h. Jaki jest rozmiar skrótu SHA-256?

i. Które algorytmy mieszające nie powinny być używane, ponieważ zostały uznane za podatne na ataki?

Wstępne uwierzytelnianie za pomocą MS-CHAP

Przyjrzymy się jednej początkowej metodzie uwierzytelniania, MS-CHAP, która jest używana przez serwery do uwierzytelniania klientów za pomocą haseł wielokrotnego użytku. W przypadku uwierzytelniania hasłem ważne jest, aby nie wysyłać haseł w postaci jawnej, to znaczy bez ochrony kryptograficznej. Jeśli hasło zostanie wysłane w sposób jawny, osoba atakująca może je przechwycić i użyć hasła do późniejszego włamania się na konto użytkownika. Rysunek ilustruje protokół Microsoft Challenge–Handshake Authentication Protocol (MS-CHAP).



Protokół MS-CHAP jest powszechnie używany, gdy użytkownicy logują się do serwera z systemem operacyjnym Microsoft Windows Server. Hasło staje się wspólnym sekretem znanym zarówno suplikantowi (użytkownikowi), jak i weryfikatorowi (serwerowi). Wnioskodawca uwierzytelnia się, udowadniając, że zna hasło do konkretnego konta.

NA MASZYNIE WSKAZANEGO: HASHING

W protokole MS-CHAP serwer (1) wysyła do komputera petenta komunikat wezwania (2), który jest po prostu losowym ciągiem bitów. Serwer wysyła tę wiadomość w sposób jawny, bez szyfrowania dla zachowania poufności. Komputer wnioskodawcy dołącza następnie hasło wnioskodawcy do tej wiadomości prowokacyjnej, tworząc dłuższy strumień bitów. Komputer petenta następnie miesza ten strumień bitów, aby wygenerować komunikat odpowiedzi (3). Komputer petenta wysyła tę wiadomość odpowiedzi do serwera, ponownie w postaci jasnej (4).

NA SERWERZE WERYFIKATORA

Aby przetestować wiadomość odpowiedzi, serwer powtarza działania klienta. Serwer odbiera wiadomość wyzwanie wysłaną do użytkownika, dołącza hasło użytkownika, które również zna, i stosuje

ten sam algorytm haszujący, którego użył suplikant (5). (Przypomnij sobie, że haszowanie jest powtarzalne.) Jeżeli hash serwera jest identyczny z komunikatem odpowiedzi, to użytkownik musi znać hasło do konta (6). Serwer loguje się do uwierzytelnionego użytkownika.

TEST LXX

a. Czy protokół MS-CHAP jest używany do uwierzytelniania początkowego lub uwierzytelniania typu wiadomość po wiadomości?

b. W jaki sposób petent tworzy wiadomość z odpowiedzią?

c. Jak weryfikator sprawdza wiadomość odpowiedzi?

d. Jakiego rodzaju szyfrowania używa MS-CHAP? (To podchwytliwe pytanie, ale ważne).

e. Czy w MS-CHAP serwer uwierzytelnia się wobec klienta?

ETAP KLUCZY

Klucze sesji

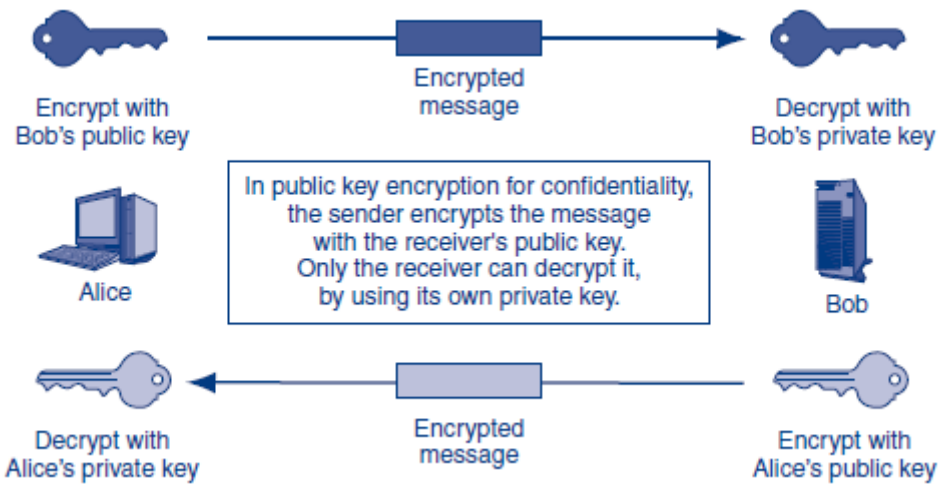
Po etapie uwierzytelniania obaj partnerzy muszą wymienić jeden lub więcej kluczy symetrycznych na poufne. Klucze te nazywane są kluczami sesji, ponieważ są używane tylko w jednej sesji komunikacyjnej. Jeśli obie strony ponownie się komunikują, wymienią się innym kluczem sesji. Przyjrzymy się dwóm metodom kluczowania, które są szeroko stosowane w organizacjach.

Szyfrowanie klucza publicznego w celu zachowania poufności

Jedna z tych metod kluczowania wykorzystuje szyfrowanie kluczem publicznym w celu zachowania poufności. Chociaż szyfrowanie kluczem symetrycznym dominuje w szyfrowaniu poufności, czasami do zachowania poufności używana jest inna rodzina szyfrów. Są to szyfry szyfrujące kluczem publicznym, zwane również szyframi szyfrującymi z kluczem asymetrycznym. Szyfrowanie kluczem publicznym może być używane w wymianie kluczy dla symetrycznych kluczy sesji (i innych sekretów).

DWA KLUCZE

W przypadku szyfrowania kluczem publicznym każda strona ma dwa klucze — klucz prywatny i klucz publiczny. Każda ze stron zachowuje swój klucz prywatny w tajemnicy, ale klucze publiczne mogą być poznane przez każdego bez stwarzania problemów. Rysunek pokazuje, w jaki sposób te dwa typy kluczy są używane do zachowania poufności.



PROCES

Na rysunku Alicja chce bezpiecznie wysłać wiadomość do Boba. Alicja szyfruje tekst jawny kluczem publicznym Boba. Po stronie odbierającej Bob odszyfrowuje zaszyfrowany tekst przy użyciu własnego klucza prywatnego. Zauważ, że nie możemy po prostu powiedzieć „klucz publiczny" i „klucz prywatny", ponieważ każda strona ma klucz publiczny i klucz prywatny. Należy również pamiętać, że nadawca szyfruje kluczem publicznym odbiorcy, który jest powszechnie znany, a odbiorca odszyfrowuje wiadomość swoim własnym kluczem prywatnym, który zna tylko on. Każdy może zaszyfrować wiadomość do strony za pomocą nietajnego klucza publicznego strony. Nie ma potrzeby wcześniejszej bezpiecznej wymiany kluczy, ponieważ istnieje szyfrowanie kluczem symetrycznym.

KŁÓDKA I ANALOGIA KLUCZY

Szyfrowanie kluczem publicznym może być mylące, gdy czytasz o tym po raz pierwszy. Użycie analogii „kłódka i klucz" może pomóc zilustrować wzajemne powiązania między kluczami publicznymi i prywatnymi. Bob idzie do ślusarza i zamawia tuzin kłódek (klucz publiczny Boba) wykonanych tylko z jednego unikalnego klucza (klucz prywatny Boba), który otworzy wszystkie kłódki. Bob następnie daje Alice odblokowane kłódki i zatrzymuje swój unikalny klucz. Alicja może użyć odblokowanych kłódek Boba (klucza publicznego Boba), aby zablokować (zaszyfrować) wiadomość w skrzynce. Nawet jeśli pudełko zostało przechwycone, nie można go otworzyć. Tylko Bob może otworzyć zamkniętą skrzynkę, ponieważ ma unikalny klucz (klucz prywatny Boba). W rzeczywistości Bob może przekazać swoje odblokowane kłódki (klucz publiczny Boba) każdemu, z kim chce się komunikować. Tylko Bob może otworzyć zamknięte kłódki swoim unikalnym kluczem prywatnym. Proces można odwrócić, jeśli Bob chciał wysłać wiadomości do Alicji. Każdy miałby własne kłódki (klucze publiczne), które mógłby swobodnie rozdawać. Mieliby również unikalny klucz (klucz prywatny), który zachowaliby w tajemnicy i używali go do odblokowywania (odszyfrowywania) własnych kłódek.

Analogia kłódki i klucza to intuicyjny sposób zrozumienia, jak działają klucze publiczne i prywatne, aby zapewnić poufność. Ta analogia załamie się, gdy omówimy użycie kluczy publicznych do uwierzytelniania (tj. do tworzenia podpisów cyfrowych) w dalszej części tego rozdziału. Jednak dla początkujących czytelników analogia jest przydatna w zrozumieniu idei działania kluczy publicznych i prywatnych.

WYSOKI KOSZT I KRÓTKIE DŁUGOŚCI WIADOMOŚCI

Szyfrowanie kluczem symetrycznym jest szybkie i niedrogie, ale wymaga bezpiecznej dystrybucji kluczy sesji. Szyfrowanie kluczem publicznym jest odwrotnością. Właśnie widzieliśmy, że w przypadku szyfrowania kluczem publicznym nie ma potrzeby tajnego rozpowszechniania kluczy przed szyfrowaniem w celu zachowania poufności. Nie jest konieczne wcześniejsze kluczowanie. Jest to bardzo pożądane. Jednak szyfry z kluczem publicznym są niezwykle złożone, a zatem powolne i drogie w użyciu. (Zazwyczaj szyfrowanie kluczem publicznym trwa od 100 do 1000 razy dłużej niż szyfrowanie kluczem symetrycznym w celu zaszyfrowania wiadomości o określonej długości). W związku z tym kryptografia wykorzystuje szyfrowanie kluczem publicznym tylko do szyfrowania bardzo krótkich wiadomości w celu zachowania poufności.

RPA I ECC

Istnieją tylko dwa powszechnie używane szyfry szyfrowania z kluczem publicznym. Pierwszym z nich jest szyfr RSA, który dominuje w szyfrowaniu klucza publicznego. Jednak coraz częściej stosowany jest bardziej wydajny szyfr z kluczem publicznym kryptografii krzywych eliptycznych (ECC).

DŁUGOŚĆ KLUCZA

Podczas gdy szyfrowanie kluczem symetrycznym opiera się na krótko używanych kluczach sesji, pary kluczy publiczny-prywatny są rzadko zmieniane. Na przykład, aby móc odbierać zaszyfrowane wiadomości, odbiorca musi chronić klucz prywatny przez tygodnie, miesiące, a nawet lata. Wraz ze wzrostem czasu użycia klucza zwiększa się natężenie ruchu, a także długość klucza dla danego stopnia bezpieczeństwa. Podczas gdy klucze sesji o długości 100 bitów są silne w szyfrowaniu kluczem symetrycznym, klucze publiczne muszą być znacznie dłuższe. W przypadku szyfrowania kluczem publicznym RSA zalecana minimalna długość klucza silnego wynosi 1024 bity. W przypadku bardziej wydajnego szyfrowania ECC klucze 512-bitowe zapewniają równoważną siłę. Dłuższa długość klucza wymaga dłuższego czasu przetwarzania podczas szyfrowania, a długa długość klucza jest jednym z powodów, dla których szyfrowanie kluczem publicznym jest tak powolne i kosztowne w implementacji.

TEST LXXI

a. Kiedy Alicja wyśle wiadomość do Boba, jakiego klucza użyje do zaszyfrowania wiadomości?

b. Dlaczego „klucz publiczny” nie jest dobrą odpowiedzią na pytanie 21?

c. Jakiego klucza użyje Bob do odszyfrowania wiadomości?

d. Dlaczego „klucz prywatny” nie jest dobrą odpowiedzią na pytanie 21b?

e. Ile będzie kluczy publicznych w klasie z 30 uczniami i nauczycielem?

f. Ile kluczy prywatnych?

a.Jaka jest główna wada szyfrowania kluczem publicznym?

b. Jaki jest najpopularniejszy szyfr szyfrujący kluczem publicznym?

c. Jaki jest inny powszechnie używany szyfr szyfrowania z kluczem publicznym?

d. Które muszą być dłuższe — klucze symetryczne czy klucze publiczne? Uzasadnij swoją odpowiedź.

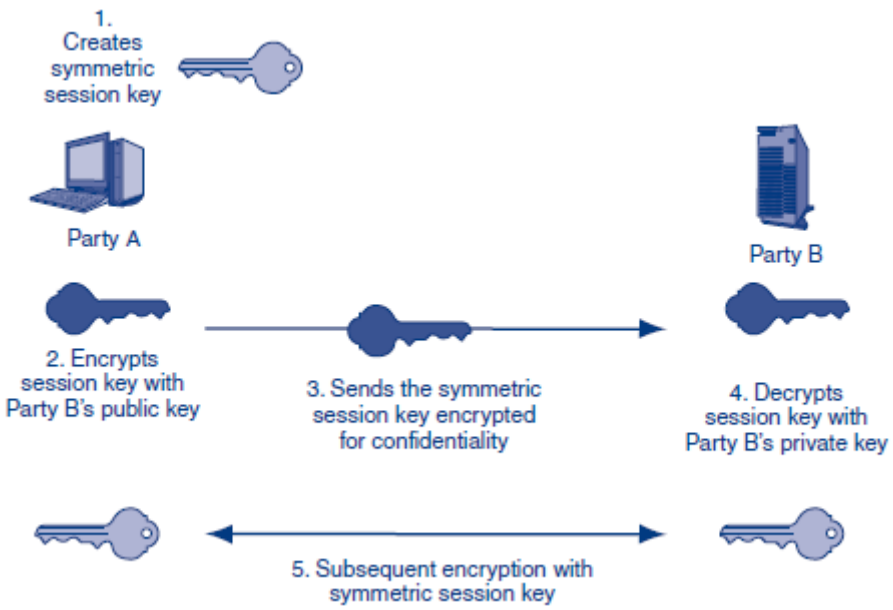
e. Jak długie są silne klucze RSA?

f. Jak długie są silne klucze ECC?

Julia szyfruje wiadomość do Davida za pomocą szyfrowania klucza publicznego w celu zachowania poufności. Czy po zaszyfrowaniu wiadomości Julia może ją odszyfrować?

Klucz symetryczny za pomocą szyfrowania klucza publicznego

Chociaż szyfrowanie kluczem publicznym i szyfrowanie kluczem symetrycznym mogą wydawać się rywalami, w rzeczywistości są one komplementarne. Na przykład szyfrowanie kluczem publicznym może bezpiecznie dostarczać symetryczne klucze sesji, jak pokazano na rysunku.



• Najpierw jedna strona (Strona A) generuje losowy ciąg bitów, który będzie używany jako symetryczny klucz sesji.

• Po drugie, Strona A szyfruje ten symetryczny klucz sesji kluczem publicznym drugiej strony (Strony B). Ponieważ ten klucz jest publiczny, nie ma potrzeby wcześniejszej dystrybucji klucza tajnego, ponieważ istnieje szyfrowanie kluczem symetrycznym dla zachowania poufności.

• Po trzecie, Strona A wysyła zaszyfrowany klucz sesji do Strony B.

• Po czwarte, Strona B odszyfrowuje zaszyfrowany klucz sesji za pomocą własnego klucza prywatnego Strony B. Może teraz odczytać oryginalny tekst jawny, który jest symetrycznym kluczem sesji wygenerowanym przez drugą stronę.

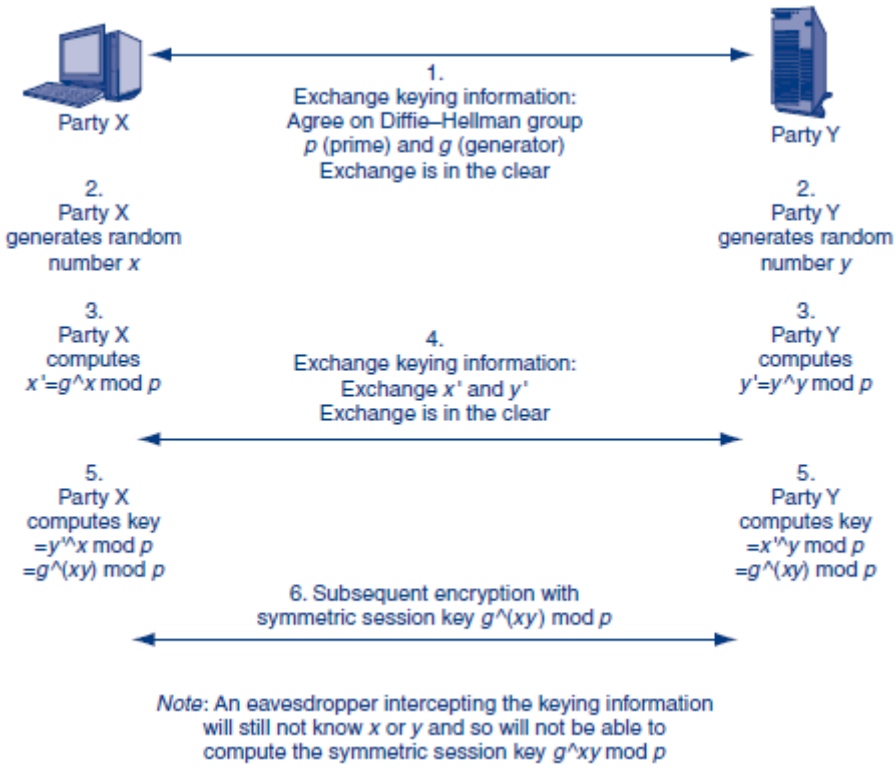
• Po piąte, teraz, gdy kluczowanie zostało zakończone, obie strony mają symetryczny klucz sesji i będą go używać do poufnego wysyłania wiadomości przy użyciu szyfrowania z kluczem symetrycznym.

TESY LXXII

Wyjaśnij, w jaki sposób szyfrowanie kluczem publicznym może ułatwić symetryczną wymianę kluczy sesji.

Kluczowanie symetryczne za pomocą klucza Diffie-Hellmana

Chociaż szyfrowanie kluczem publicznym jest szeroko rozpowszechnione, szyfrowanie kluczem publicznym jest bardzo powolne. Inna popularna metoda kluczowania, uzgadnianie klucza Diffie-Hellmana, jest znacznie szybsza. Ta technika została nazwana na cześć dwóch twórców szyfrowania z kluczem publicznym, którzy również stworzyli tę metodę kluczowania. Rysunek ilustruje pokrótce, jak uzgadnianie klucza Diffie-Hellmana wykonuje kluczowanie.



Rysunek pokazuje, że obie strony wymieniają informacje o kluczowaniu w pierwszych dwóch wymianach (kroki 1 i 4). Jeśli masz inklinacje matematyczne, możesz szczegółowo śledzić proces, ale my przyjrzymy się tylko najważniejszym momentom. Korzystając z tych informacji o kluczowaniu oraz informacji, których żadna strona nie transmituje (liczby losowe x i y), obie strony obliczają ten sam klucz symetryczny (gxy mod p). Następnie używają tego klucza jako klucza sesji do późniejszego szyfrowania kluczem symetrycznym (krok 6). Obie strony przesyłają swoje kluczowe informacje w sposób jasny. Jednak podsłuchujący nasłuchujący tych wymian nie może nauczyć się liczb losowych x i y, które Strony A i B generują, ale nie transmitują. W konsekwencji podsłuchujący nie może obliczyć klucza tylko przez odczytanie przesłanych informacji o kluczowaniu.

TEST LXXIII

a. Jaki jest cel umowy klucza Diffie-Hellman?

b. Czy osoba atakująca, która przechwytuje wymieniane informacje o kluczu, może obliczyć symetryczny klucz sesji?

UWIERZYTELNIANIE KOMUNIKAT PO KOMUNIKACIE

Po wymianie kluczy sesji przez dwie strony wstępny etap negocjacji zabezpieczeń jest zakończony. Następnie partnerzy zaczynają przesyłać wiele wiadomości tam i z powrotem na bieżącym etapie komunikacji.

Podpisy elektroniczne

W przypadku uwierzytelniania wiadomość po wiadomości, każda wiadomość musi zawierać podpis elektroniczny, jak wspomniano wcześniej. Ten podpis elektroniczny zapewnia zarówno uwierzytelnianie, jak i integralność wiadomości. Istnieją dwa popularne typy podpisów elektronicznych

– podpisy cyfrowe i kody uwierzytelniania wiadomości zakodowane kluczem (HMAC). Chociaż podpisy cyfrowe są szeroko omawiane w podręcznikach, w praktyce są one używane znacznie rzadziej niż HMAC.

Szyfrowanie kluczem publicznym do uwierzytelniania

Wcześniej widzieliśmy, że szyfrowanie kluczem publicznym może służyć do zachowania poufności. Strona wysyłająca szyfruje kluczem publicznym strony odbierającej. Odbiorca następnie odszyfrowuje przychodzący tekst zaszyfrowany swoim własnym kluczem prywatnym, który zna tylko ona. Przechwytujące w ogóle nie mogą odczytać wiadomości. Do uwierzytelniania można również użyć szyfrowania z kluczem publicznym. Wcześniej w tym rozdziale widzieliśmy, że suplikant w uwierzytelnianiu musi udowodnić swoją tożsamość, wysyłając poświadczenia do weryfikatora. Tylko jeśli te poświadczenia zostaną zweryfikowane jako należące do prawdziwej strony – osoby, za którą twierdzi, że jest petent – weryfikator zaakceptuje nadawcę jako prawdziwą stronę. (Biorąc pod uwagę możliwość podszywania się, petent może nie być prawdziwą stroną).

W uwierzytelnianiu prawdziwą stroną jest osoba, za którą podaje się petent.

W przypadku szyfrowania klucza publicznego w celu uwierzytelnienia, suplikant musi udowodnić, że wie coś, czego nikt inny nie powinien wiedzieć — klucz prywatny prawdziwej strony. Udowadniając, że zna klucz prywatny strony prawdziwej, petent może uwierzytelnić się jako strona prawdziwa. Aby to zrobić, suplikant szyfruje coś swoim kluczem prywatnym. Jeśli serwer może odszyfrować wynikowy szyfrogram za pomocą klucza publicznego strony prawdziwej, nadawca musi znać klucz prywatny strony prawdziwej, a zatem musi być stroną prawdziwą.

TEST LXXIV

a. W przypadku szyfrowania kluczem publicznym do uwierzytelniania, jakiego klucza używa suplikant do szyfrowania?

b. Czy weryfikator odszyfrowuje zaszyfrowany tekst za pomocą klucza publicznego petenta? (Jeśli nie, wyjaśnij, jakiego klucza używa.)

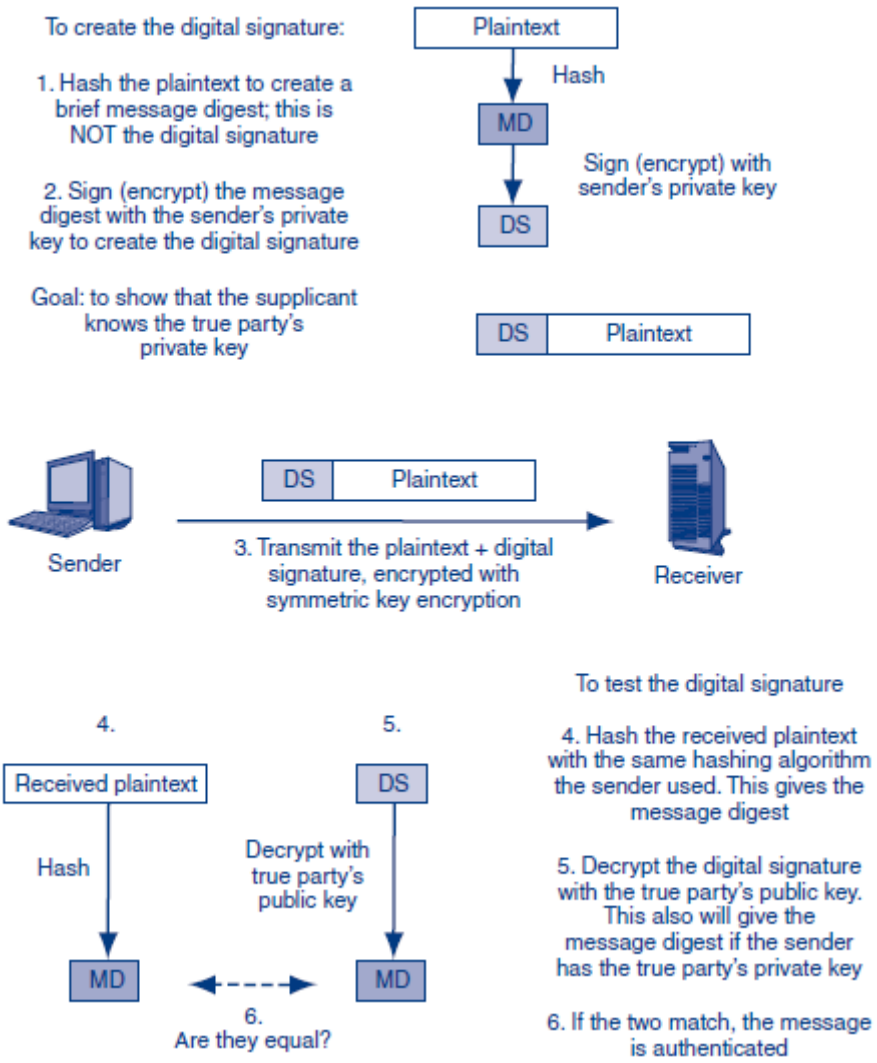
c. Kim jest prawdziwa impreza?

d. Co nadawca próbuje udowodnić, że wie, że powinna wiedzieć tylko prawdziwa strona?

Uwierzytelnianie wiadomość po wiadomości za pomocą podpisów cyfrowych

Szyfrowanie kluczem publicznym dla zachowania poufności jest używane w jednej wspólnej metodzie podpisu elektronicznego, podpisach cyfrowych.

Uwaga dla czytelnika: Zwolnij podczas czytania tej sekcji. Upewnij się, że rozumiesz ogólny przepływ na rysunku i dobrze rozumiesz każdy krok.



PODPISY CYFROWE

Rysunek pokazuje, jak utworzyć podpis cyfrowy, który uwierzytelnia pojedynczą wiadomość za pomocą szyfrowania klucza publicznego. Proces ten jest z grubsza analogiczny do sposobu, w jaki ludzkie podpisy uwierzytelniają dokumenty.

HASHING DO WYTWORZENIA PRZEGLĄDU WIADOMOŚCI

Pierwszym krokiem (1) w tworzeniu podpisu cyfrowego do uwierzytelniania jest zaszyfrowanie wiadomości w postaci zwykłego tekstu. Wynikowy skrót nazywa się skrótem wiadomości. Nadawca (który jest suplikantem) nie dodaje niczego do tekstu jawnego przed jego haszowaniem, jak to ma miejsce w MS-CHAP. Ten skrót jest wystarczająco krótki, aby można go było zaszyfrować za pomocą szyfrowania klucza publicznego.

PODPISANIE PRZEGLĄDU WIADOMOŚCI W CELU WYTWORZENIA PODPISU CYFROWEGO

W drugim kroku (2) nadawca szyfruje skrót wiadomości własnym kluczem prywatnym nadawcy. Zwróć uwagę, że nadawca użył własnego klucza prywatnego, a nie klucza publicznego odbiorcy. Ten krok tworzy podpis cyfrowy. Należy również zauważyć, że skrót wiadomości nie jest podpisem cyfrowym; służy tylko do tworzenia podpisu cyfrowego.

Zauważ, że skrót wiadomości nie jest podpisem cyfrowym; służy wyłącznie do składania podpisu cyfrowego,

Gdy strona szyfruje skrót wiadomości własnym kluczem prywatnym, nazywa się to podpisaniem skrótu wiadomości. Nadawca udowadnia swoją tożsamość jak osoba podpisująca list. Nadawca „podpisuje" skrót wiadomości swoim kluczem prywatnym, aby utworzyć podpis cyfrowy.

Podpisanie skrótu wiadomości oznacza zaszyfrowanie jej kluczem prywatnym nadawcy.

WYSYŁANIE WIADOMOŚCI Z POUFNOŚCIĄ

Trzecim krokiem (3) w wykorzystaniu podpisu cyfrowego do uwierzytelniania jest wysłanie wiadomości (Rysunek 3-16). Wiadomość, którą nadawca chce wysłać, składa się z oryginalnej wiadomości w postaci zwykłego tekstu oraz podpisu cyfrowego. Jeśli poufność nie stanowi problemu, nadawca może po prostu wysłać połączoną wiadomość w sposób jawny. Zwykle jednak poufność jest ważna, więc nadawca zwykle szyfruje połączenie oryginalnej wiadomości i podpisu cyfrowego dla zachowania poufności. Połączona wiadomość prawdopodobnie będzie długa, więc nadawca musi użyć szyfrowania kluczem symetrycznym. Z drugiej strony odbiorca (weryfikator) odszyfrowuje całą wiadomość za pomocą klucza symetrycznego używanego do zachowania poufności. Ponownie, ten krok ma na celu zachowanie poufności i nie ma nic wspólnego z uwierzytelnianiem.

WERYFIKACJA WNIOSKODAWCY

Ponownie, prawdziwą stroną jest osoba (lub proces oprogramowania), za którą podaje się petent. Jeśli nadawca jest prawdziwą stroną, nadawca zostanie uwierzytelniony. W przeciwnym razie nadawca jest oszustem i nie powinien być uwierzytelniany. W kroku czwartym (4) weryfikator haszuje oryginalną wiadomość w postaci zwykłego tekstu za pomocą tego samego algorytmu haszującego, którego użył suplikant. Powinno to spowodować podsumowanie wiadomości. W kroku piątym (5) rozpoczyna się proces weryfikacji, a odbiorca najpierw odszyfrowuje podpis cyfrowy za pomocą powszechnie znanego klucza publicznego prawdziwej strony. Spowoduje to wygenerowanie oryginalnego podsumowania wiadomości, jeśli suplikant/nadawca podpisał podsumowanie wiadomości kluczem prywatnym prawdziwej strony. Zauważ ponownie, że weryfikacja wymaga znajomości klucza publicznego prawdziwej strony. Zazwyczaj nadawca jest prawdziwą stroną. Jednak nadawca może być oszustem. Dlatego weryfikator nie używa klucza publicznego od nadawcy. Zamiast tego uzyskuje klucz publiczny z zaufanego źródła zwanego urzędem certyfikacji. Urzędy certyfikacji zostały omówione w następnej sekcji. Na koniec w kroku szóstym (6) porównywane są skróty wiadomości. Jeśli skróty wiadomości wygenerowane na te dwa różne sposoby (pokazane w krokach 4 i 5) są zgodne, nadawca musi mieć klucz prywatny strony prawdziwej, który tylko strona prawdziwa powinna znać. Wiadomość jest uwierzytelniana jako pochodząca od prawdziwej strony.

INTEGRALNOŚĆ KOMUNIKATU

Jeśli ktoś zmienił przesyłaną wiadomość, dwa skróty wiadomości nie będą pasować. Dlatego podpisy cyfrowe zapewniają również integralność wiadomości — możliwość odrzucenia zmienionej wiadomości. Wszystkie rzeczywiste metody uwierzytelniania wiadomość po wiadomości zapewniają integralność wiadomości jako produkt uboczny.

SZYFROWANIE KLUCZY PUBLICZNYCH W CELU POUFNOŚCI I UWIERZYTELNIANIA

W tym rozdziale zobaczyliśmy, że szyfrowanie kluczem publicznym jest używane zarówno do zachowania poufności, jak i uwierzytelniania. Częstym źródłem nieporozumień dla uczniów jest to, że

szyfrowanie kluczem publicznym wykorzystuje różne klucze do tych dwóch celów. Rysunek 3-17 ilustruje te różnice.

W przypadku szyfrowania kluczem publicznym w celu zachowania poufności nadawca szyfruje kluczem publicznym odbiorcy. Odbiorca odszyfrowuje kluczem prywatnym odbiorcy, który zna tylko odbiorca.

Encryption Goal	Sender Encrypts with	Receiver Decrypts with
Public key encryption for confidentiality	The receiver's public key	The receiver's private key
Public key encryption for authentication	The sender's private key	The True Party's public key (not the sender's public key)

W przypadku szyfrowania kluczem publicznym w celu zachowania poufności nadawca szyfruje kluczem publicznym odbiorcy. Odbiorca odszyfrowuje kluczem prywatnym odbiorcy, który zna tylko odbiorca. Jednak w przypadku szyfrowania klucza publicznego w celu uwierzytelnienia nadawca (suplikant) próbuje udowodnić, że zna tajny klucz prywatny prawdziwej strony. Nadawca szyfruje wiadomość własnym kluczem prywatnym. Odbiorca (weryfikator) następnie odszyfrowuje wiadomość za pomocą klucza publicznego prawdziwej strony. Zauważ ponownie, że weryfikator nie używa klucza publicznego nadawcy do odszyfrowania wiadomości, ponieważ nadawca może być oszustem.

TEST LXXV

a. W przypadku uwierzytelniania klucza publicznego, co musi wiedzieć nadawca, czego oszust nie powinien być w stanie się dowiedzieć?

b. Do jakiego rodzaju uwierzytelniania używany jest podpis cyfrowy — uwierzytelnianie wstępne czy uwierzytelnianie typu wiadomość po wiadomości?

c. W jaki sposób petent tworzy skrót wiadomości?

d. W jaki sposób petent tworzy podpis cyfrowy?

e. Czym jest „podpisywanie” w szyfrowaniu z kluczem publicznym?

f. Jaką łączną wiadomość wysyła petent?

g. W jaki sposób połączona wiadomość jest szyfrowana w celu zachowania poufności?

h. Jak weryfikator sprawdza podpis cyfrowy?

i. Czy weryfikator używa klucza publicznego nadawcy czy klucza publicznego prawdziwej strony do testowania podpisu cyfrowego?

a. Jakie korzyści w zakresie bezpieczeństwa zapewnia podpis cyfrowy oprócz uwierzytelniania?

b. Wyjaśnij, co oznacza ta korzyść.

c. Czy większość metod uwierzytelniania wiadomość po wiadomości zapewnia integralność wiadomości jako produkt uboczny?

a. Porównaj klucz, którego nadawca używa do szyfrowania, z szyfrowaniem kluczem publicznym w celu zachowania poufności i szyfrowaniem z kluczem publicznym w celu uwierzytelniania.

b. Porównaj klucz, którego odbiorca używa do odszyfrowania w szyfrowaniu kluczem publicznym w celu zachowania poufności i szyfrowaniu kluczem publicznym w celu uwierzytelniania. (Ostrożny!)

Certyfikaty cyfrowe

ORGANY CERTYFIKUJĄCE

Klucze publiczne nie są tajne, ale musisz uzyskać klucz publiczny prawdziwej strony z zaufanego źródła, jeśli chcesz go bezpiecznie używać podczas uwierzytelniania. Źródłem zwykle jest urząd certyfikacji (CA)28, który jest niezależnym i zaufanym źródłem informacji o kluczach publicznych prawdziwych stron. Niestety, niewiele krajów reguluje urzędy certyfikacji, więc weryfikator musi akceptować tylko certyfikaty cyfrowe od urzędów certyfikacji, którym ufa pod względem reputacji. Niektóre znane urzędy certyfikacji to między innymi VeriSign (47,5% udziału w rynku), Go Daddy (23,4%), Comodo (15,4%) i Network Solutions (2,5%).29 W rzeczywistości korporacje mogą wystawiać własne certyfikaty cyfrowe do użytku wewnętrznego. Microsoft Windows Server® 2008 posiada możliwość wystawiania i zarządzania certyfikatami cyfrowymi. Nawiasem mówiąc, powszechnym błędnym przekonaniem jest to, że urzędy certyfikacji ręczą za uczciwość strony wymienionej w certyfikacie. Oni nie! Poręczają jedynie za klucz publiczny wymienionej strony. Chociaż certyfikaty klientów, którzy zachowują się niewłaściwie, mogą zostać unieważnione, urzędy certyfikacji rzadko dają silne gwarancje wiarygodności posiadaczy certyfikatów. To nie jest ich praca. Ich zadaniem jest powiązanie klucza publicznego z nazwą.

Gdy urząd certyfikacji wydaje certyfikat cyfrowy osobie lub organizacji, nie oznacza to, że urząd ten ręczy za uczciwość strony wymienionej w certyfikacie. Twierdzi jedynie, że dana strona ma określony klucz publiczny.

CERTYFIKAT CYFROWY

CA wyśle weryfikatorowi certyfikat cyfrowy. Certyfikaty cyfrowe są zgodne ze składnią X.509. Certyfikat cyfrowy zawiera szereg pól, które pokazano na rysunku.

Field	Description
Version Number	Version number of the X.509 standard. Most certificates follow Version 3. Different versions have different fields. This figure reflects the Version 3 standard.
Issuer	Name of the certificate authority (CA).
Serial Number	Unique serial number for the certificate, set by the CA.
Subject	The name of the person, organization, computer, or program to which the certificate has been issued. This is the true party.
Public Key	The public key of the subject (the true party).
Public Key Algorithm	The algorithm the subject uses to sign messages with digital signatures.
Valid Period	The period before which and after which the certificate should not be used. ***Note:*** Certificate may be revoked before the end of this period.
Digital Signature	The digital signature of the certificate, signed by the CA with the CA's own private key. For testing certificate authentication and integrity. User must know the CA's public key independently.
Signature Algorithm Identifier	The digital signature algorithm the CA uses to sign its certificates.
Other Fields	…

Co najważniejsze, certyfikat cyfrowy zawiera nazwę strony prawdziwej (w polu Temat) oraz klucz publiczny strony prawdziwej (w polu Klucz publiczny). Weryfikator wyszukuje certyfikat cyfrowy

prawdziwej strony, a następnie używa tego klucza publicznego w certyfikacie cyfrowym do przetestowania podpisu cyfrowego suplikanta.

WERYFIKACJA CERTYFIKATU CYFROWEGO

Skąd weryfikator wie, że certyfikat cyfrowy jest legalny? Odpowiedź brzmi, że weryfikator musi wykonać trzy kroki. Testowanie własnego podpisu cyfrowego certyfikatu. Najpierw weryfikator musi sprawdzić, czy certyfikat cyfrowy jest autentyczny i nie został zmodyfikowany. Każdy certyfikat cyfrowy zawiera swój własny podpis cyfrowy, który jest podpisany przez urząd certyfikacji kluczem prywatnym CA. Weryfikator może użyć dobrze znanego klucza publicznego urzędu certyfikacji, aby przetestować podpis cyfrowy certyfikatu cyfrowego. Jeśli test działa, certyfikat cyfrowy musi być autentyczny i niezmodyfikowany. Wszystkie przeglądarki mają wbudowane listy kluczy publicznych popularnych urzędów certyfikacji .

Testowanie podpisu cyfrowego

Certyfikat cyfrowy posiada własny podpis cyfrowy

Podpisany kluczem prywatnym urzędu certyfikacji

Musi być przetestowany za pomocą dobrze znanego klucza publicznego urzędu certyfikacji

Jeśli test działa, certyfikat jest autentyczny i niezmodyfikowany

Sprawdzanie okresu ważności

Certyfikat jest ważny tylko w okresie ważności certyfikatu cyfrowego

Sprawdzanie odwołania

Certyfikaty mogą zostać unieważnione z powodu niewłaściwego zachowania lub z innych powodów Unieważnienie musi zostać przetestowane

Weryfikator może pobrać całą listę unieważnionych certyfikatów z urzędu certyfikacji

Sprawdź, czy numer seryjny znajduje się na liście unieważnionych certyfikatów

Jeśli tak, nie akceptuj certyfikatu

Lub weryfikator może wysłać zapytanie do urzędu certyfikacji

Wymaga, aby urząd certyfikacji obsługiwał protokół stanu certyfikatu online

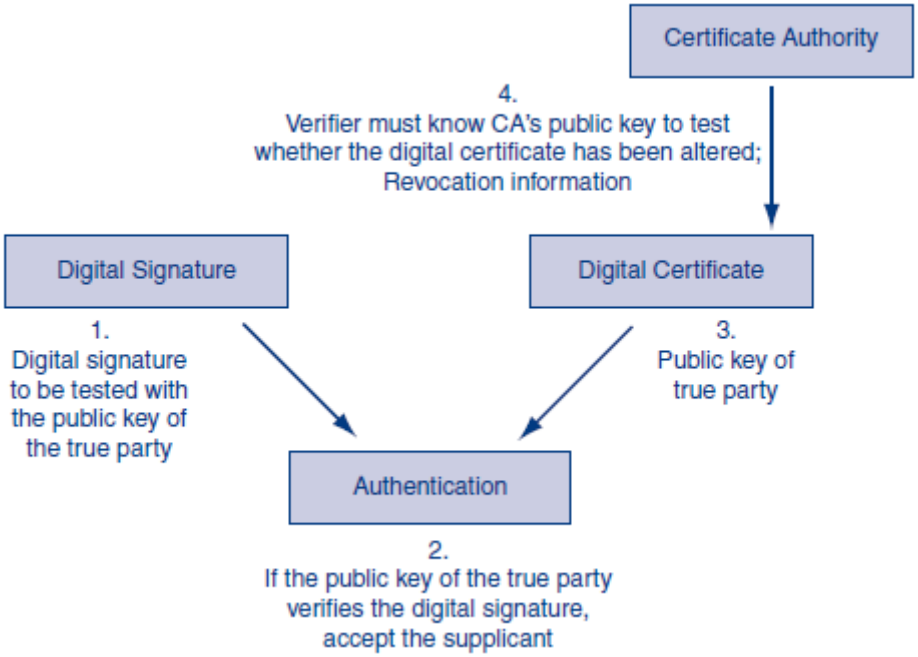
Ważny okres. Po drugie, każdy certyfikat cyfrowy ma daty, przed którymi i po których jest nieważny. Odbiorca musi sprawdzić, czy certyfikat cyfrowy jest w swoim okresie ważności.

Sprawdzanie odwołania. Po trzecie, nawet w okresie ważności certyfikatu cyfrowego urząd certyfikacji może unieważnić certyfikat cyfrowy, na przykład w przypadku niewłaściwego zachowania podmiotu certyfikatu. Odbiorcy nie powinni akceptować unieważnionych certyfikatów. Aby sprawdzić unieważnienie, weryfikator może pobrać listę unieważnionych certyfikatów urzędu certyfikacji. Jeśli numer seryjny certyfikatu znajduje się na liście, urząd certyfikacji unieważnił certyfikat cyfrowy. Chociaż pobieranie list odwołania certyfikatów działa, listy odwołania dużych urzędów certyfikacji są dość długie. Pobranie i sprawdzenie długiej listy unieważnionych certyfikatów może znacznie opóźnić rozpoczęcie komunikacji. Na szczęście większość urzędów certyfikacji oferuje bardziej uproszczony sposób sprawdzania odwołań. To jest protokół stanu certyfikatu online. Korzystając z tego protokołu, program może po prostu wysłać numer seryjny certyfikatu cyfrowego do urzędu certyfikacji. Urząd

certyfikacji odeśle odpowiedź informującą, czy numer seryjny jest prawidłowy, unieważniony lub nieznany.

ROLA CERTYFIKATU CYFROWEGO I PODPISU CYFROWEGO

Należy zauważyć, że certyfikat cyfrowy sam w sobie nie uwierzytelnia suplikanta. Jak pokazuje Rysunek, certyfikaty dostarczają jedynie klucz publiczny prawdziwej strony, który weryfikator może użyć do przeprowadzenia uwierzytelnienia. Każdy może posiadać certyfikat cyfrowy strony prawdziwej, nie będąc stroną prawdziwą, więc samo posiadanie certyfikatu cyfrowego nie uwierzytelnia osoby lub procesu posiadającego certyfikat. Podobnie w przypadku samego podpisu cyfrowego weryfikator nie ma sprawdzonego sposobu poznania klucza publicznego prawdziwej strony. Dlatego samego podpisu cyfrowego nie można przetestować, a zatem nie uwierzytelnia wnioskodawcy.



Ogólnie rzecz biorąc, certyfikaty cyfrowe i podpisy cyfrowe muszą być używane razem w uwierzytelnianiu klucza publicznego. Ani sam z siebie nie zapewnia uwierzytelniania. W szczególności certyfikat cyfrowy zapewnia klucz publiczny, którego używają metody uwierzytelniania (takie jak podpisy cyfrowe) do uwierzytelniania wnioskodawcy.

Certyfikat cyfrowy zapewnia klucz publiczny, którego używają metody uwierzytelniania (takie jak podpisy cyfrowe) do uwierzytelniania wnioskodawcy.

TEST LXXVI

a. Od jakiej organizacji weryfikator może otrzymać certyfikaty cyfrowe?

b. Czy większość urzędów certyfikacji podlega regulacjom?

c. Czy certyfikat cyfrowy wskazuje, że osoba lub firma wymieniona w certyfikacie jest godna zaufania? Wyjaśnij.

a. Jakie są dwa najbardziej krytyczne pola w certyfikacie cyfrowym?

b. Jakie pole w certyfikacie cyfrowym umożliwia odbiorcy certyfikatu stwierdzenie, czy certyfikat został zmieniony?

c. Jakie trzy rzeczy musi sprawdzić odbiorca certyfikatu cyfrowego, aby upewnić się, że certyfikat cyfrowy jest ważny?

d. Jakie są dwa sposoby sprawdzenia statusu unieważnienia certyfikatu?

a. Czy podpis cyfrowy sam w sobie zapewnia uwierzytelnianie? Wyjaśnij, dlaczego lub dlaczego nie.

b. Czy certyfikat cyfrowy sam w sobie zapewnia uwierzytelnianie? Wyjaśnij, dlaczego lub dlaczego nie.

c. W jaki sposób podpisy cyfrowe i certyfikaty cyfrowe są używane razem podczas uwierzytelniania?

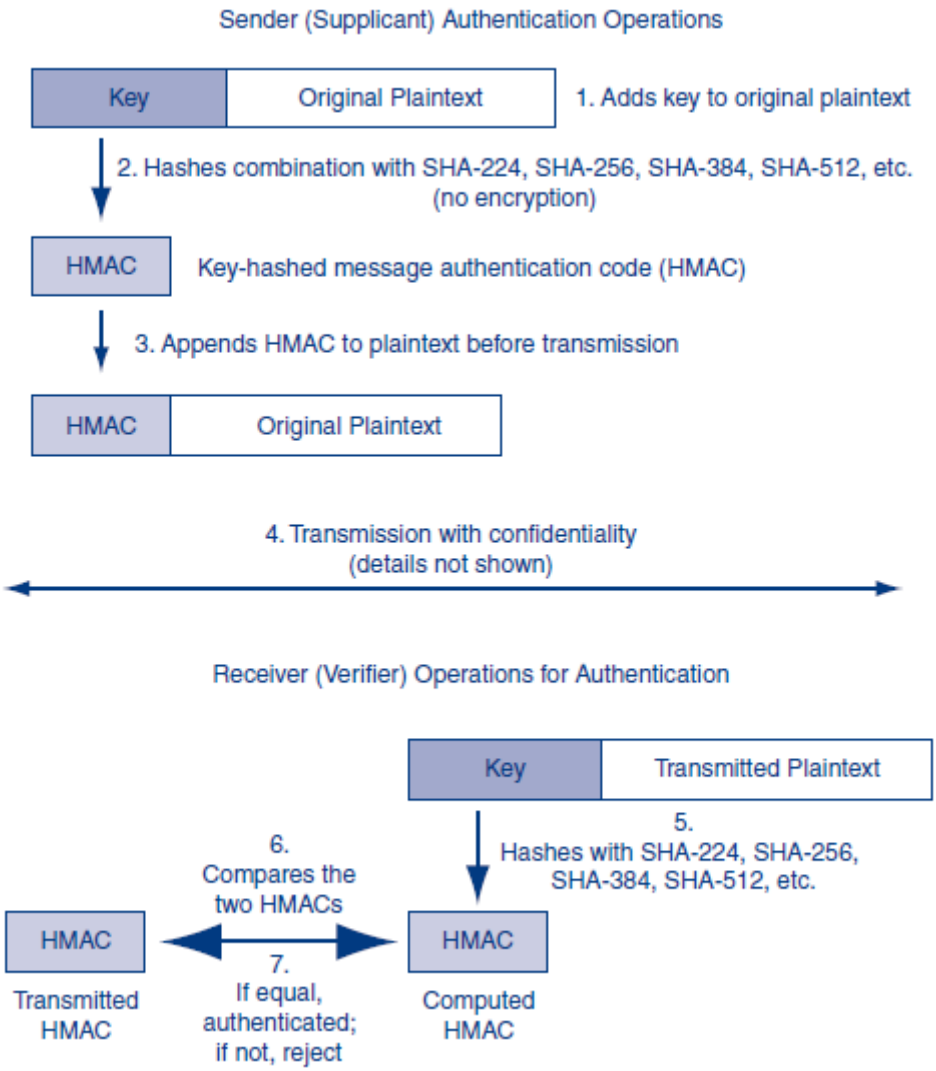
Kody uwierzytelniania wiadomości zaszyfrowanych kluczem (HMAC)

PROBLEM Z PODPISAMI CYFROWYMI

Właśnie widzieliśmy, jak podpisy cyfrowe zapewniają uwierzytelnianie wiadomość po wiadomości i integralność wiadomości. Niestety, chociaż podpisy cyfrowe zapewniają bardzo silne zabezpieczenia, zużywają również dużą moc obliczeniową. Ponadto utworzenie infrastruktury klucza publicznego do dystrybucji kluczy prywatnych i certyfikatów cyfrowych jest niezwykle trudne i kosztowne. W konsekwencji systemy kryptograficzne zwykle wykorzystują inną technikę uwierzytelniania wiadomości po wiadomości i integralności wiadomości. Jest to kod uwierzytelniania wiadomości zaszyfrowany kluczem (HMAC).

Tworzenie i testowanie HMAC

HMAC wykorzystuje klucz wymieniany podczas początkowej fazy negocjacji. Jednak nie używa tego klucza do szyfrowania kluczem symetrycznym. Raczej, jak pokazano na rysunku 3-22, nadawca dodaje klucz do każdej wiadomości wychodzącej (1), a następnie haszuje połączoną wiadomość i klucz (2).



Ten skrót to kod uwierzytelniania metody z kluczem skrótu (HMAC). Nadawca dodaje kod HMAC do wiadomości (3), a następnie szyfruje ten połączony strumień bitów za pomocą szyfrowania kluczem symetrycznym (4). Odbiornik odszyfrowuje przesyłany ciąg bitów w celu zachowania poufności. Następnie testuje HMAC. Robi to, dodając klucz (który również zna) do wiadomości, a następnie mieszając połączoną wiadomość i klucz za pomocą tego samego algorytmu mieszającego, którego użył nadawca (5). Ten obliczony HMAC powinien być zgodny z przesłanym HMAC (6). Jeśli tak, nadawca jest uwierzytelniany (7). Podobnie jak podpisy cyfrowe, HMAC zapewniają również integralność wiadomości. Haszowanie jest znacznie szybsze, a przez to tańsze niż szyfrowanie kluczem publicznym. Jest to bardzo ważne, biorąc pod uwagę dużą liczbę wiadomości wymienianych podczas sesji. Ponadto nie jest wymagany certyfikat cyfrowy. W związku z tym HMAC są używane znacznie częściej niż podpisy cyfrowe do uwierzytelniania i integralności wiadomości po wiadomości w systemach kryptograficznych.

TEST LXXVII

a. Jakie dwie ochrony kryptograficzne zapewnia HMAC?

b. Czy HMAC używają szyfrowania kluczem symetrycznym, szyfrowania kluczem publicznym lub haszowania?

c. Jaka jest przewaga HMAC nad podpisami cyfrowymi?

Niezaprzeczalność

Chociaż HMAC są bardzo szybkie i zużywają mało mocy obliczeniowej, mają jedno ograniczenie, które czasami jest poważne. Jednym z możliwych celów podpisów elektronicznych jest niezaprzeczalność, co oznacza, że nadawca nie może wysłać ważnej wiadomości, takiej jak umowa, a później twierdzić, że jej nie wysłał. HMAC nie zapewniają niezaprzeczalności, ponieważ zarówno nadawca, jak i odbiorca znają tajny klucz. W konsekwencji domniemany nadawca mógł argumentować w sądzie, że odbiorca mógł sfałszować HMAC w wiadomości; więc HMAC nie udowodnił, że nadawca faktycznie go wysłał. Natomiast podpisy cyfrowe dają niezaprzeczalność. Żaden oszust, w tym odbiorca, nie może utworzyć wiadomości z ważnym podpisem cyfrowym, ponieważ tylko prawdziwa strona powinna znać swój klucz prywatny. Jeśli do utworzenia podpisu cyfrowego zostanie użyty klucz prywatny strony prawdziwej, wiadomość mogła wysłać tylko strona prawdziwa. (Oczywiście ten mechanizm załamuje się, jeśli prawdziwa strona nie chroni swojego klucza prywatnego.) Praktycznym sposobem na pokonanie ograniczeń HMAC jest użycie ich do uwierzytelniania pojedynczych pakietów w warstwie internetowej. Następnie w dokumencie aplikacji można zastosować uwierzytelnianie kluczem publicznym. W ten sposób, chociaż pojedynczy pakiet może zostać odrzucony, dokument wniosku, taki jak umowa, nie może zostać odrzucony.

TEST LXXVIII

a. Dlaczego HMAC nie mogą zapewnić niezaprzeczalności?

b. Dlaczego zwykle nie jest problemem to, że HMAC nie zapewniają niezaprzeczalności?

BEZPIECZEŃSTWO KWANTOWE

Na poziomie cząstek elementarnych fizyka staje się niewiarygodnie złożona, a nawet dziwna. Jednocześnie mechanika kwantowa, która rządzi oddziaływaniami na małą skalę, może być wykorzystywana do wykonywania działań niemożliwych na poziomie normalnych urządzeń i obwodów. Różnice te mają dwie ważne implikacje dla bezpieczeństwo. Po pierwsze, widzieliśmy kluczowanie przy użyciu umowy klucza Diffie-Hellmana i szyfrowania klucza publicznego w celu zapewnienia poufności. Mechanika kwantowa oferuje nową metodę, dystrybucję kluczy kwantowych, która może dostarczyć niezwykle długie klucze do partnerów komunikacyjnych. Przy tak długich kluczach tradycyjne formy łamania kluczy stają się bezużyteczne. Dystrybucja klucza kwantowego tworzy jednorazowy klucz, który jest tak długi, jak cała wiadomość. Wiadomość zaszyfrowana jednorazowym kluczem tak długim jak sama nie jest podatna na kryptoanalizę.

W wiadomościach

Norwescy naukowcy z Uniwersytetu Nauki i Technologii w Trondheim odkryli technologiczną słabość w komercyjnym sprzęcie, który jest powszechnie używany w kwantowych systemach kryptograficznych. Badaczom udało się użyć lasera o mocy 1 miliwata do tymczasowego zaślepienia jednej strony bezpiecznej komunikacji i uzyskania klucza szyfrującego bez zakłócania działania systemu. Przed opublikowaniem wyników swoich eksperymentów naukowcy powiadomili producentów sprzętu o słabości, aby system mógł zostać załatany. Jeden z producentów, ID Quantique, powiedział, że komercyjne systemy sprzedawane korporacjom oprócz kryptografii kwantowej wykorzystują tradycyjne zabezpieczenia kryptograficzne.

Mechanika kwantowa

Opisuje zachowanie cząstek elementarnych

Złożone, a nawet dziwne wyniki

Dystrybucja kluczy kwantowych

Przesyła bardzo długi klucz tak długo, jak wiadomość

To jest klucz jednorazowy

Jednorazowy klucz, o ile wiadomość nie może zostać złamana przez kryptoanalizę

Jeśli przechwytujący odczyta część klucza w tranzycie, będzie to natychmiast widoczne

Łamanie kluczy kwantowych

Testuje wiele klawiszy jednocześnie

Jeśli stanie się zdolny do pracy na długich kluczach, dzisiejsze mocne klucze nie zapewnią żadnej ochrony

Ponadto, jeśli podsłuchujący próbuje przechwycić informacje o kluczu, działanie to będzie natychmiast widoczne, a dwie legalne strony odrzucą złamany klucz zamiast go używać. Produkty do dystrybucji kluczy kwantowych już istnieją, ale tradycyjne metody kluczowania są wystarczające dla prawie wszystkich zastosowań. Po drugie, kwantowe łamanie kluczy może być wykorzystane do szybkiego złamania kluczy, próbując dziesiątki, setki lub potencjalnie tysiące kluczy naraz. Obecnie komputery kwantowe mogą łamać tylko klucze o długości kilku bitów, ale jeśli komputery kwantowe staną się znacznie bardziej wydajne, wiele tradycyjnych metod kryptograficznych nie będzie już bezpiecznych, a długości kluczy uważane są obecnie za silne.

TEST LXXX

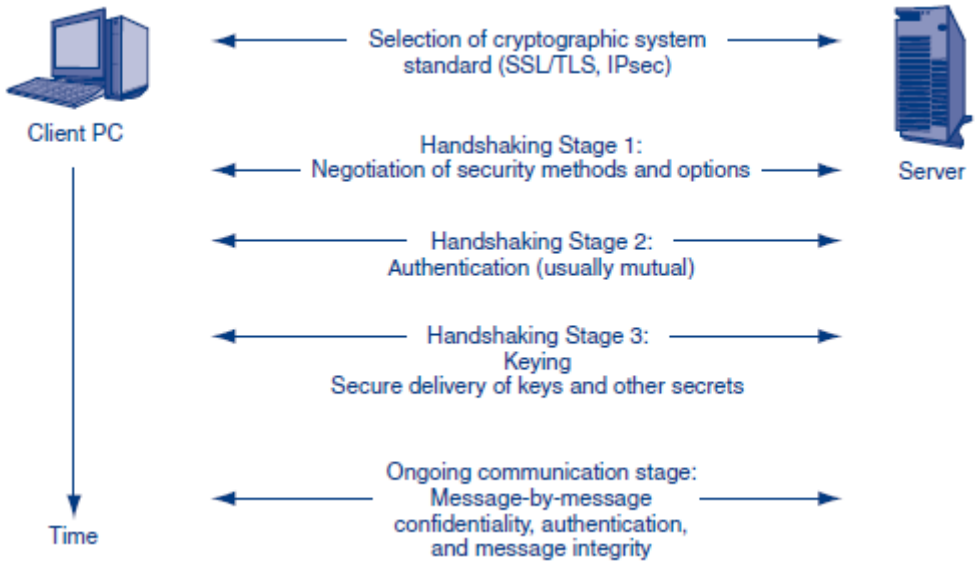
a. Co to jest dystrybucja klucza kwantowego?

b. Jakie są dwie zalety dystrybucji kluczy kwantowych?

c. Dlaczego łamanie klucza kwantowego stanowi poważne zagrożenie dla wielu tradycyjnych metod kryptograficznych?

SYSTEMY KRYPTOGRAFICZNE

Systemy kryptograficzne łączą wszystkie zabezpieczenia kryptograficzne, w tym poufność, uwierzytelnianie i integralność w jednym systemie. Systemy kryptograficzne chronią dialogi użytkowników przed atakującymi i eliminują potrzebę zrozumienia przez użytkowników konkretnych szczegółów kryptograficznych. Pierwszym zadaniem przy tworzeniu systemu kryptograficznego jest wybór standardu systemu kryptograficznego dla dialogu.



Dzięki standardom systemów kryptograficznych firmy nie muszą wymyślać własnych niestandardowych zabezpieczeń kryptograficznych. Przyjrzymy się kilku ważniejszym standardom systemów kryptograficznych, w tym Secure Sockets Layer (SSL)/Transport Layer Security (TLS) i IPsec (IPsec). Rysunek pokazuje, że po wybraniu standardu systemu kryptograficznego wykonywane są pozostałe etapy uzgadniania. Jest to ten sam proces omówiony wcześniej. Istnieje kilka innych standardów systemów kryptograficznych, których nie mamy czasu omówić. Przyjrzymy się Kerberosowi w następnym rozdziale.

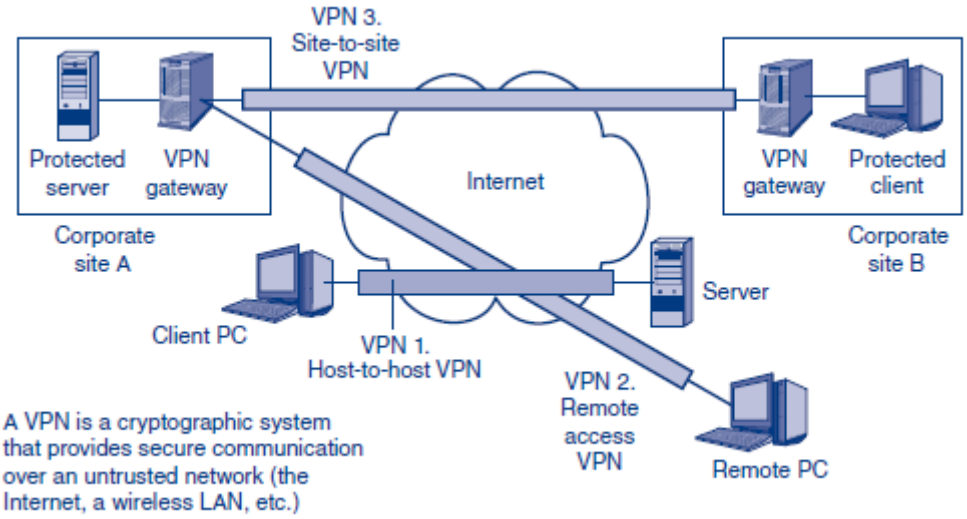
W wiadomościach

Ustawa o gospodarce cyfrowej to nowe ustawodawstwo w Wielkiej Brytanii, które tymczasowo przerywałoby połączenie internetowe osobom przyłapanym na nielegalnym udostępnianiu plików. Organy ścigania i agencje wywiadowcze obawiają się, że groźba kary zachęci pobierających do maskowania swoich działań za pomocą szyfrowania. Szyfrowanie połączeń w sieciach peer-to-peer zwiększyłoby koszty i obciążenie pracą niezbędne do monitorowania sieci w kraju. Mogłoby to również praktycznie uniemożliwić monitorowanie połączeń internetowych i zwiększyć ryzyko poważniejszych zagrożeń bezpieczeństwa.

Wirtualne sieci prywatne (VPN)

Systemy kryptograficzne są często używane w niezaufanych sieciach. Rysunek 3-25 pokazuje, że wirtualna sieć prywatna (VPN) jest tworzona przy użyciu systemu kryptograficznego w celu zabezpieczenia komunikacji w niezaufanej sieci (Internet, bezprzewodowa sieć LAN itp.).

Wirtualna sieć prywatna (VPN) jest tworzona przy użyciu systemu kryptograficznego w celu zabezpieczenia komunikacji w niezaufanej sieci (Internet, bezprzewodowa sieć LAN itp.).



Dlaczego VPN?

Po co w ogóle zawracać sobie głowę transmisją przez niezaufane sieci? W przypadku internetowych sieci VPN odpowiedź jest prosta: transmisja internetowa jest znacznie tańsza na bit przesyłany niż komercyjne sieci rozległe (WAN), takie jak Frame Relay. Ogromny rozmiar Internetu przynosi duże korzyści skali. Z kolei sieci VPN w bezprzewodowych sieciach LAN pozwalają firmie czerpać korzyści z mobilności pomimo wątpliwego bezpieczeństwa wielu sieci WLAN - zwłaszcza tych w bezprzewodowych punktach dostępowych. W następnym rozdziale zobaczymy, jak VPN mogą pokonać ataki „złych bliźniaków" na klientów bezprzewodowych.

Sieci VPN typu host-host

Rysunek ilustruje trzy typy sieci VPN. Najprostszym typem jest VPN typu host-host. Jak pokazano na przykładzie VPN 1, sieć VPN typu host-to-host łączy pojedynczego klienta przez niezaufaną sieć z pojedynczym serwerem. Gdy łączysz się z serwerem handlu elektronicznego w Internecie, serwer zazwyczaj tworzy między sobą a przeglądarką sieć VPN typu host-host, zanim zaczniesz wprowadzać poufne informacje, takie jak numery kart kredytowych. Sieć VPN typu host-host łączy pojedynczego klienta przez niezaufaną sieć z pojedynczym serwerem.

Sieci VPN dostępu zdalnego

Z kolei sieć VPN dostępu zdalnego łączy pojedynczy komputer zdalny przez niezaufaną sieć z siecią lokalną (patrz VPN 2 na rysunku). Sieci VPN z dostępem zdalnym zapewniają pracownikom pracującym w domu lub w podróży dostęp do zabezpieczonej wewnętrznej sieci korporacyjnej. Sieci VPN mogą również zapewnić bezpieczny dostęp do sieci wybranym klientom, przedstawicielom dostawców lub innym zatwierdzonym partnerom komunikacyjnym. Użytkownicy dostępu zdalnego łączą się z bramą VPN, która uwierzytelnia ich i daje im dostęp do autoryzowanych zasobów w witrynie. Należy zauważyć, że ta brama zapewnia użytkownikom zdalnym dostęp do wielu komputerów w witrynie, podczas gdy sieć VPN typu host-host zapewnia dostęp tylko do jednego komputera.

Zdalny dostęp VPN łączy pojedynczy zdalny komputer przez niezaufaną sieć z siecią lokacji.

Sieci VPN typu Site-to-Site

Wreszcie, sieci VPN typu site-to-site (patrz VPN 3 na rysunku) chronią cały ruch przepływający przez niezaufaną sieć między parą lokacji. Mogą to być dwie witryny firmowe lub witryna firmowa i witryna klienta lub witryna dostawcy. Połączenie lokacja-lokacja kryptograficznie chroni ruch wielu jednoczesnych konwersacji zachodzących między różnymi komputerami w obu lokacjach. W sieciach VPN typu site-to-site wysyłanie bram VPN szyfruje wiadomości wychodzące. Odbierające bramy VPN następnie odszyfrowują wiadomości przychodzące i przekazują je do właściwych hostów docelowych w witrynie odbierającej.

Sieci VPN typu lokacja lokacja chronią cały ruch przepływający przez niezaufaną sieć między parą lokacji.

TEST LXXX

a. Jaka jest definicja VPN?

b. Dlaczego firmy transmitują przez Internet?

c. Dlaczego przesyłają przez niezaufane sieci bezprzewodowe?

d. Rozróżnij trzy typy VPN.

e. Co robi brama VPN dla sieci VPN dostępu zdalnego?

f. Co robi brama VPN w przypadku sieci VPN typu lokacja-lokacja?

g. Jakie typy VPN korzystają z bram VPN?

SSL/TLS

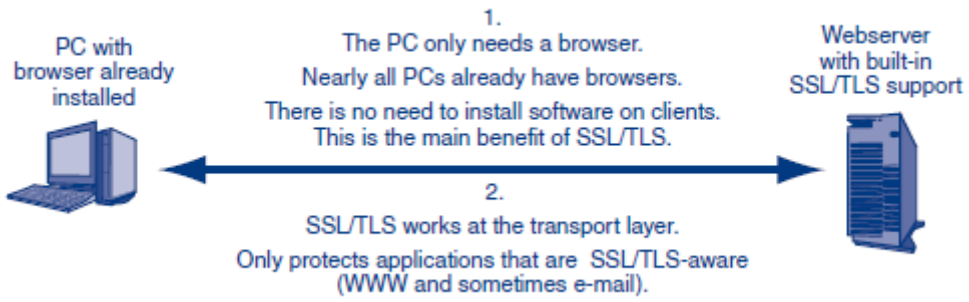
Po ogólnym przyjrzeniu się VPN, zaczniemy teraz przyglądać się określonym standardom VPN. Dzisiaj zaczniemy przyglądać się popularnemu standardowi VPN, SSL/TLS. Ten standard systemu kryptograficznego jest szeroko stosowany w przypadku sieci VPN typu host-host i sieci VPN dostępu zdalnego. Kiedy dokonujesz zakupu przez Internet, Twój wrażliwy ruch jest prawie zawsze chroniony przez standard systemu kryptograficznego, który pierwotnie nosił nazwę Secure Sockets Layer (SSL), gdy go stworzyła firma Netscape Corporation. Netscape przekazał starania o standaryzację Grupie Roboczej ds. Inżynierii Internetu (IETF), która zmieniła nazwę standardu Transport Layer Security (TLS), aby podkreślić, że działa on w warstwie transportowej. Będziemy go nazywać SSL/TLS, ale w praktyce ludzie nazywają to po prostu SSL lub TLS. Rysunek pokazuje, jak działa VPN typu host-host SSL/TLS. Chociaż SSL/TLS początkowo był standardem VPN typu host-to-host, ostatnio stał się VPNem dostępu zdalnego, dzięki pojawieniu się bram SSL/TLS. Jednak zobaczymy, że SSL/TLS jest ograniczone dla obu tych ról VPN.

TEST LXXXI

a. Rozróżnij SSL i TLS.

b. Dla jakiego typu VPN opracowano SSL/TLS?

c. Do jakiego typu VPN coraz częściej stosuje się SSL/TLS?



Nieprzejrzysta ochrona

Ponieważ protokół SSL/TLS działa w warstwie transportowej, może chronić ruch warstwy aplikacji zawarty w komunikatach warstwy transportowej. Ten wzorzec systemu kryptograficznego w jednej warstwie chroniącej komunikację w wyższych warstwach zobaczymy ponownie, gdy będziemy omawiać IPsec. Jednak ochrona komunikatów warstwy aplikacji przez SSL/TLS nie jest przezroczysta, co oznacza, że nie chroni automatycznie wszystkich komunikatów wyższych warstw. Chroni tylko aplikacje obsługujące SSL/TLS, co oznacza, że aplikacje te zostały specjalnie napisane lub przepisane do pracy z SSL/TLS. Chociaż wszystkie przeglądarki i aplikacje serwera WWW obsługują protokół SSL/TLS, a wiele programów pocztowych oferuje SSL/TLS jako opcjonalną ochronę, niewiele innych aplikacji może współpracować z SSL/TLS.

Niedroga operacja

Największą atrakcją SSL/TLS jest to, że każdy komputer ma dziś przeglądarkę, a wszystkie przeglądarki wiedzą, jak działać jako klienci SSL/TLS. Oznacza to, że SSL/TLS nie wymaga konfiguracji na klientach. Ponadto wszystkie serwery internetowe i większość serwerów pocztowych wiedzą, jak pracować z SSL/TLS. W związku z tym korzystanie z SSL/TLS jest prawie bezpłatne (poza moc obliczeniową potrzebnądo wdrożenia SSL/TLS).

TEST LXXXII

a. W jakiej warstwie działa SSL/TLS?

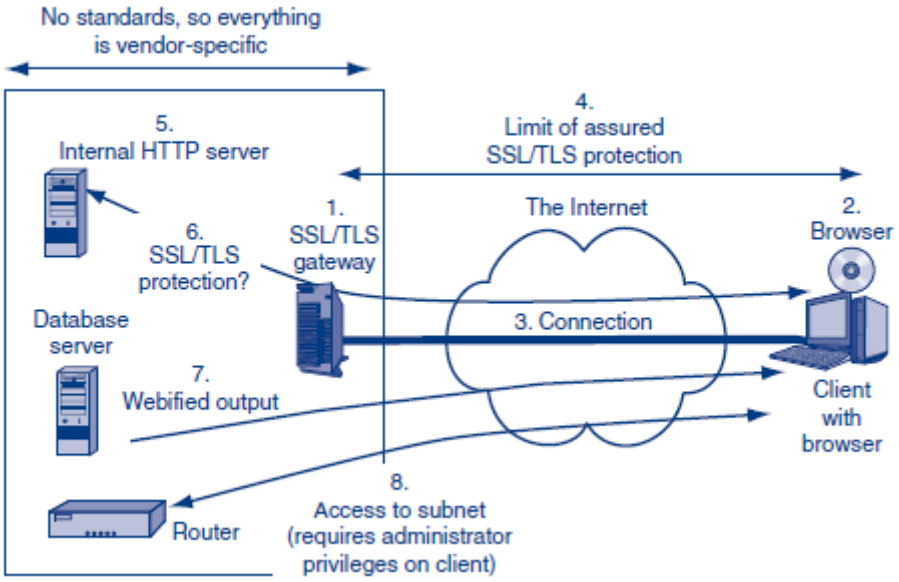
b. Jakie typy aplikacji może chronić SSL/TLS?

c. Jakie są dwie powszechnie używane aplikacje obsługujące SSL/TLS?

d. Dlaczego SSL/TLS jest popularny?

Bramy SSL/TLS i sieci VPN dostępu zdalnego

Do tej pory przyjrzeliśmy się sieciom VPN typu host-to-host SSL/TLS. Jak pokazuje Rysunek 3-27, aby przekonwertować SSL/TLS z sieci VPN typu host-host na VPN dostępu zdalnego, firmy umieszczają bramę SSL/TLS na granicy każdej witryny (1). Przeglądarka klienta zdalnego (2) nawiązuje pojedyncze połączenie SSL/TLS z bramą SSL/TLS (3), a nie z poszczególnymi hostami w witrynie.



Przeglądarka klienta zdalnego nawiązuje pojedyncze połączenie SSL/TLS z bramą SSL/TLS, a nie z poszczególnymi hostami w witrynie.

STANDARDY BRAM VPN

Sytuacja ze standardami bramek SSL/TLS jest bardzo prosta. Nie ma żadnych. SSL/TLS jedynie zarządza łączem między klientem a bramą SSL/TLS (3), a SSL/TLS tylko definitywnie chroni ruch między klientem a bramą (4). W efekcie brama SSL/TLS jest po prostu serwerem internetowym, jeśli chodzi o SSL/TLS. Nie ma potrzeby dodawania czegokolwiek do standardu SSL/TLS.

Brama SSL/TLS to po prostu serwer WWW, jeśli chodzi o SSL/TLS. Nie ma potrzeby dodawania czegokolwiek do standardu SSL/TLS.

Poza bramą, w witrynie klienta, wszystko zależy od dostawcy. To sprawia, że trudno jest ogólnie mówić o działaniu i usługach bramy VPN. Jednak bramy SSL/TLS mają zwykle kilka wspólnych cech.

UWIERZYTELNIANIE

Po pierwsze, brama SSL/TLS zawsze uwierzytelnia się wobec klienta, używając uwierzytelniania klucza publicznego. Jest to obowiązkowe w bramkach SSL/TLS. Po zakończeniu ochrony SSL/TLS brama wymaga od użytkownika uwierzytelnienia się, zwykle przy użyciu nazwy użytkownika i hasła. Uwierzytelnianie klienta jest poza procesem SSL/TLS.

PODŁĄCZANIE KOMPUTERA KLIENTA DO AUTORYZOWANYCH ZASOBÓW

Jeśli uwierzytelnianie się powiedzie, brama SSL/TLS umożliwia użytkownikowi łączenie się z wybranymi zasobami w witrynie.

• W wielu przypadkach bramka SSL/TLS umożliwia komputerowi klienckiemu połączenie z wieloma wewnętrznymi serwerami WWW (5). Zwykle brama po prostu otwiera połączenie z witryną i ignoruje ruch wychodzący poza nią.

• W innych przypadkach brama VPN łączy komputer kliencki z serwerem bazy danych lub innym serwerem, który nie wie, jak pracować z przeglądarkami jako klientami (7). Podczas transmisji klienta brama VPN konwertuje stronę internetową na zapytanie do bazy danych lub inne zapytanie. Następnie brama VPN przechwytuje odpowiedzi z serwera. Brama VPN „webizuje” te wiadomości (przekształca

je w strony internetowe), aby przeglądarka mogła je zaprezentować użytkownikowi. Bramy VPN różnią się znacznie pod względem liczby aplikacji, które mogą obsługiwać w ten sposób, oraz sposobu, w jaki obsługują te aplikacje.

• W jeszcze innych przypadkach brama SSL/TLS łączy komputer kliencki z całą podsiecią sieci lokalnej (8). Klient może następnie połączyć się z dowolnym serwerem w podsieci.

BEZPIECZEŃSTWO USŁUG

Jak już wspomniano, SSL/TLS zapewnia ochronę między klientem a bramą SSL/TLS (4). Jednak pomiędzy bramą SSL/TLS a zasobami w sieci może być lub nie być bezpieczeństwo (6). Wszystko zależy od wyborów projektowych dostawcy bramy. Na przykład, jeśli wewnętrzny serwer WWW będzie obsługiwać klienta zewnętrznego, brama SSL/TLS może utrzymywać dwa bezpieczne połączenia — jedno między wewnętrznym serwerem WWW a bramą, a drugie między bramą a klientem zewnętrznym. Lub może nie być żadnego zabezpieczenia między bramą VPN a wewnętrznym serwerem sieciowym.

PRZEGLĄDARKA NA KLIENCIE

Co musi mieć klient, aby korzystać z SSL/TLS? Dla podstawowych nie wymaga dodatkowego oprogramowania. W związku z tym SSL/TLS może współpracować z dowolnym komputerem klienckim podłączonym do Internetu, w tym z komputerem w pracy, w hotelach, w kawiarenkach internetowych oraz w witrynach klientów lub dostawców. To sprawia, że SSL/TLS są niezwykle atrakcyjne jako VPN zdalnego dostępu.

USŁUGI ZAAWANSOWANE WYMAGAJĄ UPRAWNIEŃ ADMINISTRATORA NA PCS

Jednak, aby umożliwić klientowi uzyskanie przezroczystego dostępu do podsieci (8) i świadczenie niektórych innych usług, brama SSL/TLS musi pobrać moduł wtyczki dla przeglądarki komputera klienckiego. Niestety, instalacja dodatku wymaga, aby użytkownik klienta miał uprawnienia administratora na komputerze klienckim. Kafejki internetowe i inne komputery publiczne prawdopodobnie nie zapewnią użytkownikom takiego poziomu uprawnień. Podobnie jak większość innych miejsc, które użytkownik może odwiedzać.

Co więcej, używanie SSL/TLS do zdalnego dostępu lub połączeń między hostami do serwera WWW jest niebezpieczne, ponieważ SSL/TLS pozostawia informacje na dysku twardym komputera klienckiego po zakończeniu przez użytkownika sesji SSL/TLS. Jest to poważne zagrożenie bezpieczeństwa dla osób pracujących przy komputerach publicznych. Wiele bram SSL/TLS umożliwia pobieranie wtyczek, które usuwają wszelkie ślady sesji użytkownika. Ponownie jednak miejsca odwiedzane przez użytkownika prawdopodobnie nie nadają statusu administracyjnego niż instalowanie informacji o sesji wymaga usunięcia dodatku. Innymi słowy, wymazywanie śladów jest rzadko możliwe, gdy jest to najbardziej potrzebne - gdy nie korzystasz z własnego komputera.

PERSPEKTYWICZNY

Chociaż firma Netscape zaprojektowała protokół SSL/TLS w jednym celu — ochrony komunikacji między przeglądarką a serwerem WWW — bramy VPN znacznie rozszerzyły jego zastosowanie. Brama SSL/TLS może zapewnić zdalny dostęp do prawie każdego komputera bez modyfikacji lub konfiguracji. To sprawia, że SSL/TLS jest bardzo atrakcyjną technologią zdalnego dostępu VPN. Jednak wdrażanie ma tendencję do bycia ograniczonym i niezgrabnym. Ponadto bramy SSL/TLS są całkowicie niestandaryzowane i znacznie różnią się pod względem oferowanych usług. Korzystanie z SSL/TLS do zdalnego dostępu VPN wymaga dużej należytej staranności w ocenie potrzeb i analizie produktów.

Wymaga to również sporego operacyjnego trzymania za rękę przez personel sieci. Ponadto SSL/TLS nie jest w stanie tworzyć sieci VPN typu site-to-site. W większości korporacji sieci VPN typu site-to-site będą przenosić znacznie większy ruch niż sieci VPN dostępu zdalnego. Mimo to brak konieczności dodawania żadnego oprogramowania do zdalnego komputera użytkownika jest tak przekonujący, że bramy SSL/TLS bardzo szybko zyskują na znaczeniu.

TEST LXXXIII

a. SSL/TLS został stworzony do komunikacji między hostami (przeglądarka-serwer). Jakie urządzenie może zmienić SSL/TLS w VPN zdalnego dostępu?

b. W sieciach VPN dostępu zdalnego SSL/TLS, na jakim urządzeniu klient sam się uwierzytelnia?

c. Kiedy zdalny klient transmituje w SSL/TLS VPN, jak daleko zdecydowanie rozciąga się poufna transmisja?

d. Jakie trzy usługi zazwyczaj zapewniają bramy SSL/TLS?

e. Czym jest webifikacja?

f. Jakiego oprogramowania potrzebuje klient do podstawowej obsługi SSL/TLS VPN?

g. Do jakich celów klient może potrzebować dodatkowego pobranego oprogramowania?

h. Dlaczego instalacja dodatkowego pobranego oprogramowania w przeglądarce może być problematyczna?

i. Dlaczego SSL/TLS jest atrakcyjny jako technologia VPN zdalnego dostępu?

J. Jakie problemy napotykają firmy, jeśli używają go jako technologii zdalnego dostępu VPN?

k. Który z trzech typów sieci VPN może obsługiwać protokół SSL/TLS?

IPSEC

Firmy, które wymagają najsilniejszych zabezpieczeń VPN, stosują rodzinę standardów bezpieczeństwa kryptograficznego IETF, zwanych zbiorczo IPsec (IP security). IP to protokół internetowy, a „sec" jest skrótem od zabezpieczeń. Innymi słowy, standardy te zabezpieczają adres IP (w tym wszystko, co znajduje się w polu danych pakietu IP).

Atrakcje IPsec

Rysunek porównuje IPsec ze standardem bezpieczeństwa kryptograficznego SSL/TLS, który właśnie widzieliśmy. IPsec jest bardziej złożony i dlatego droższy do wprowadzenia niż SSL/TLS, ale IPsec jest złotym standardem bezpieczeństwa VPN. Oferuje najsilniejsze zabezpieczenia i obsługuje scentralizowaną kontrolę korporacyjną nad wszystkimi operacjami IPsec na wszystkich urządzeniach.

SSL/TLS ZAPEWNIA NIEPRZEZROCZYSTE BEZPIECZEŃSTWO WARSTWY TRANSPORTOWEJ

Wcześniej widzieliśmy, że protokół SSL/TLS, który działa w warstwie transportowej, może chronić tylko aplikacje obsługujące protokół SSL/TLS - głównie usługi internetowe HTTP i niektóre systemy poczty e-mail. Widzieliśmy również, że bramy SSL/TLS rozszerzają standard o obsługę zdalnego dostępu, aczkolwiek niezręcznie.

IPSEC: BEZPIECZEŃSTWO PRZEZROCZYSTEJ WARSTWY INTERNETOWEJ

Natomiast IPsec działa w warstwie internetowej. Chroni pakiet IP i wszystko w polu danych pakietu IP. Obejmuje to komunikaty ICMP, TCP i UDP oraz wszystkie aplikacje.

IPsec działa w warstwie internetowej.

W IPsec ochrona w wyższych warstwach jest całkowicie przezroczysta. Nie ma potrzeby modyfikowania aplikacji ani protokołów warstwy transportowej do pracy z IPsec. W rzeczywistości protokoły warstwy transportowej i protokoły aplikacji nie są nawet świadome obecności IPsec, gdy używany jest IPsec. W porównaniu z SSL/TLS przezroczysta ochrona IPsec zmniejsza koszty wdrożenia i eksploatacji poprzez ograniczenie obejść. Jednak oszczędności wynikające z obniżonych kosztów operacyjnych nie są całkowicie kompensowane. IPsec jest jeszcze bardziej kosztowny i skomplikowany w instalacji. SSL/TLS działa w warstwie transportowej i nie zapewnia przezroczystej ochrony komunikatów warstwy aplikacji. Protokół IPsec działa w warstwie internetowej i zapewnia przezroczystą ochronę wiadomościom warstwy transportowej i warstwy aplikacji.

IPSEC W ZARÓWNO IPV4 I IPV6

IETF zaprojektował IPsec pierwotnie dla najnowszej wersji protokołu internetowego, IP w wersji 6 (IPv6). Jednak, gdy został utworzony, IPsec został również napisany do pracy z obecnie dominującą wersją IP-IP w wersji 4 (IPv4). Innymi słowy, bez względu na wersję IP używaną przez sieć, IPsec będzie ją chronić.

TEST LXXXIV

a. W jakiej warstwie działa IPsec?

b. Jakie warstwy chroni protokół IPsec?

c. Porównaj poziom zabezpieczeń kryptograficznych w IPsec z zabezpieczeniami SSL/TLS.

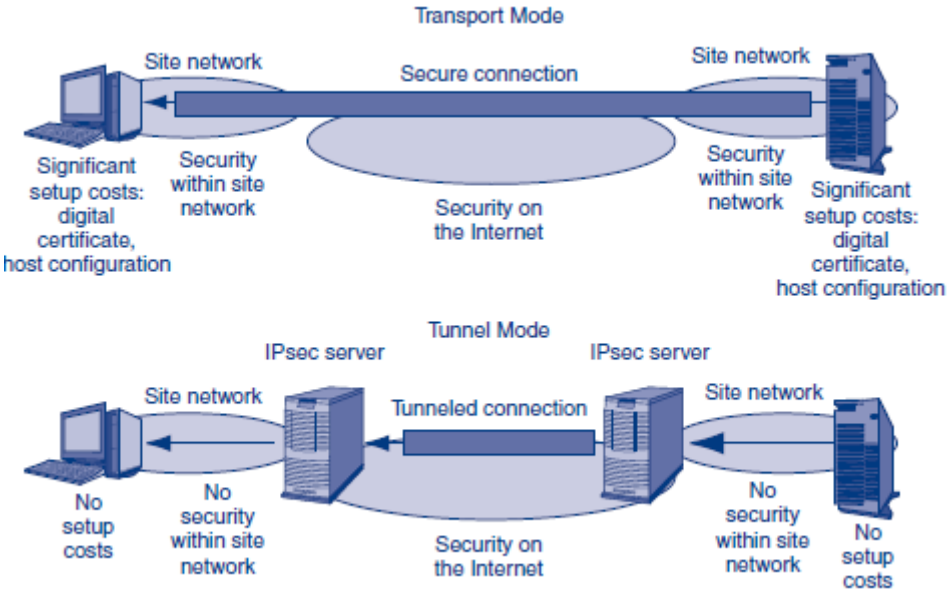
d. Porównaj scentralizowane zarządzanie w IPsec i SSL/TLS.

e. Dlaczego przezroczysta ochrona IPsec jest atrakcyjna w porównaniu z nieprzejrzystą ochroną SSL/TLS?

f. Które wersje protokołu IP mogą korzystać z protokołu IPsec?

Tryb transportu IPsec

W IPsec istnieją dwa tryby pracy. Są to tryb transportu i tryb tunelowy. Rysunek 3-29 ilustruje działanie tych dwóch trybów. Rysunek 30 porównuje ich cechy w tabeli.



Characteristic	Transport Mode	Tunnel Mode
Uses an IPsec VPN gateway?	No	Yes
Cryptographic protection	All the way from the source host to the destination host, including the Internet and the two site networks.	Only over the Internet between the IPsec gateways. Not within the two site networks.
Setup costs	High. Setup requires the creation of a digital certificate for each client and significant configuration work.	Low. Only the IPsec gateways must implement IPsec, so only they need digital certificates and need to be configured.
Firewall friendliness	Bad. A firewall at the border to a site cannot filter packets because the content is encrypted.	Good. Each packet is decrypted by the IPsec gateway. A border firewall after the IPsec gateway can filter the decrypted packet.
The "bottom line"	End-to-end security at high cost.	Low cost and protects the packet over the most dangerous part of its journey.

BEZPIECZEŃSTWO HOST-HOST

Tryb transportu IPsec zapewnia bezpieczeństwo między hostami. Innymi słowy, implementuje sieci VPN typu host-host. Tryb transportu umożliwia dwóm hostom bezpieczną komunikację bez względu na to, co jeszcze dzieje się w sieci.

PEŁNA OCHRONA

Tryb transportu jest atrakcyjny, ponieważ zapewnia bezpieczeństwo, gdy pakiety są przesyłane przez wewnętrzne sieci lokacji, a także przez Internet. Zapewnia to kompleksowe bezpieczeństwo, nawet jeśli wewnętrzne sieci nadawcy i odbiorcy nie są zaufane.

KOSZT USTAWIENIA

Z drugiej strony, tryb transportu IPsec wymaga, aby firma jawnie skonfigurowała IPsec na każdym kliencie i serwerze. Obejmuje to wygenerowanie pary klucz prywatny-certyfikat cyfrowy, umieszczenie klucza prywatnego na każdym komputerze, a następnie zarządzanie certyfikatem cyfrowym w całym jego cyklu życia. Ponadto, chociaż wszystkie najnowsze systemy operacyjne dla komputerów klienckich mogą implementować protokół IPsec, skonfigurowanie ich do korzystania z niego zwykle wiąże się z ręczną konfiguracją. Chociaż koszt robocizny przypadający na klienta i serwer jest skromny, całkowity koszt robocizny związanej z instalacją trybu transportu może być zniechęcający w firmie, która ma wielu klientów i serwerów.

IPSEC W TRYBIE TRANSPORTOWYM I ZAPORY ZAPOROWE

Chociaż tryb transportu IPsec zapewnia wysoki poziom bezpieczeństwa dialogów, zmniejsza skuteczność innego środka zaradczego, jakim jest firewall graniczny. Zapora graniczna powinna badać każdy przechodzący przez nią pakiet, szukając oznak niedopuszczalnej zawartości. Jednak w przypadku zaszyfrowanych pakietów IP zapory sieciowe są bezużyteczne, ponieważ nie mogą odczytać zawartości zwykłego tekstu pakietu, aby go przefiltrować. Jeśli host źródłowy wysyła pakiet ataku do hosta docelowego za pośrednictwem trybu transportu IPsec, zapora nie może zatrzymać pakietu ataku.

Tryb tunelu IPsec

Rysunek pokazuje natomiast, że tryb tunelowania IPsec chroni tylko ruch między dwiema bramami IPsec w różnych lokacjach. Te bramy bezpiecznie przesyłają ruch przez Internet między sobą. Tryb tunelowy tworzy VPN typu site-to-site.

OCHRONA JEST ZAPEWNIANA PRZEZ BRAMKI IPSEC

Źródłowa brama IPsec odbiera oryginalne (niezaszyfrowane) pakiety IP od hostów swojej witryny, szyfruje je i wysyła do innej bramy IPsec. Odbierająca brama IPsec odszyfrowuje pakiety IP i wysyła je w postaci czystej do hosta docelowego.

TANIEJ NIŻ TRYB TRANSPORTOWY

Główną zaletą pracy w trybie tunelowym jest koszt. Cała praca kryptograficzna jest wykonywana na serwerach bram IPsec. Klienci i serwery po prostu przesyłają i odbierają swoje pakiety w sposób jawny. Firma nie musi wprowadzać żadnych zmian w swoich klientach i serwerach, tak jak musi to zrobić w trybie transportu. Brak konieczności tworzenia i zarządzania certyfikatami cyfrowymi dla wszystkich klientów i serwerów sprawia, że tryb tunelowy jest znacznie tańszy niż tryb transportowy.

OCHRONA PRZYJAZNA PRZEZ FIREWALL

Ponadto tryb tunelowania IPsec jest przyjazny dla zapory. Pakiety są szyfrowane tylko między dwiema bramami IPsec, więc po przybyciu pakietu można go filtrować przez zaporę sieciową umieszczoną za bramą IPsec w każdej lokalizacji.

BRAK OCHRONY W DWÓCH OBIEKTACH

Wadą trybu tunelowego jest to, że nie zapewnia on absolutnie żadnej ochrony pakietom IP, gdy przemieszczają się one w sieciach lokacji w obu lokacjach. To pozostawia pakiety otwarte na atak w sieciach lokacji. Jednak transmisja w sieciach witryn jest ogólnie bezpieczniejsza niż transmisja przez Internet, więc utrata ochrony w witrynach jest często uważany za dobry kompromis ze względu na niższy koszt pracy w trybie tunelu IPsec i przyjazność zapory sieciowej IPsec.

TEST LXXXV

a. Rozróżnij tryby transportu i tunelu w IPsec pod względem ochrony pakietów.

b. Jakie są atrakcje każdego z nich?

b. Jakie są problematyczne kwestie każdego z nich?

Powiązania zabezpieczeń IPsec (SA)

Zanim dwa hosty lub bramy IPsec komunikują się, muszą najpierw ustanowić skojarzenia zabezpieczeń. Security Association (SA) to umowa określająca, jakich metod i opcji zabezpieczeń IPsec będą używać dwa hosty lub dwie bramy IPsec. SA w IPsec przypomina zestaw szyfrów SSL/TLS.

Security Association (SA) to umowa określająca, jakich metod i opcji zabezpieczeń IPsec będą używać dwa hosty lub dwie bramy IPsec.

ODDZIELNE SA W DWÓCH KIERUNKACH

Rysunek ilustruje, w jaki sposób partnerzy komunikujący się negocjują powiązania bezpieczeństwa. Należy pamiętać, że gdy dwie strony komunikują się, muszą ustanowić dwa SA – po jednym w każdym kierunku. Jeśli Sal i Julia komunikują się, musi istnieć SA, którą Sal ma śledzić podczas wysyłania do Julii i oddzielne SA, którą Julia ma śledzić podczas wysyłania do Sal.

To użycie dwóch SA umożliwia inny poziom ochrony w każdym kierunku, jeśli jest to pożądane.

POLITYKI OPARTE NA SA

Jak wspomniano wcześniej, niektóre dopuszczalne metody i opcje bezpieczeństwa w standardach bezpieczeństwa kryptograficznego mogą być nieodpowiednie dla potrzeb bezpieczeństwa firmy. Firma chciałaby ustalić zasady dotyczące akceptowalnych metod i opcji bezpieczeństwa oraz egzekwować te zasady na wszystkich urządzeniach, które wdrażają standard. SSL/TLS nie ma możliwości centralnego ustawiania i egzekwowania zasad, ale IPsec ma. Jak pokazano na rysunku 3-31, protokół IPsec obsługuje korzystanie z serwerów zasad IPsec, które przesyłają listę odpowiednich zasad do poszczególnych serwerów lub hostów bram IPsec. Z punktu widzenia zarządzania bezpieczeństwem jest to kluczowa zdolność.

TEST LXXXVI

a. Co określa SA? (Nie tylko przeliteruj SA.)

b. Kiedy dwie strony chcą komunikować się w obie strony z bezpieczeństwem, ile IPsec SA jest potrzebnych?

c. Czy mogą istnieć różne SA w obu kierunkach?

d. Jaka jest z tego korzyść?

e. Dlaczego firmy chcą tworzyć polityki dla SA?

f. Czy mogą to zrobić w SSL/TLS?

g. Jak IPsec ustawia i egzekwuje zasady?

WNIOSEK

Przyjrzeliśmy się podstawowym pojęciom kryptograficznym, które każdy specjalista ds. bezpieczeństwa IT musi znać. Przyjrzeliśmy się również, w jaki sposób systemy kryptograficzne zapewniają bezpieczną komunikację w przejrzysty i ujednolicony sposób. Kryptografia może być wyzwaniem. Próbowaliśmy podsumować niektóre kluczowe punkty wymienione w rozdziale. Jednym z powszechnych zabezpieczeń kryptograficznych jest szyfrowanie zapewniające poufność, w którym oryginalna wiadomość w postaci zwykłego tekstu jest szyfrowana za pomocą szyfru (metoda szyfrowania/deszyfrowania) i klucza. Daje to zaszyfrowany tekst, którego nie może odczytać nikt, kto go przechwytuje. Odbiorca stosuje szyfr w odwrotnej kolejności z tym samym kluczem lub innym kluczem (w zależności od szyfru), aby odzyskać oryginalną wiadomość w postaci zwykłego tekstu. W rozdziale przyjrzano się dwóm operacjom powszechnie stosowanym w szyfrach — podstawieniu i transpozycji. W przypadku szyfrowania kluczem symetrycznym zapewniającym poufność nadawca i odbiorca używają tego samego klucza w obu kierunkach. W szyfrowaniu kluczem publicznym każda strona ma zarówno klucz publiczny, jak i klucz prywatny. W przypadku szyfrowania kluczem publicznym w celu zachowania poufności nadawca szyfruje kluczem publicznym odbiorcy. Odbiorca deszyfruje własnym kluczem prywatnym. Aby zapewnić silne bezpieczeństwo, klucze muszą być bardzo długie, aby uniemożliwić włamanie przez wyczerpujące wyszukiwanie. Szyfry szyfrujące kluczem symetrycznym potrzebują kluczy o długości co najmniej 100 bitów, aby były dziś silne. Klucze publiczne i prywatne muszą być jeszcze dłuższe, aby były silne. Klucze RSA muszą mieć co najmniej 1024 bity, a klucze ECC muszą mieć co najmniej 512 bitów. Inną ważną ochroną kryptograficzną jest uwierzytelnianie, w którym suplikant (taki jak komputer kliencki) próbuje udowodnić swoją tożsamość weryfikatorowi (zwykle serwerowi) poprzez przesłanie poświadczeń. Uwierzytelnianie zwykle odbywa się zarówno na początku sesji komunikacyjnej, jak i podczas wysyłania każdej wiadomości. Często wspominaliśmy o trzech podstawowych procesach kryptograficznych: szyfrowaniu kluczem symetrycznym, szyfrowaniu kluczem publicznym i haszowaniu. Łatwo je pomylić. Rysunek porównuje, w jaki sposób te trzy procesy są wykorzystywane do zachowania poufności i uwierzytelniania.

	Confidentiality	**Authentication**
Symmetric key encryption	Applicable. Sender encrypts with key shared with the receiver.	Not applicable.
Public key encryption	Applicable. Sender encrypts with *receiver's public key*. Receiver decrypts with the *receiver's own private key*.	Applicable. Sender (supplicant) encrypts with *own private key*. Receiver (verifier) decrypts with the *public key* of the *true party*, usually obtained from the true party's digital certificate.
Hashing	Not applicable.	Applicable. Used in MS-CHAP for initial authentication and in HMACs for message-by-message authentication.

• Należy zauważyć, że zarówno do celów poufności, jak i uwierzytelniania używane jest tylko szyfrowanie kluczem publicznym, a pary kluczy publiczny-prywatny są używane w tych procesach w różny sposób.

• W przeciwieństwie do tego, szyfrowanie kluczem symetrycznym jest używane tylko w celu zachowania poufności.

• Z kolei haszowanie jest używane tylko do uwierzytelniania. Chociaż haszowanie do uwierzytelniania wykorzystuje klucz, nie oznacza to, że jest to szyfrowanie kluczem symetrycznym, co jest zupełnie innym procesem.

Zabezpieczenia kryptograficzne rzadko są używane samodzielnie. Raczej prawie zawsze są one pakowane w systemy kryptograficzne, które zabezpieczają dialogi z pełnym zakresem zabezpieczeń. Systemy kryptograficzne rozpoczynają się od trzech początkowych etapów uzgadniania, a następnie przechodzą do etapu ciągłej komunikacji. Etapy uzgadniania rozpoczynają się od negocjacji zestawów metod i opcji bezpieczeństwa, z których będą korzystać partnerzy komunikacji. Polityki korporacyjne mogą ograniczać, które zestawy metod i opcji można stosować, aby uniemożliwić komunikującym się partnerom stosowanie słabych metod i opcji. Następnie obie strony przeprowadzają wstępne uwierzytelnianie — zwykle uwierzytelnianie wzajemne. W szczególności przyjrzeliśmy się uwierzytelnianiu MS-CHAP, które jest przeznaczone dla użytkowników logujących się na serwery Microsoft. MS-CHAP chroni hasło logowania użytkownika z zachowaniem poufności. Zwykle dwóch partnerów komunikacyjnych dokonuje wzajemnego uwierzytelnienia. Jednak MS-CHAP tylko uwierzytelnia użytkownika. MS-CHAP nie używa szyfrowania. Raczej używa hashowania. Ze względu na użycie haseł wielokrotnego użytku jako tajnych i brak wzajemnego uwierzytelniania, MS-CHAP jest słabą początkową metodą kryptograficzną. Na koniec, na etapie uzgadniania kluczy, obie strony muszą bezpiecznie wymieniać symetryczne klucze sesji (i inne klucze tajne). Klucze sesji są używane tylko w jednej sesji komunikacyjnej. Zobaczyliśmy, jak wykonać kluczowanie za pomocą dystrybucji klucza publicznego i umowy klucza Diffie-Hellman. To kończy etapy uścisku dłoni. Na bieżącym etapie komunikacji obaj partnerzy bezpiecznie wymieniają wiele wiadomości. Każda wiadomość otrzymuje podpis elektroniczny w celu uwierzytelniania wiadomości po wiadomości i integralności wiadomości. Istnieją dwa rodzaje podpisów elektronicznych – HMAC i podpisy cyfrowe. HMAC używają skrótu i klucza (tak naprawdę wspólnego sekretu). HMAC są niedrogie we wdrażaniu i są najczęściej używanymi podpisami elektronicznymi. Podpisy cyfrowe wykorzystują szyfrowanie kluczem publicznym. Nadawca szyfruje skrót skrótu wiadomości własnym kluczem prywatnym nadawcy. Odbiorca (weryfikator) odszyfrowuje wiadomość za pomocą klucza publicznego prawdziwej strony – strony, za którą podaje się petent. Podpisy cyfrowe zapewniają niezwykle silne uwierzytelnianie. Jednak podpisy cyfrowe wykorzystują szyfrowanie kluczem publicznym, które jest niezwykle powolne, a przez to drogie. Ponadto szyfrowanie kluczem publicznym na potrzeby uwierzytelniania jest zwykle testowane przy użyciu informacji zawartych w certyfikacie cyfrowym prawdziwej strony. Wymaga to systemu zaufanych urzędów certyfikacji. Urząd certyfikacji podaje klucz publiczny strony rzeczywistej, którego należy użyć do sprawdzenia, czy podpis cyfrowy został utworzony przy użyciu klucza prywatnego strony prawdziwej. Ten rozdział zawierał krótką sekcję na temat dystrybucji kluczy kwantowych i łamania kluczy kwantowych. Podczas trwającego etapu komunikacji systemy kryptograficzne wykorzystują szyfrowanie kluczem symetrycznym do szyfrowania każdej wiadomości w celu zachowania poufności. Przyjrzeliśmy się, w jaki sposób elementy kryptograficzne są pakowane w systemy kryptograficzne, które zapewniają elementy bezpieczeństwa w jednym zintegrowanym pakiecie. Określone systemy kryptograficzne wykorzystują standardy bezpieczeństwa kryptograficznego. W tym rozdziale przyjrzeliśmy się niektórym z głównych standardów bezpieczeństwa kryptograficznego. Przyjrzeliśmy się wirtualnym sieciom prywatnym (VPN), które są systemami kryptograficznymi zapewniającymi bezpieczną komunikację w niezaufanych sieciach (Internet, bezprzewodowa sieć LAN itp.). Istnieją sieci VPN typu host-host, dostęp zdalny i site-to-site. Jednym z powszechnie stosowanych standardów VPN jest SSL/TLS. SSL/TLS jest bardzo popularny, ponieważ klient potrzebuje tylko przeglądarki, a wszystkie dzisiejsze komputery klienckie mają przeglądarki. Widzieliśmy, jak stworzono protokół SSL/TLS dla sieci VPN typu host-host, a konkretnie dla sieci VPN typu przeglądarka-serwer. Wszystkie przeglądarki i serwery internetowe wiedzą, jak skonfigurować VPN SSL/TLS, więc korzystanie z nich jest niedrogie. Następnie zobaczyliśmy, jak bramy SSL/VPN mogą zmienić SSL/TLS w technologię VPN zdalnego dostępu. Jednak SSL/TLS nie zapewnia przejrzystej ochrony dla wszystkich aplikacji, a konfigurowanie bram SSL/TLS do zdalnego dostępu może być niezręczne. Złotym standardem dla VPN jest IPsec. IPsec oferuje niezwykle silne zabezpieczenia, w tym wymóg, aby obaj partnerzy komunikacji uwierzytelniali

się za pomocą uwierzytelniania klucza publicznego za pomocą certyfikatów cyfrowych. Ponadto protokół IPsec ma silne możliwości kontroli polityki, dzięki czemu partnerzy komunikujący się nie mogą wybrać słabych opcji zabezpieczeń. Zarządzanie polityką jest scentralizowane i dlatego łatwe w administrowaniu.

IPsec działa w dwóch trybach. W trybie transportu protokół IPsec zapewnia bezpieczeństwo na całej drodze między hostem źródłowym i docelowym. Jednak tryb transportu IPsec jest kosztowny ze względu na wymagania dotyczące konfiguracji wszystkich klientów i serwerów oraz zarządzanie certyfikatami cyfrowymi w całym ich cyklu życia. Tryb transportu również uniemożliwia lub przynajmniej utrudnia filtrowanie przez firewall. W trybie tunelu protokół IPsec zapewnia bezpieczeństwo tylko między bramami IPsec w każdej lokacji. Eliminuje to wymagania dotyczące konfiguracji komputera i umożliwia filtrowanie zapory. Z drugiej strony tryb tunelowy nie zapewnia żadnego bezpieczeństwa w witrynach.

Pytania do przemymyślenia

1. Całkowita szybkość przetwarzania mikroprocesorów (w oparciu o częstotliwość taktowania i liczbę obwodów) podwaja się mniej więcej co roku. Dzisiaj symetryczny klucz sesji musi mieć długość 100 bitów, aby można go było uznać za silny. Jak długo będzie musiał mieć symetryczny klucz sesji za 30 lat, aby był uważany za silny? (Wskazówka: Zastanów się, jak długo trwa deszyfrowanie, jeśli długość klucza zostanie zwiększona o jeden bit.)

2. Dłuższe klucze są trudniejsze do złamania. Większość dzisiejszych kluczy symetrycznych ma długość od 100 do 300 bitów. Dlaczego systemy nie używają znacznie dłuższych kluczy symetrycznych, powiedzmy 1000-bitowych kluczy?

3. Do złamania 100-bitowego klucza używana jest brutalna siła. Klucz został złamany tylko w 5000 próbach. Jak to może być?

4. W praktyce uwierzytelnianie za pomocą klucza publicznego jest często używane do uwierzytelniania początkowego, ale rzadko do uwierzytelniania typu wiadomość po wiadomości. Biorąc pod uwagę intensywną moc obliczeniową wymaganą do uwierzytelniania za pomocą klucza publicznego oraz fakt, że uwierzytelnianie za pomocą klucza publicznego zapewnia najsilniejsze uwierzytelnianie, wyjaśnij te dwa wzorce użytkowania.

5. Czy w tym rozdziale widzieliśmy szyfrowanie kluczem symetrycznym używane do uwierzytelniania? Jeśli tak, w jaki sposób został wykorzystany?

6. Czym są podobne certyfikaty cyfrowe i prawa jazdy, a czym się różnią?

7. Czym są podobne do cyfrowych certyfikatów i paszportów, a czym się różnią?

8. W jaki sposób certyfikaty cyfrowe i dyplomy uniwersyteckie są podobne, a czym się różnią?

9. Czym są podobne certyfikaty cyfrowe i bilety do kina, a czym się różnią?

10. Zidentyfikuj potencjalne zagrożenia bezpieczeństwa związane z uwierzytelnianiem za pomocą podpisów cyfrowych i certyfikatów cyfrowych. Wyjaśnij każde z nich i opisz, jak poradziłbyś sobie z każdym zagrożeniem.

11. Opisano, w jaki sposób uwierzytelnianie kluczem publicznym jest wykorzystywane do uwierzytelniania wiadomości po wiadomości w podpisach cyfrowych. Jednakże, uwierzytelnianie kluczem publicznym jest szeroko stosowane do wstępnego uwierzytelniania. Opisz procesy, które petent i weryfikator zastosowaliby, gdyby szyfrowanie kluczem publicznym zostało użyte w

początkowym uwierzytelnianiu typu challenge-response. W dużym stopniu korzystaj ze swojej wiedzy na temat podpisów cyfrowych, ale umieść te informacje w kontekście wyzwania-odpowiedź.

12. Jeśli petent wręczy Ci certyfikat cyfrowy, czy powinieneś go zaakceptować? Wyjaśniać. (Zastanów się nad tym uważnie. Odpowiedź nie jest oczywista.)

13. Pretty Good Privacy (PGP) wykorzystuje szyfrowanie kluczem publicznym i szyfrowanie kluczem symetrycznym do szyfrowania długich dokumentów. Jak to możliwe?

BEZPIECZNE SIECI

W rozdziale 3 przyjrzano się, w jaki sposób można wykorzystać kryptografię do ochrony komunikacji poprzez zapewnienie poufności, autentyczności i integralności (CIA) wiadomości. W tym rozdziale zmienimy punkt ciężkości i przyjrzymy się, w jaki sposób same sieci są atakowane. Przyjrzy się, w jaki sposób atakujący mogą złośliwie zmienić normalne działanie sieci. Przed powstaniem nowoczesnych sieci telekomunikacyjnych wiadomości były dostarczane głównie ręcznie, wypowiadane przez telefon lub wysyłane za pomocą fal radiowych. Głównymi celami bezpieczeństwa w tym czasie były (1) utrzymanie wiadomości w tajemnicy (poufność), (2) upewnienie się, że wiadomość pochodzi od prawdziwego nadawcy (autentyczność) oraz (3) upewnienie się, że wiadomość nie została zmieniona (integralność) . Systemy kryptograficzne mogą i nadal mogą osiągnąć każdy z tych celów. Jednak wraz z pojawieniem się nowoczesnych sieci telekomunikacyjnych stało się jasne, że należy zająć się nowymi kwestiami bezpieczeństwa. Sposoby dostarczania wiadomości można było zatrzymać, spowolnić lub zmienić. Trasa, którą obierały wiadomości, mogła zostać zmieniona. Wiadomości mogą być przekierowywane do fałszywych odbiorców. Atakujący mogli również uzyskać dostęp do kanałów komunikacji, które wcześniej uważano za zamknięte i poufne.

Tworzenie bezpiecznych sieci

Tworząc bezpieczne środowisko sieciowe, należy wziąć pod uwagę cztery ogólne cele. Cele te są rozszerzeniem ram CIA (poufność, integralność i dostępność). Cele te obejmują dostępność, poufność, funkcjonalność i kontrolę dostępu. Ataki na sieci zazwyczaj koncentrują się na pokonaniu jednego lub więcej z tych wspólnych celów.

DOSTĘPNOŚĆ

Zapewnienie dostępności sieci oznacza, że autoryzowani użytkownicy mają dostęp do informacji, usług i zasobów sieciowych. Ataki typu „odmowa usługi" (DoS) to jeden z najczęstszych rodzajów ataków sieciowych na korporacje. Mogą być uruchamiane z dowolnego miejsca na świecie i mają natychmiastowe efekty osłabiające. Ataki na dostępność sieci mogą uniemożliwić klientom, dostawcom i pracownikom zawieranie transakcji biznesowych. Rentowność sprzedawców internetowych zależy od ciągłej dostępności usług sieciowych, takich jak serwer WWW. Nawet najlepsze systemy kryptograficzne stają się nieistotne, jeśli wiadomości nie mogą zostać dostarczone.

POUFNOŚĆ

Termin poufność ma nieco inne znaczenie w kontekście bezpieczeństwa sieci niż w poprzedniej części dotyczącym kryptografii, co oznaczało, że osoby przechwytujące wiadomości nie mogą ich odczytać. W kontekście bezpieczeństwa sieci poufność oznacza zapobieganie uzyskiwaniu przez nieautoryzowanych użytkowników informacji o strukturze sieci, danych przepływających przez sieć, używanych protokołach sieciowych lub wartościach nagłówków pakietów. Załóżmy na przykład, że wewnętrzny pracownik marnuje większość dnia, logując się na stronie pornograficznej, korzystając z szyfrowanego połączenia SSL. Sesja jest w pełni zaszyfrowana, a zawartość pakietów nie jest widoczna dla pracodawcy. Pracodawca może jednak zobaczyć adres IP nadawcy, adres IP odbiorcy, żądanie DNS w celu rozwiązania nazwy hosta (PornographicSite.com), używane numery portów i ilość przesłanych danych. Dostęp do zawartości pakietów może nie być konieczny. Atakujący może zdobyć cenne informacje, pasywnie monitorując ruch przychodzący i wychodzący z sieci firmowej. Nawet jeśli ruch jest zaszyfrowany, atakujący nadal może zobaczyć, które witryny są odwiedzane, ile danych jest wysyłanych lub odbieranych oraz jakie numery portów są używane. Informacje te mogą mieć znaczenie

strategiczne, gdyby zostały zebrane na przykład z ruchu pochodzącego z sieci badawczo-rozwojowej konkurencji. Atakujący może również być w stanie mapować sieć wewnętrzną i pasywnie odciskać palec (identyfikować na podstawie znanych cech) hostów wewnętrznych na podstawie informacji z nagłówka. Na przykład pakiety z komputerów z systemem Microsoft Windows będą miały domyślną wartość TTL wynoszącą 128, podczas gdy pakiety z systemu Mac OS X mają domyślną wartość TTL wynoszącą 64.

FUNKCJONALNOŚĆ

Innym celem do rozważenia przy tworzeniu bezpiecznych sieci jest funkcjonalność. Zapewnienie odpowiedniej funkcjonalności sieci oznacza uniemożliwienie napastnikom zmiany możliwości lub działania sieci. Odpowiednia funkcjonalność sieci obejmuje prawidłowe routing pakietów, prawidłowe rozwiązywanie nazw hostów, wykluczanie niezatwierdzonych protokołów, prawidłowe przypisywanie adresów IP i tak dalej. Na przykład niezadowolony pracownik mógłby zmienić funkcjonalność sieci wewnętrznej za pomocą zatruwania ARP. ARP poisoning przekierowuje ruch sieciowy przez komputer atakującego. Umożliwiłoby to atakującemu skanowanie pakietów wysyłanych przez niezaszyfrowaną sieć lokalną. Pracownik wykorzystałby atak typu man-in-the-middle (MITM), aby wykraść tajemnice handlowe, do których normalnie nie miałby dostępu. Zatrucie ARP zostanie omówione bardziej szczegółowo w dalszej części.

KONTROLA DOSTĘPU

Ostatnim ogólnym celem, który należy wziąć pod uwagę podczas zabezpieczania sieci, jest kontrola dostępu. W kontekście bezpieczeństwa sieci kontrola dostępu to oparta na zasadach kontrola dostępu do systemów, danych i dialogów. Zasadniczo celem jest powstrzymanie atakujących przed dostępem do jakichkolwiek zasobów wewnętrznych. Obejmie to również ograniczenie dostępu do pracowników wewnętrznych. Kontrola dostępu jest tak ważnym celem ogólnym, że Część 5 poświęcona jest szerszej dyskusji na ten temat. Podczas gdy ta Część koncentruje się w szczególności na kontroli dostępu do sieci, następny rozdział skupi się na bezpieczeństwie fizycznym (drzwi, budynki itp.), biometrii, audytach i serwerach katalogowych. W tym rozdziale przyjrzymy się kontrolowaniu dostępu do sieci Ethernet i bezprzewodowych. Dokładniej, przyjrzymy się, jak uwierzytelniać i autoryzować legalny dostęp do sieci wewnętrznych.

Przyszłość bezpiecznych sieci

Zabezpieczanie sieci korporacyjnych jest trudne z kilku powodów. Co roku pojawiają się nowe wektory ataków, czyli sposoby atakowania sieci. Stare wektory ataków, które kiedyś uważano za „rozwiązane", są zmieniane przy użyciu nowszych technologii, mediów lub protokołów. Tworzenie bezpiecznych sieci to proces, który wymaga ciągłej edukacji i adaptacji. Na przykład nowsze telefony komórkowe umożliwiają laptopom bezprzewodowym łączenie się z telefonem komórkowym i udostępnianie połączenia z Internetem. Dopuszczenie telefonów komórkowych do sieci firmowej całkowicie omija procedury kontroli dostępu, zapory sieciowe, ochronę antywirusową, systemy zapobiegania utracie danych i tak dalej.

Cztery główne cele bezpiecznych sieci:

Dostępność - użytkownicy mają dostęp do usług informacyjnych i zasobów sieciowych

Poufność - uniemożliwia nieautoryzowanym użytkownikom uzyskanie informacji o sieci

Funkcjonalność - uniemożliwianie atakującym zmianę możliwości lub normalnego działania sieci

Kontrola dostępu — uniemożliwić atakującym lub nieautoryzowanym pracownikom dostęp do zasobów wewnętrznych

ŚMIERĆ OBWODU

Nie ma zgody co do tego, czy w ogóle można budować bezpieczne sieci. Niektórzy twierdzą, że zabezpieczenia obwodowe są w dużej mierze bezużyteczne. Tradycyjny zamkowy model obrony sieciowej miał dobrych ludzi wewnątrz, a atakujących na zewnątrz. Był dobrze strzeżony pojedynczy punkt wejścia. Jedyne, co musieli zrobić administratorzy sieci, to zabezpieczyć ten punkt wejścia, a atakujący zostaliby powstrzymani. W ostatnich dziesięcioleciach ta mentalność graniczna powoli zanika. „Śmierć obwodu" to wyrażenie używane przez administratorów sieci, aby przekazać ideę, że stworzenie w 100% bezpiecznej sieci jest niemożliwe. Twierdzą, że jest niepraktyczne, jeśli nie niemożliwe, aby przeforsować wszystkie informacje w organizacji przez jeden punkt w organizacji sieci. Wydanie dekretu, że wszyscy pracownicy, w tym prezes, muszą zostawić telefony komórkowe w swoich samochodach, prawdopodobnie spotka się z oporem. Granica między „dobrymi" a „złymi" również się zatarła. Czasami dobrzy ludzie mogą znajdować się poza granicami sieci fizycznej, ale nadal potrzebują dostępu do zasobów wewnętrznych. Pracownicy pracujący zdalnie i partnerstwa z innymi korporacjami to przypadki, w których osoby spoza obwodu potrzebowałyby dostępu do systemów wewnętrznych. I odwrotnie, zbyt często zdarza się, że zły facet zostaje dotychczasowym pracownikiem.

POWRÓT MIASTA

Lepszym paradygmatem bezpieczeństwa sieci jest model miasta. Model miasta nie ma wyraźnego obwodu i istnieje wiele sposobów wejścia do sieci. Podobnie jak w prawdziwym mieście, to kim jesteś, decyduje o tym, do jakich budynków będziesz mieć dostęp. Wymagania bezpieczeństwa dla miasta są znacznie bardziej złożone niż wymagania bezpieczeństwa dla zamku. W mieście potrzebna będzie dodatkowa policja, budynki, drzwi, ogrodzenia i zamki. Z technicznego punktu widzenia będzie to oznaczać więcej wewnętrznych systemów wykrywania włamań, wirtualnych sieci LAN, centralnych serwerów uwierzytelniających i szyfrowanego ruchu wewnętrznego. Postęp technologiczny zmieni sposób, w jaki korzystamy z sieci. Z konieczności zmienią się również sposoby zabezpieczania sieci. W poniższych sekcjach przyjrzymy się kilku bardziej znanym sposobom atakowania sieci.

TEST LXXXVII

a. Wyjaśnij cztery ogólne cele bezpiecznej sieci.

b. Jak można zbierać informacje z zaszyfrowanego ruchu sieciowego?

c. Podaj przykład, w jaki sposób nowa technologia zmniejszyła bezpieczeństwo sieci.

d. Jak model zamku odnosi się do bezpiecznej sieci?

e. Co należy rozumieć przez „śmierć obwodu"?

f. Jak model miasta odnosi się do bezpiecznej sieci?

ATAKI DoS

Jednym z najczęstszych ataków sieciowych, o których usłyszysz w wiadomościach, jest atak typu „odmowa usługi" (DoS). Atak DoS ma na celu uniemożliwienie legalnym użytkownikom dostępu do serwera lub sieci. Jeśli chodzi o cele ogólne omówione wcześniej, ataki DoS są sposobem na zmniejszenie dostępności. Atak typu „odmowa usługi" (DoS) ma na celu uniemożliwienie dostępu do serwera lub sieci przez uprawnionych użytkowników poprzez zalanie go pakietami ataku. Ataki DoS zdarzają się codziennie. Korporacje i podmioty rządowe są głównymi celami atakujących. Wcześniej w

pokrótce przyjrzałeś się jednemu rodzajowi ataku DoS, zwanemu atakiem rozproszonym DoS (DDoS). W tej sekcji dokładniej przyjrzymy się mechanice ataku DDoS, a także kilku innym rodzajom ataków DoS.

Odmowa usługi. . . Ale nie atak

Zanim przyjrzymy się szczegółom działania ataków DoS, należy wiedzieć, że nie wszystkie przerwy w świadczeniu usług są atakami. Ze względu na częste występowanie ataków Dos i ich widoczność w prasie, łatwo jest zrzucić winę na przerwy w działaniu usług na atakujących z zewnątrz. Pracownicy i menedżerowie wewnętrzni są niewinni za przestoje, którym mogli zapobiec lub nawet spowodować.

BŁĘDNE KODOWANIE

Na przykład w 2011 r. Newsnet Scotland twierdził, że padł ofiarą ataku DoS ze strony prounijnych przeciwników politycznych. Okazało się jednak, że przyczyną utraty usługi było tandetne kodowanie. Dyrektor naczelny Newsnet Scotland, Alex Porter, wydał poprawkę stwierdzającą, że „byliśmy w stanie rozszyfrować, że nie był to atak DDoS, jak wcześniej sądzono. Rzecz w tym, że dostosowanie do modułu stworzyło w istocie skrót, który powodował dużą cykliczną aktywność na serwerze."

POLECENIA Z DUŻYCH STRON

Inna częsta utrata usługi bez ataku ma miejsce, gdy duża witryna prowadzi do znacznie mniejszej witryny. Jest to częste zjawisko w agregatorach wiadomości, takich jak Slashdot, Drudge Report i The Huffington Post, które zawierają linki do mniejszych witryn zawierających artykuły z wiadomościami. Mniejszy serwis informacyjny może zostać przytłoczony dramatycznym wzrostem ruchu. Chociaż efekt jest taki sam jak w przypadku ataku DoS, utrata usługi była niezamierzona. Duży wzrost ruchu lub utrata usługi niekoniecznie oznacza złośliwy atak DoS.

Cel ataków DoS

Ostatecznym celem ataku DoS jest wyrządzenie szkody. W przypadku korporacji może to przybrać formę strat związanych ze sprzedażą online, reputacją branży, wydajnością pracowników lub lojalnością klientów. Ataki DoS mogą wyrządzić szkody poprzez (1) zatrzymanie krytycznej usługi lub (2) powolną degradację usług w miarę upływu czasu.

ZATRZYMAJ USŁUGI KRYTYCZNE

Atakujący często przeprowadzają ataki DoS na najważniejszą usługę organizacji. Najpopularniejszą usługą atakowaną przez atakujących jest HTTP. Usługi internetowe są popularnym celem ze względu na szkody gospodarcze, jakie można wyrządzić. Na przykład strony internetowe Amazon, Walmart i Gap były nieosiągalne przez około godzinę podczas jednego z najbardziej ruchliwych sezonów zakupowych w roku. Dwa dni przed Bożym Narodzeniem przeprowadzono atak DDoS na dostawcę DNS (Neustar) na te duże firmy. Kupujący nie byli w stanie uzyskać dostępu do niczego od tych sprzedawców internetowych ani ich kupić. Oprócz zamknięcia strony internetowej firmy, osoby atakujące mogą uniemożliwić pracownikom dostęp do ich poczty e-mail, serwerów plików lub zamknąć zastrzeżoną aplikację.

DEGRADACJA UJSŁUG

Zazwyczaj ataki DoS na krytyczne usługi są łatwe do zidentyfikowania i nie trwają długo. Administratorzy sieci będą działać szybko, aby powstrzymać znane ataki. Jednak najbardziej szkodliwe ataki to te, których nie można zidentyfikować. Te ataki trwają długo. Atak, który powoli degraduje usługi, jest trudniejszy do wykrycia, ponieważ nie następuje gwałtowna zmiana jakości usług.

Administratorzy sieci nie widzą wyraźnego rozróżnienia między rzeczywistym wzrostem ruchu sieciowego a postępującym atakiem DoS. Mogą być zmuszeni do niepotrzebnych nakładów inwestycyjnych na dodatkową przepustowość, sprzęt i oprogramowanie.

TEST LXXXXVIII

a. Co to jest atak typu „odmowa usługi”?

b. Co poza atakiem DoS może spowodować awarię serwera internetowego firmy?

c. Jakie są główne cele ataków DoS?

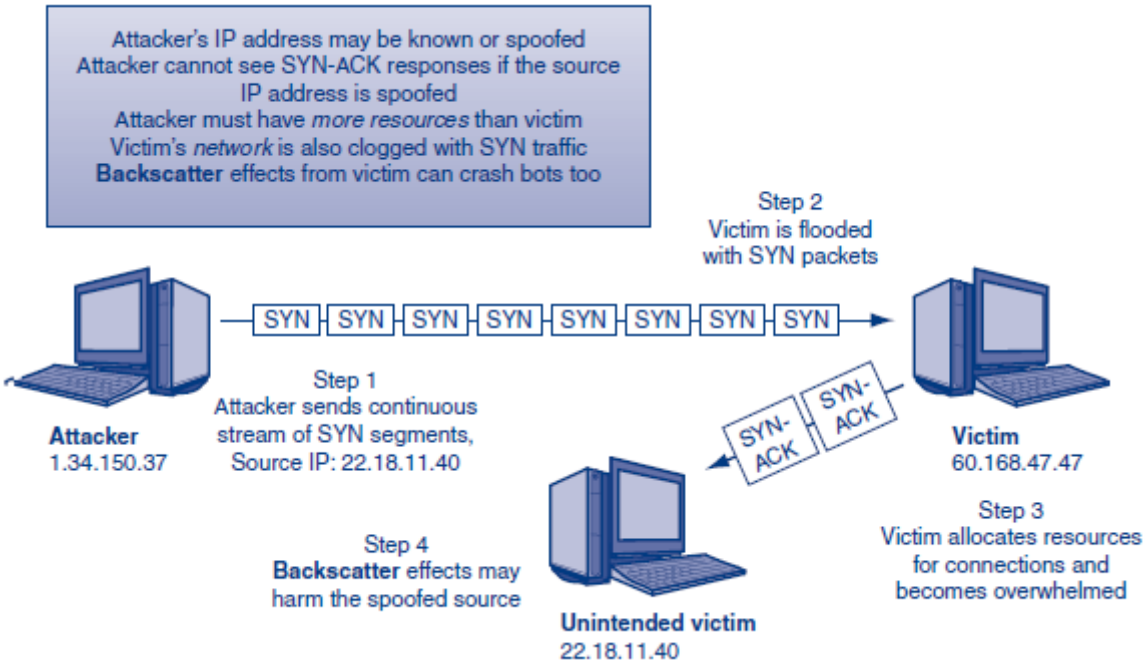
d. Czy powolna degradacja usług jest gorsza niż całkowity przestój? Czemu?

Metody ataków DoS

Istnieją cztery główne metody, którymi posługują się napastnicy przeprowadzając atak DoS. Mogą również stosować hybrydowe ataki DoS, które wykorzystują elementy każdej metody. Poniższa lista nie stanowi wyczerpującej listy wszystkich typów ataków DoS. Jest to raczej wprowadzenie do metod DoS. Główne metody ataków DoS, którym się przyjrzymy, to (1) bezpośrednie/pośrednie, (2) pośrednie, (3) odbite i (4) wysyłanie zniekształconych pakietów. Każda metoda ma swoje zalety i wady. Prostsze ataki mogą być łatwiejsze do wdrożenia, ale są też łatwiejsze do powstrzymania. Z drugiej strony ataki, które są z natury bardziej złożone, mogą być niezwykle trudne do powstrzymania bez powodowania dodatkowych szkód.

ATAKI BEZPOŚREDNIE I POŚREDNIE

Najprostszą formą ataku DoS jest atak bezpośredni, podobny do tego pokazanego na rysunku 4-3.



Atak bezpośredni ma miejsce, gdy atakujący próbuje zalać ofiarę strumieniem pakietów bezpośrednio z komputera atakującego. Atak pośredni próbuje zalać komputer ofiary w ten sam sposób, ale adres IP

atakującego jest sfałszowany (tj. sfałszowany), a atak wydaje się pochodzić z innego komputera (Krok 1).

Powódź. Ataki bezpośrednie lub pośrednie mogą się powieść tylko wtedy, gdy napastnik może zalać ofiarę większą liczbą żądań, niż ofiara jest w stanie obsłużyć (Krok 2). Atakujący musi mieć większą przepustowość, pamięć (RAM) i/lub moc procesora niż ofiara (Krok 3). Biorąc pod uwagę wielkość większości firmowych farm serwerów, jest mało prawdopodobne, że pojedynczy użytkownik będzie w stanie wygenerować wystarczający ruch, aby skutecznie zdegradować istniejące usługi. Serwery korporacyjne mogą obsłużyć więcej żądań, niż może wygenerować pojedynczy atakujący.

Podszywanie się. Bezpośrednie ataki są rzadkie. Atakujący nie lubią bezpośrednio atakować ofiar, ponieważ ich źródłowy adres IP jest wyświetlany we wszystkich przychodzących pakietach. Atakujący wolą raczej używać sfałszowanych adresów IP, które ukrywają ich adres IP. Minusem fałszowania adresu IP jest to, że atakujący nie może uzyskać bezpośredniej informacji zwrotnej na temat ataku. Muszą polegać na pośrednich środkach monitorowania ataku, takich jak wysyłanie żądań do ofiary z innego komputera w celu przetestowania dostępności.

Rozproszenie wsteczne. Efektem ubocznym fałszowania adresu IP przez atakującego jest rozproszenie wsteczne. Rozproszenie wsteczne występuje, gdy ofiara wysyła odpowiedzi na sfałszowany adres IP używany przez atakującego i nieumyślnie zaleje niezamierzoną ofiarę (Krok 4). Odmiana efektu rozproszenia wstecznego jest wykorzystywana do celowania w ofiary w ataku odbitym.

Rodzaje wysyłanych pakietów. Czasami ataki DoS są nazywane po typie pakietu wysłanego podczas ataku, a nie od metody ataku. Niektóre ataki DoS opisane w tej sekcji mogą wykorzystywać wiele typów pakietów (np. DDoS). Inne metody ataku, takie jak powódź Smurf, wykorzystują jeden typ pakietu. Poniżej znajduje się tylko kilka typów pakietów, które mogą zostać wysłane w ataku DoS.

TCP : Transmission Control Protocol : Gwarantuje dostarczanie pakietów przez Internet

SYN : Synchronizuj : Pierwsza część trójstronnego uzgadniania TCP w celu nawiązania połączenia sieciowego

SYN-ACK : Synchronize-Acknowledge : Druga część trójstronnego uzgadniania TCP wysłanego w odpowiedzi na SYN

ICMP : Internet Control Message Protocol : Protokół nadzorczy używany do wysyłania komunikatów o błędach między komputerami

HTTP : Hypertext Transfer Protocol : Protokół do przesyłania danych przez Internet

• SYN FloodAvictim jest zalewany pakietami SYN w celu nawiązania wielu półotwartych połączeń TCP. Pamięć jest przydzielana dla każdego fałszywego połączenia powodującego brak pamięci i awarię ofiary.

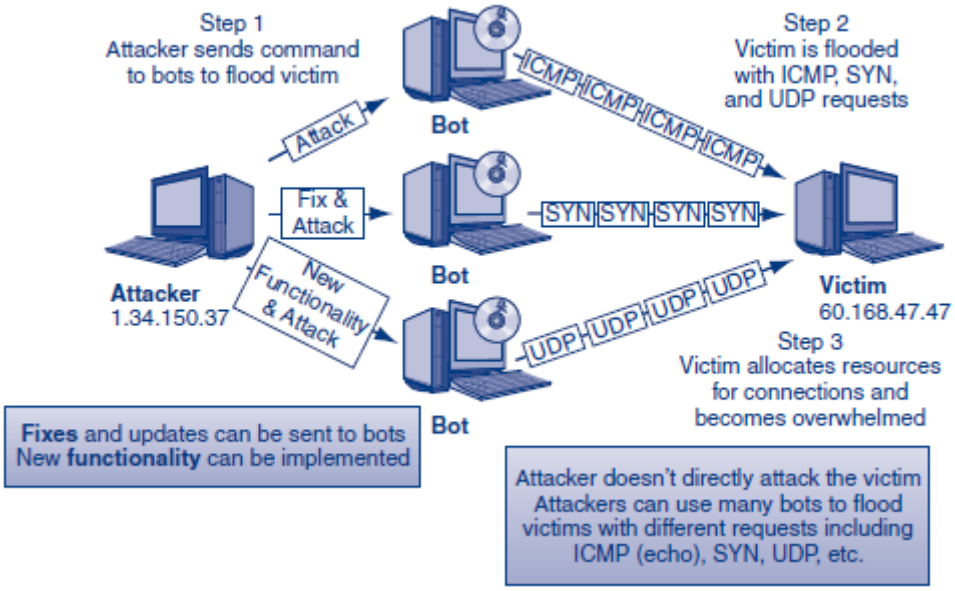
• Ping Flood Ofiara jest zalewana pakietami ICMP (znanymi również jako żądania echa), które wydają się być normalnym ruchem nadzorczym. Przepustowość i cykle procesora są zużywane do punktu, w którym ofiara ulega awarii.

• HTTP Flood Ofiara, zazwyczaj serwer sieciowy, jest zalewana żądaniami sieciowymi w warstwie aplikacji. Serwer sieciowy ulega awarii z powodu niewystarczającej pamięci i mocy procesora.

Przykład powodzi SYN. ASYN flood lub półotwarty atak TCP ma miejsce, gdy atakujący wysyła dużą liczbę segmentów TCP SYN do serwera ofiary (Krok 1). Każdy segment SYN rozpoczyna proces otwierania sesji TCP na serwerze (Krok 2). Serwer odkłada pamięć RAM i inne zasoby na połączenie. Serwer następnie odsyła segment SYN/ACK. Atakujący nigdy nie kończy otwierania połączenia, wysyłając ostateczne ACK. Gdy atakujący wysyła więcej segmentów SYN, ofiara hosta odkłada zasoby, dopóki nie ulegnie awarii lub odmówi udostępnienia kolejnych połączeń, nawet uprawnionym użytkownikom (Krok 3). Tak czy inaczej, atakujący wygrywa.

POŚREDNIK

Drugą podstawową metodą DoS stosowaną przez atakujących jest wykorzystanie pośredników do zaatakowania ofiary. Pośrednicy, zwykle określani jako boty, są w rzeczywistości zaatakowanymi hostami, na których działa złośliwe oprogramowanie kontrolowane przez atakującego. Atak DoS rozpoczyna się, gdy botmaster wysyła sygnał do botów, aby zaatakowały ofiarę. Atakujący kontrolujący boty w skoordynowanym ataku na ofiarę, pokazany na rysunku, jest znany jako atak typu rozproszona odmowa usługi (DDoS).



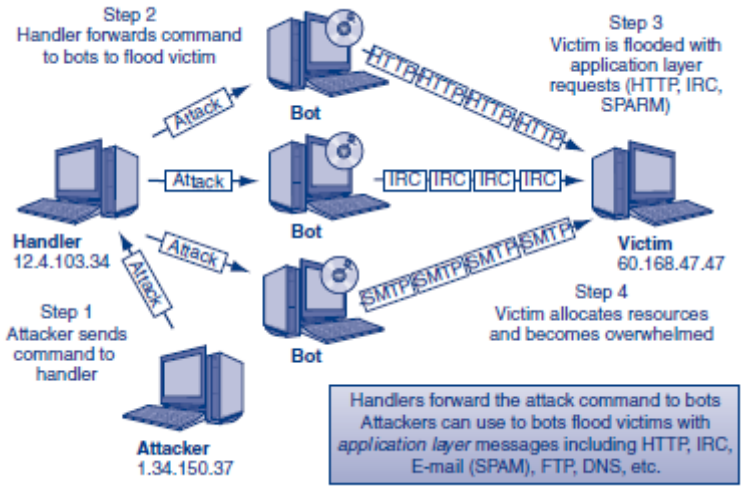
Ataki DDoS są najczęstszą formą ataków DoS z kilku powodów. Po pierwsze, tożsamość napastnika może być ukryta za warstwami botów (Krok 1), które bezpośrednio atakują ofiarę (Krok 2). Po drugie, możliwość kontrolowania tysięcy botów może zapewnić atakującemu zasoby potrzebne do przytłoczenia ofiary (Krok 3).

Boty. Jak pokazuje Rysunek, botmaster (atakujący) nie ogranicza się do wysyłania poleceń ataku do zainstalowanych botów. Botmaster może również wysyłać aktualizacje oprogramowania do botów. Najprostsze aktualizacje są wysyłane w celu naprawienia błędów w kodzie programu. W przeszłości twórcy złośliwego oprogramowania często odkrywali po wydaniu, że program zawiera nieprzewidziane błędy, które uniemożliwiały mu działanie zgodnie z założeniami. Te wady umożliwiły firmom antymalware zniszczenie wielu z tych programów. Jednak możliwość pobierania aktualizacji umożliwia twórcom złośliwego oprogramowania naprawianie błędów.

Rysunek pokazuje, że botmaster może wysyłać aktualizacje, które dają botom nowe funkcje. Na przykład wiele armii botów jest pierwotnie zaprogramowanych do wysyłania spamu. Później, gdy wysiłki antyspamowe blokują adresy IP tych botów, atakujący może wysyłać aktualizacje, aby

umożliwić botom przeprowadzanie ataków DoS. Atakujący może następnie użyć ich do przeprowadzenia ataków lub wydzierżawienia botnetu innym przestępcom w celu przeprowadzenia ataków DoS. W 2003 roku botnety z 10 000 komputerów można było kupić za 500,5 USD

Obsługa. Zarządzanie tysiącami botów może być trudne. Programy obsługi to dodatkowa warstwa zhakowanych hostów, która służy do zarządzania dużymi grupami botów (Krok 1).



Programy obsługi, czasami nazywane serwerami dowodzenia i kontroli, ułatwiają koordynację ataku i są mniej widoczne. Dodatkowa warstwa utrudnia również śledzenie ataku z powrotem do pierwotnego napastnika (Krok 2). Rysunek pokazuje również, że programy obsługi mogą nakazać botom wysyłanie różnych pakietów w zależności od docelowej usługi. Atakujący mogą atakować Internet, transport i dobrze znane usługi warstwy aplikacji, w tym HTTP, IRC (czat), SMTP (Spam), FTP, DNS itd. (Krok 3). Ofiary mogą być nawet przytłoczone kombinacją różnych rodzajów pakietów (Krok 4).

TEST LXXXIX

a. Jaka jest różnica między bezpośrednim a pośrednim atakiem DoS?

b. Co to jest rozproszenie wsteczne?

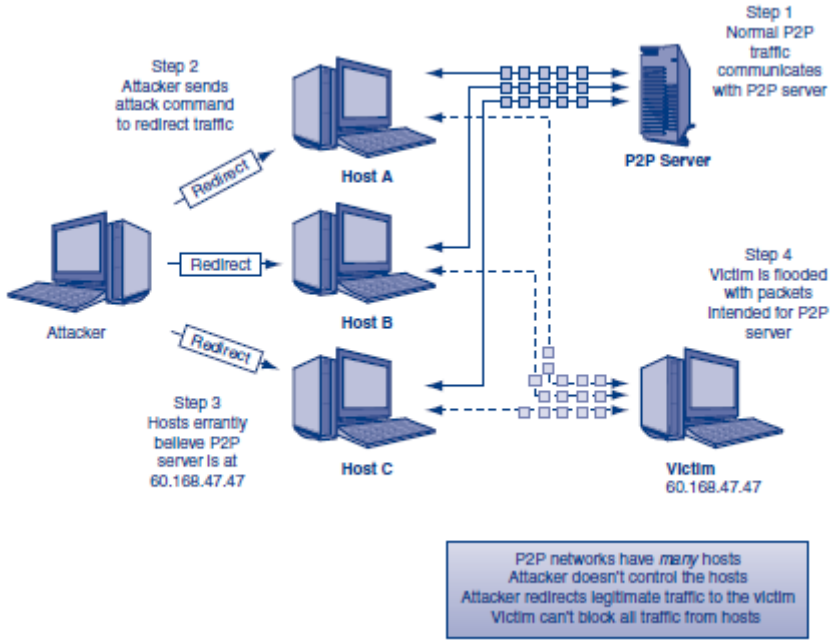
c. Jakie rodzaje pakietów można wysyłać w ramach ataku DoS?

d. Opisz powódź SYN.

e. Jak działa atak DDoS?

f. Co robi przewodnik?

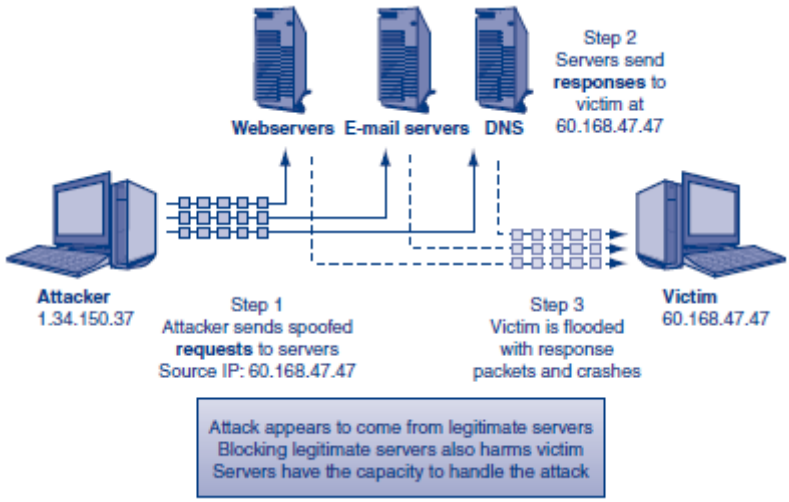
Przekierowanie peer-to-peer. Podobnie jak w przypadku ataku DDoS, atak przekierowania peer-to-peer (P2P) wykorzystuje wiele hostów do przytłoczenia ofiary przy użyciu normalnego ruchu P2P (Krok 1).



Atak przekierowujący P2P różni się od tradycyjnego ataku DDoS na kilka sposobów. Atakujący nie musi kontrolować każdego z hostów (tj. robić z nich botów) używanych do atakowania ofiary. Atakujący musi jedynie przekonać hosty do przekierowania swojego legalnego ruchu P2P (Krok 2) z serwera P2P do ofiary (Krok 3). Nastąpiła zmiana wzorca ruchu, ale ogólny ruch jest taki sam. Ofiara nie może zablokować całego ruchu przychodzącego bez blokowania uprawnionych użytkowników (Krok 4). Zatrzymanie ataku zależy od rozmiaru sieci P2P i zdolności ofiary do zablokowania określonego portu P2P. Przekierowanie P2P to odpowiednik wystawienia domu znajomego na sprzedaż w lokalnych ogłoszeniach (najlepiej po bardzo niskiej cenie). Ofiara jest zalana wieloma legalnymi nabywcami domów.

ATAK ODBIJAJĄCY

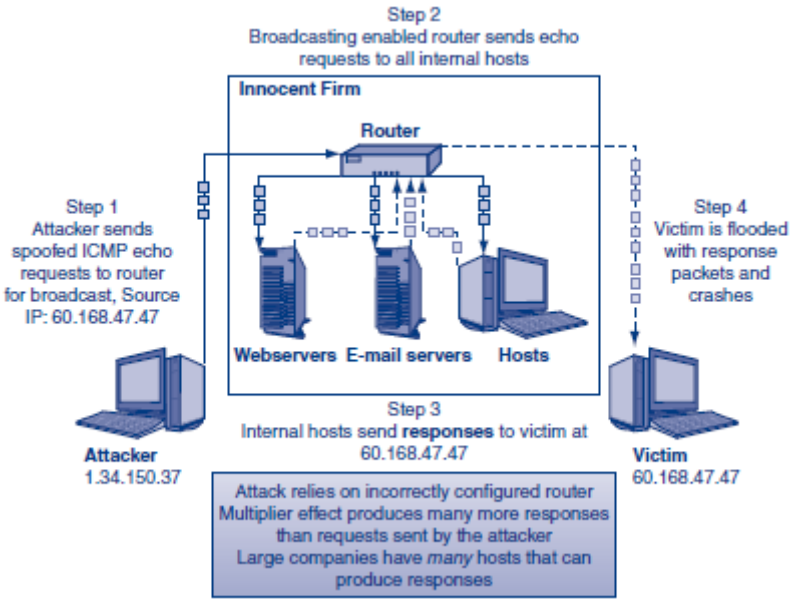
Trzecią metodą ataku DoS jest atak odbity. Podobnie jak w przypadku przekierowania P2P, atak odbity wykorzystuje odpowiedzi z legalnych usług do zalania ofiary. Rysunek 4-8 pokazuje, że atakujący wysyła sfałszowane żądania do istniejących legalnych serwerów (Krok 1).



Serwery wysyłają następnie wszystkie odpowiedzi do ofiary (Krok 2). Nie ma przekierowania ruchu. Atakujący wybierają serwery, które zwykle odbierają duży ruch i mają wystarczającą pojemność, aby

przytłoczyć ofiarę (Krok 3). Z punktu widzenia ofiary wydaje się, że atak pochodzi z legalnych serwerów. Próbując powstrzymać atak, ofiara może próbować zablokować serwery, które odzwierciedlają atak. Może to spowodować dodatkowe szkody dla ofiary. Ofiara może nieświadomie zablokować partnera korporacyjnego, usługi DNS, swojego dostawcę poczty e-mail lub inną krytyczną usługę. Wykorzystywanie botnetu w ataku odbitym jest znane jako rozproszony atak odbitej odmowy usługi (DRDoS).

Powódź Smurf. Powódź Smurf to odmiana ataku odbitego, w którym wykorzystuje się niepoprawnie skonfigurowane urządzenie sieciowe (router) do zalania ofiary. Atakujący wysyła sfałszowane żądanie echa ICMP do urządzenia sieciowego (Krok 1), które ma włączone rozgłaszanie do wszystkich hostów wewnętrznych.



Urządzenie sieciowe przekazuje żądanie echa do wszystkich hostów wewnętrznych (Krok 2). Wszystkie hosty wewnętrzne odpowiadają na sfałszowane żądanie echa ICMP (Krok 3) i ofiara zostaje zalana. Atakujący korzysta z efektu mnożnika, ponieważ na jedno żądanie ICMP odpowiada wiele hostów (Krok 4). Wyłączenie rozgłaszania do hostów wewnętrznych zatrzyma powódź Smerfa.

WYSYŁANIE NIEPRAWIDŁOWYCH PAKIETÓW

Ostatnią metodą DoS stosowaną przez atakujących jest wysyłanie zniekształconych pakietów, które spowodują awarię ofiary. Na przykład ping of death to dobrze znany starszy atak, który wykorzystuje nielegalnie duży pakiet IP do awarii systemu operacyjnego ofiary. Ta usterka została naprawiona i atak jest już rzadko używany. Jednak koncepcja wysyłania źle sformatowanych pakietów do hostów ulegających awarii jest nadal używana. Pod koniec 2010 roku badacze bezpieczeństwa Collin Mulliner i Nico Golde wykazali, że zniekształcone wiadomości SMS (znane również jako wiadomości tekstowe) mogą zostać wykorzystane do awarii telefonów komórkowych podczas ataku, który nazwali SMS-em śmierci6. Zauważyli, że Samsung, Sony Ericsson, Motorola, wszystkie telefony LG były podatne na atak. Błędy w systemach operacyjnych hosta podatne na zniekształcone pakiety będą nadal ujawniane i wykorzystywane.

TEST XC

a. Jak działa atak P2P?

b. Jak działa atak odbity?

c. Co to jest atak DRDoS i jak działa?

d. Co to jest powódź Smerfów?

e. Jaki typ pakietu jest wysyłany podczas powodzi Smerfa? Czemu?

f. Jak źle sformatowany pakiet może spowodować awarię hosta?

W wiadomościach

„Wirtualne sit-in" zostało zorganizowane przez mianowanego profesora UC San Diego Ricardo Domingueza jako akt „elektronicznego nieposłuszeństwa obywatelskiego". Zwolenników zachęcano do odwiedzenia strony internetowej Biura Prezydenta ds. systemu edukacji Uniwersytetu Kalifornijskiego. Oczywistym celem było spowolnienie dostępu do witryny w proteście przeciwko cięciom budżetowym w kalifornijskim systemie edukacyjnym. Administratorzy na Uniwersytecie Kalifornijskim w San Diego uznali wirtualną okupację za kryminalny atak typu „odmowa usługi" (DoS). Jednak w przeciwieństwie do typowego ataku DoS (lub DDoS), przestój nie został spowodowany przez pojedynczą nieautoryzowaną osobę kontrolującą wiele botów. Pozorne spowolnienie spowodowane było wielokrotnym dostępem ponad 400 autoryzowanych użytkowników do publicznej witryny internetowej. Jak na ironię, profesor Ricardo Dominguez został mianowany przez UC San Diego za swoją pracę nad elektronicznym nieposłuszeństwem obywatelskim.

Obrona przed atakami typu „odmowa usługi"

Większość ataków DoS jest łatwa do wykrycia. Jednak wiele z nich jest bardzo trudnych do powstrzymania, nawet jeśli zostaną wykryte. Prawie wszystkie główne firewalle graniczne również wykonują filtrowanie DoS. W Części 6 („Zapory ogniowe") omówimy bardziej szczegółowo, w jaki sposób można skonfigurować zapory ogniowe w celu powstrzymania ataków zewnętrznych. Poniżej znajdują się trzy popularne sposoby powstrzymania wspomnianych wcześniej ataków DoS.

CZARNE OTWORY

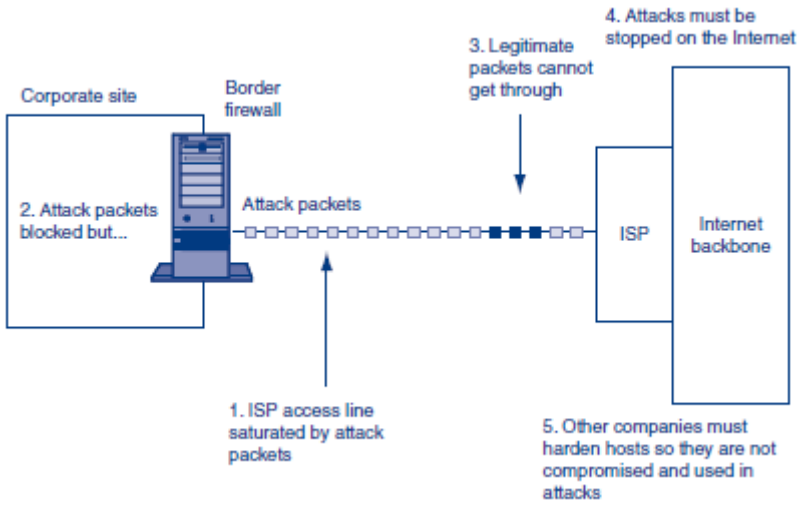
Jednym z możliwych sposobów powstrzymania ataku DoS jest odrzucenie wszystkich pakietów IP od atakującego. Nazywa się to czarną dziurą. Umieszczenie atakującego w czarnych dziurach nie jest dobrą długoterminową strategią, ponieważ atakujący mogą szybko zmienić źródłowe adresy IP. Czarna dziura może mieć szkodliwe skutki, jeśli jest wykonywana automatycznie. Atakujący może świadomie sfałszować pakiety ataków z adresami IP partnera korporacyjnego. Automatyczne zabezpieczenia mogą blokować legalny ruch od tego partnera i powodować dodatkowe problemy.

WERYFIKACJA UTRZYMANIA DŁONI

Niektóre zapory rozwiązują zalewy SYN Flood, wstępnie weryfikując uzgadnianie TCP. Odbywa się to poprzez tworzenie fałszywych otwarć. Za każdym razem, gdy nadchodzi segment SYN, zapora sama odsyła segment SYN/ACK bez przekazywania segmentu SYN do serwera docelowego. Tylko wtedy, gdy zapora otrzyma z powrotem potwierdzenie ACK, co ma miejsce tylko w przypadku prawidłowych połączeń, zapora wysyła oryginalny segment SYN do serwera, dla którego pierwotny segment SYN był przeznaczony. Zapora nie odkłada zasobów na połączenie, gdy nadchodzi segment SYN, więc obsługa dużej liczby fałszywych segmentów SYN jest tylko niewielkim obciążeniem.

OGRANICZENIE STAWKI

W przypadku bardziej subtelnych ataków DoS można zastosować ograniczanie szybkości, aby zredukować określony rodzaj ruchu do rozsądnej ilości. Na przykład skutki powodzi Smerf można złagodzić poprzez ograniczenie liczby pakietów ICMP wchodzących do sieci. Nadal można korzystać z transmisji do sieci wewnętrznej, ale z ograniczoną szybkością. Jest to dobre, jeśli atak jest wymierzony w pojedynczy serwer, ponieważ utrzymuje linie transmisyjne przynajmniej częściowo otwarte dla innej komunikacji. Jednak ograniczanie szybkości frustruje zarówno atakujących, jak i legalnych użytkowników. Pomaga, ale nie rozwiązuje problemu. Jeszcze bardziej niepokojące jest to, że gdy ruch DoS zatka linię dostępową witryny prowadzącą do Internetu, graniczna zapora ogniowa nie może nic zrobić, aby złagodzić sytuację.



Ogólnie rzecz biorąc, ataki DoS to problemy społeczności, które można powstrzymać tylko z pomocą dostawców usług internetowych i organizacji, których komputery są przejmowane jako boty i wykorzystywane do atakowania innych firm.

TEST XCI

a. Co to jest czarna dziura?

b. Czy czarna dziura jest skuteczną obroną przed atakami DoS? Czemu?

c. Jak można złagodzić skutki powodzi SYN?

d. Co to jest fałszywe otwarcie?

e. Dlaczego ograniczanie szybkości jest dobrym sposobem na zmniejszenie obrażeń niektórych ataków DoS?

f. Dlaczego ma ograniczoną skuteczność?

g. Dlaczego ochrona przed atakami DoS jest problemem społeczności, a nie tylko problemem, który muszą rozwiązać poszczególne firmy będące ofiarami przestępstw?

ZATRUCIE ARP

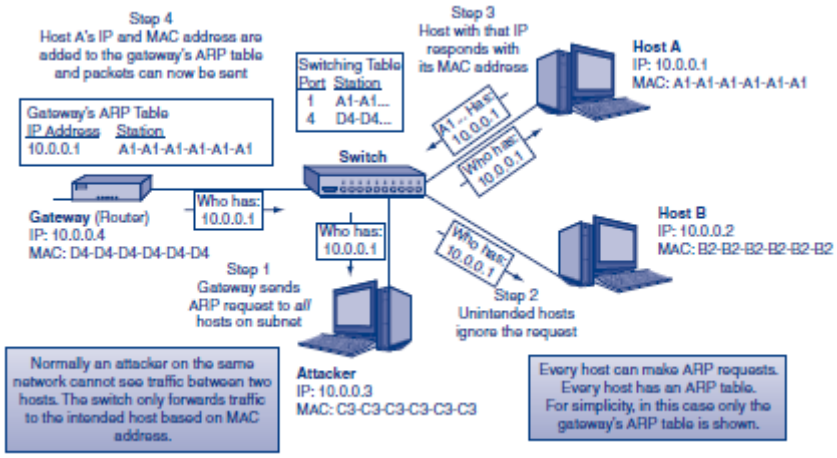
Protokół ARP (Address Resolution Protocol) służy do rozwiązywania 32-bitowych adresów IP (np. 55.91.56.21) na 48-bitowe lokalne adresy MAC (np. 01-1C-23-0E-1D-41). Hosty w tej samej sieci muszą znać swoje adresy MAC, zanim będą mogły wysyłać i odbierać pakiety przy użyciu adresów IP. Hosty budują tabele ARP, podobne do pokazanej na rysunku, wysyłając do siebie żądania i odpowiedzi ARP.

Internet Address	Physical Address	Type
55.91.74.11	f8-66-f2-75-58-7f	dynamic
55.91.74.12	00-24-e8-c4-df-b1	dynamic
55.91.74.13	00-22-19-03-1a-ff	dynamic
55.91.74.14	00-15-c5-41-d9-04	dynamic
55.91.74.15	5c-26-0a-0f-7d-c9	dynamic

ARP poisoning to atak sieciowy, który manipuluje tablicami ARP hosta w celu przekierowywania ruchu w sieci lokalnej (LAN). Atakujący może przekierować ruch w celu przeprowadzenia ataku typu man-in-the-middle lub zatrzymać to wszystko razem w ataku ARP DoS. Zatruwanie ARP działa tylko w ruchu LAN. Wymaga to od atakującego posiadania komputera w sieci lokalnej, aby zatruwanie ARP zadziałało. Przekierowywanie ruchu z wykorzystaniem ARP poisoning jest atakiem zarówno na funkcjonalność, jak i poufność sieci. Atakujący zmienia normalne działanie sieci i zbiera informacje o ruchu w sieci. Atak ARP DoS to atak na dostępność sieci poprzez przekierowanie ruchu do nieistniejącego hosta, a tym samym wymuszenie jego odrzucenia. Aby zrozumieć, jak działa zatrucie ARP, najpierw przyjrzymy się, jak normalnie działa ARP. Następnie zobaczymy, jak żądania i odpowiedzi ARP można wykorzystać w zatruwaniu ARP i ataku ARP DoS.

Normalna praca ARP

Rysunek pokazuje, jak normalnie działa ARP w sieci LAN.



Jeśli brama (router) odbiera pakiet zaadresowany do hosta wewnętrznego (10.0.0.1), wysyła żądanie ARP do każdego hosta w sieci LAN z pytaniem, czy mają ten adres IP (Krok 1). Odpowiada tylko host, który ma żądany adres IP. Wszystkie inne hosty ignorują żądanie (Krok 2). W tym przykładzie host A miał żądany adres IP (10.0.0.1). Host A odpowiada odpowiedzią ARP, która zawiera jego adres fizyczny lub adres MAC (A1-A1-A1-A1-A1-A1) (Krok 3).

Przełącznik rejestruje adresy MAC bramy i hosta A, a także ich odpowiednie numery portów. Brama odbiera odpowiedź ARP i rejestruje adres IP hosta A oraz odpowiadający mu adres MAC (Krok 4). Teraz, gdy brama ma adres MAC hosta A, może przekazywać wszystkie pakiety zaadresowane do 10.0.0.1. Przełącznik sprawdza tylko adres MAC, gdy pakiet jest przekazywany z bramy do hosta A. Przełącznik nie sprawdza adresów IP w pakietach. Inne hosty w sieci LAN nie widzą żadnych pakietów adresowanych do hosta A, ponieważ przełącznik przekazuje pakiety na podstawie numerów portów i adresów MAC w swojej tabeli przełączania. Ponieważ brama zaadresowała pakiet do A1-A1-A1-A1-A1-

A1, musi on wyjść do portu 1, jak pokazano w tabeli przełączania. Żaden inny host nie widzi ruchu hosta A.

PROBLEM

Problem z żądaniami i odpowiedziami ARP polega na tym, że nie wymagają one uwierzytelniania ani weryfikacji. Wszystkie hosty ufają wszystkim odpowiedziom ARP. Spoofing ARP wykorzystuje fałszywe odpowiedzi ARP do mapowania dowolnego adresu IP na dowolny adres MAC. Sfałszowane odpowiedzi ARP są rozgłaszane do innych hostów w sieci LAN. Dzięki temu atakujący może manipulować tabelami ARP na wszystkich hostach LAN.

TEST XCII

a. Dlaczego gospodarze używają ARP?

b. Czy zatrucie ARP może być używane poza siecią LAN? Dlaczego nie?

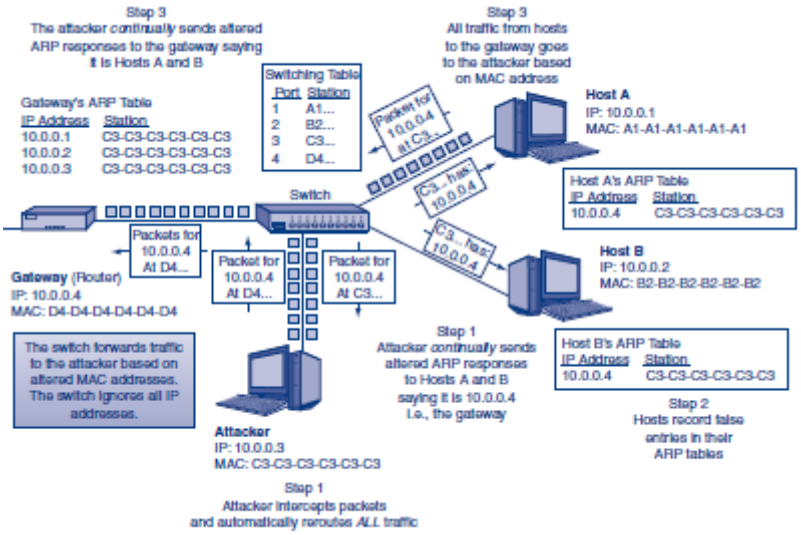
c. Dlaczego hosty wysyłają żądania ARP?

d. Co to jest spoofing ARP?

e. W jaki sposób atakujący może wykorzystać fałszowanie ARP do manipulowania tablicami ARP hosta?

Zatrucie ARP

Rysunek pokazuje, w jaki sposób zatrucie ARP może zostać wykorzystane do przekierowania ruchu w przypadku ataku MITM.



Atakujący rozpoczyna atak, wysyłając ciągły strumień niezamówionych odpowiedzi ARP do wszystkich hostów w sieci LAN (z wyjątkiem bramy) (Krok 1). Ta fałszywa odpowiedź ARP informuje inne hosty w sieci LAN, że brama (10.0.0.4) jest teraz na C3-C3-C3-C3-C3-C3. Hosty w sieci LAN rejestrują fałszywą odpowiedź ARP w swoich tabelach ARP (Krok 2). Teraz błędnie wierzą, że brama (10.0.0.4) znajduje się na C3-C3-C3-C3-C3-C3 (atakujący). Wszelkie pakiety, które chcą wysłać, będą adresowane do 10.0.0.4 w C3-C3-C3-C3-C3-C3. Ponieważ przełącznik sprawdza tylko adresy MAC, nie może zidentyfikować nieprawidłowej rozdzielczości ARP wysyłanej do wszystkich innych hostów. Po prostu przekazuje wszystkie pakiety na podstawie adresu MAC. Nie sprawdza adresu IP w pakiecie. Teraz, gdy atakujący pomyślnie przekierował ruch hosta, musi przekierować ruch przychodzący i wychodzący z bramy. Używa podobnej sfałszowanej odpowiedzi ARP, aby zatruć bramę. Atakujący wysyła ciągły strumień

sfałszowanych odpowiedzi ARP do bramy, informując, że wszystkie inne hosty wewnętrzne znajdują się w C3-C3-C3-C3-C3-C3 (Krok 3). Brama rejestruje wszystkie wewnętrzne adresy IP (10.0.0.1, 10.0.0.2 i 10.0.0.3) oraz ten sam adres MAC (C3-C3-C3-C3-C3-C3) w swojej tablicy ARP. Każdy pakiet otrzymany przez bramę zostanie przesłany do tego samego hosta wewnętrznego (atakującego), ponieważ wszystkie wewnętrzne adresy IP zostaną przetłumaczone na ten sam adres MAC (C3-C3-C3-C3-C3-C3). Atakujący z powodzeniem wykorzystał sfałszowane odpowiedzi ARP do zapisania fałszywych wpisów w tabelach ARP dla wszystkich hostów wewnętrznych i bramy. Cały ruch wysyłany z hostów wewnętrznych do bramy trafi do atakującego (Krok 4). Cały ruch z bramy przechodzi również przez atakującego i jest teraz przekierowywany przez jego komputer w ramach ataku MITM (Krok 5). Należy zauważyć, że atakujący musi mieć dostęp do sieci lokalnej, aby ten atak zadziałał. Atakujący musi również wysyłać ciągły strumień sfałszowanych odpowiedzi ARP, aby uniemożliwić samokorygowanie tabel ARP drugiego hosta.

TEST XCIII

a. Wytłumacz zatrucie ARP?

b. Dlaczego atakujący musi wysyłać ciągły strumień niezamówionych odpowiedzi ARP?

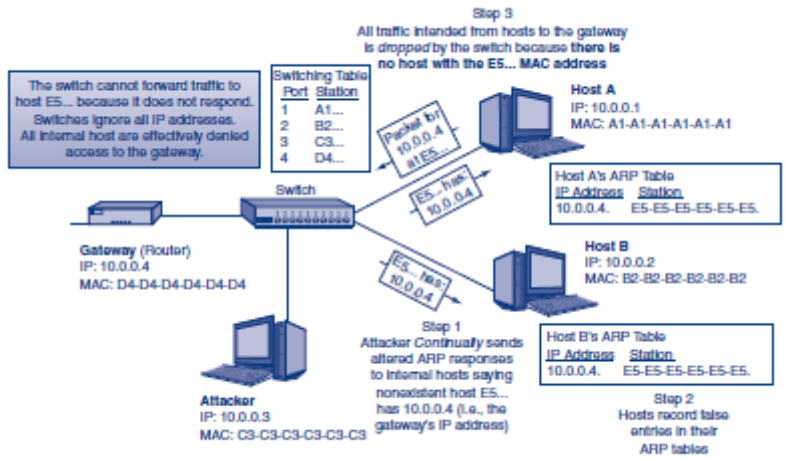
c. Czy przełączniki rejestrują adresy IP? Dlaczego nie?

d. Czy atakujący musi również zatruwać tabele ARP bramki? Czemu?

e. Dlaczego cały ruch sieciowy przechodzi przez atakującego po zatruciu sieci?

Atak ARP DoS

Po niewielkiej modyfikacji te same sfałszowane odpowiedzi ARP mogą zostać użyte do zatrzymania całego ruchu w sieci lokalnej w ramach ataku ARP DoS, jak pokazano na rysunku.



Atakujący wysyła do wszystkich hostów wewnętrznych ciągły strumień niezamówionych sfałszowanych odpowiedzi ARP, mówiących, że brama (10.0.0.4) znajduje się pod adresem E5-E5-E5-E5-E5-E5 (Krok 1). Hosty rejestrują adres IP bramy i nieistniejący adres MAC (Krok 2). Hosty wewnętrzne będą wysyłać cały ruch przeznaczony dla bramy do E5-E5-E5-E5-E5-E5. Problem w tym, że E5-E5-E5-E5-E5-E5 nie istnieje. Przełącznik odbiera pakiety z hostów wewnętrznych zaadresowanych do E5-E5-E5-E5-E5-E5, ale nie może ich dostarczyć, ponieważ host nie istnieje. Pakiety adresowane do E5-E5-E5-E5-E5-E5 są odrzucane (Krok 3). Ponownie przełącznik nie sprawdza adresu IP w pakiecie. Sprawdza tylko docelowy adres MAC. Nie może przesłać dalej pakietu, mimo że jest fizycznie połączony bezpośrednio z bramą.

Zapobieganie zatruciu ARP

STATYCZNE TABELE

Zatruciu ARP można zapobiec, używając statycznych tabel IP i statycznych tabel ARP. Statyczne tabele ARP są ustawiane ręcznie i nie mogą być dynamicznie aktualizowane za pomocą ARP. Każdy komputer ma znany statyczny adres IP, który się nie zmienia. Wszystkie hosty w sieci LAN wiedzą, który adres IP jest przypisany do każdego adresu MAC (hosta). Trudność w korzystaniu ze statycznych tabel IP i ARP polega na tym, że organizacje się zmieniają. Możliwe byłoby zarządzanie małą siecią z niewielkimi zmianami. Wyeliminowałoby to możliwość zatrucia ARP. Jednak większość organizacji jest zbyt duża, zmienia się zbyt szybko i nie ma doświadczenia w efektywnym zarządzaniu statycznymi tabelami adresów IP i ARP. Obciążenie pracą byłoby przytłaczające.

OGRANICZ DOSTĘP LOKALNY

Innym sposobem zapobiegania zatruciu ARP jest ograniczenie dostępu do sieci lokalnej. Hosty obce nie mogą być dopuszczone do sieci LAN. Większość dużych korporacji całkiem nieźle radzi sobie z powstrzymywaniem złych ludzi. W rzeczywistości reszta tego rozdziału skupi się na kontrolowaniu dostępu do sieci.

TEST XCIV

a. W jaki sposób zatrucie ARP można wykorzystać jako atak DoS?

b. W jaki sposób można wykorzystać statyczne tabele adresów IP i ARP, aby zapobiec zatruciu ARP?

c. Czy statyczne tablice IP i ARP mogą być efektywnie wykorzystywane w dużych sieciach? Dlaczego nie?

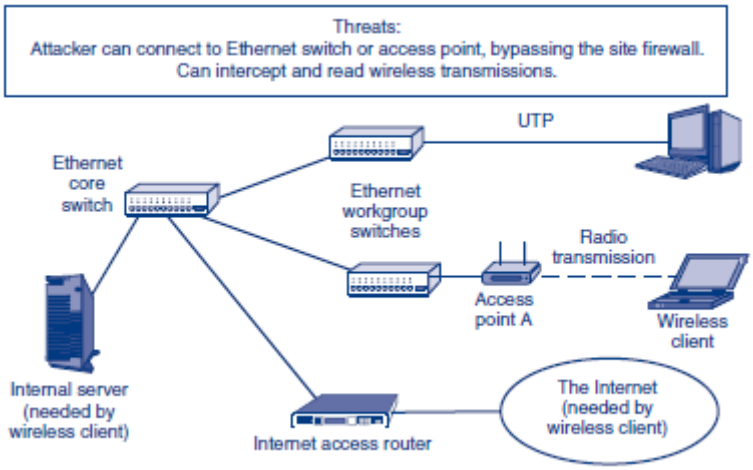
d. Dlaczego ograniczenie dostępu lokalnego miałoby zapobiegać atakom DoS?

KONTROLA DOSTĘPU DO SIECI

W Części 3 można było zobaczyć, że pojawiły się wirtualne sieci prywatne (VPN), które mają chronić poufną komunikację w sieciach rozległych przez Internet. SSL/TLS został stworzony w celu ochrony e-commerce w Internecie. Z kolei IPsec to ogólny protokół VPN dla sieci IP, z których najbardziej widoczny jest Internet. Sieci LAN w lokalizacjach korporacyjnych wymagają również dodatkowej ochrony, aby zapewnić poufność danych przesyłanych przez sieci wewnętrzne. Korporacyjne sieci LAN muszą również zapewniać kontrolę dostępu, która zezwala na dostęp do sieci tylko uwierzytelnionemu i autoryzowanemu personelowi. Pozostała część tego rozdziału skupi się na zabezpieczaniu sieci przewodowych (Ethernet) i bezprzewodowych.

Połączenia LAN

Rysunek ilustruje uproszczoną sieć LAN w siedzibie firmy.



Komputery łączą się z siecią LAN za pomocą przełączników Ethernet. Niektóre robią to za pomocą 4-parowych przewodów UTP podłączonych do gniazdek ściennych. Chociaż możliwe są całkowicie bezprzewodowe sieci LAN, większość komunikacji bezprzewodowej w sieciach LAN służy do łączenia klientów bezprzewodowych z przewodową siecią Ethernet firmy. Klient bezprzewodowy komunikuje się drogą radiową z bezprzewodowym punktem dostępowym, który z kolei łączy się poprzez 4-parową skrętkę UTP z przełącznikiem Ethernet. Dlaczego klient musi łączyć się z przewodową siecią LAN? Po prostu serwery, których potrzebuje klient bezprzewodowy, znajdują się w przewodowej sieci LAN, podobnie jak router dostępu do Internetu, którego potrzebuje klient bezprzewodowy, aby uzyskać dostęp do Internetu.

Zagrożenia kontroli dostępu

Tradycyjnie sieci Ethernet LAN nie oferowały zabezpieczenia kontroli dostępu. Każdy intruz, który wszedł do budynku korporacji, mógł podejść do dowolnego gniazdka w ścianie i podłączyć notebooka. Intruz miałby wówczas nieograniczony dostęp do komputerów w sieci LAN, omijając zaporę graniczną witryny. To był kompletny załamek w kontroli dostępu.

Bezprzewodowe sieci LAN mają jeszcze większe zagrożenia dostępu. Podobnie jak w przypadku sieci Ethernet LAN, intruz może połączyć się drogą radiową z niechronionym bezprzewodowym punktem dostępowym. To ponownie wprowadza atakującego do sieci, omijając zaporę graniczną. Intruz bezprzewodowy nie musi nawet wchodzić do budynku. Haker drive-by może siedzieć w samochodzie poza murami korporacji. W przypadku anteny o wysokim zysku intruz może znajdować się na tyle daleko, że jest niewidoczny z budynku.

Podsłuchiwanie zagrożeń

Zarówno w przypadku przewodowych, jak i bezprzewodowych sieci LAN, gdy intruzi uzyskają dostęp, mogą użyć sniffera pakietów do przechwytywania i odczytywania legalnego ruchu. W sieciach Ethernet LAN szyfrowanie jest rzadkie, ale trudno jest uzyskać fizyczny dostęp do przewodów Ethernet lub gniazd ściennych. Jednak w bezprzewodowych sieciach LAN transmisja radiowa sprawia, że podsłuchiwanie staje się trywialne, chyba że ruch jest silnie zaszyfrowany. Niestety, jak zobaczymy w tym rozdziale, ruch bezprzewodowy jest często szyfrowany w sposób, który jest dziecinnie łatwy do złamania za pomocą oprogramowania hakerskiego, które można łatwo pobrać z Internetu. W niektórych przypadkach w ogóle nie ma szyfrowania.

TEST XCV

a. Jakie jest główne zagrożenie kontroli dostępu w sieciach Ethernet LAN?

b. Jakie jest główne zagrożenie kontroli dostępu w bezprzewodowych sieciach LAN?

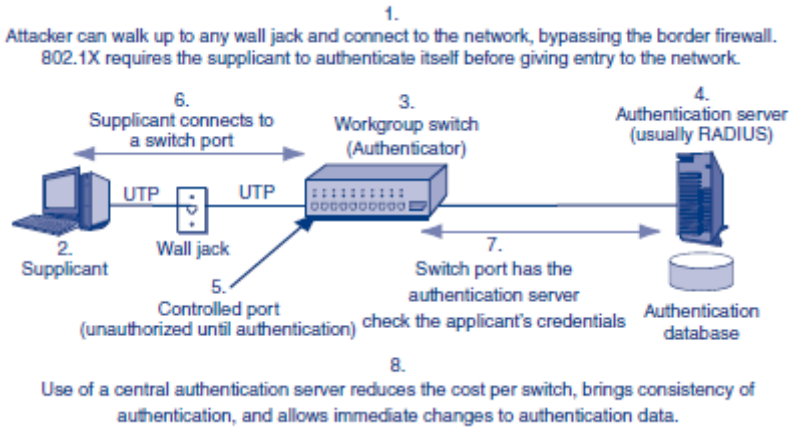
c. Dlaczego zagrożenie związane z kontrolą dostępu w bezprzewodowych sieciach LAN jest poważniejsze?

d. Czy podsłuchiwanie jest zwykle problemem w przypadku przewodowych i bezprzewodowych sieci LAN, czy też obu?

BEZPIECZEŃSTWO ETHERNETU

Ethernet i 802.1X

Zaczniemy przyglądać się specyfice bezpieczeństwa sieci LAN za pomocą Ethernetu i 802.1X. Standard 802.1X zapewnia kontrolę dostępu, aby uniemożliwić nielegalnym klientom łączenie się z siecią. Zaczniemy od Ethernetu, ponieważ 802.1X jest stosunkowo łatwe do wdrożenia w przewodowych sieciach LAN. Rysunek ilustruje główne elementy bezpieczeństwa Ethernet i 802.1X. 802.1X sprawia, że przełącznik grupy roboczej Ethernet9 (3) staje się bramą do sieci.



Komputer użytkownika łączy się przez UTP z gniazdkiem ściennym lub bezpośrednio z przełącznikiem. Mówiąc dokładniej, komputer łączy się z określonym portem na przełączniku grupy roboczej. Ten port jest prawdziwym punktem kontroli dostępu. Nic dziwnego, że nazwa standardu 802.1X to kontrola dostępu oparta na portach. Standard 802.1X zapewnia kontrolę dostępu, aby uniemożliwić nielegalnym klientom łączenie się z siecią. Przełącznik grupy roboczej to przełącznik, z którym łączy się klient. Natomiast przełączniki rdzeniowe łączą przełączniki z innymi przełącznikami. Przełączniki do grup roboczych zapewniają dostęp do sieci, więc umieszczenie kontroli dostępu w przełącznikach do grup roboczych jest oczywistym wyborem. Kiedy komputer łączy się po raz pierwszy, port jest w nieautoryzowanym stanie (5). Nie pozwoli użytkownikowi komunikować się przez sieć. Port pozostaje nieautoryzowany, dopóki komputer się nie uwierzytelni. Po uwierzytelnieniu port przechodzi w stan autoryzowany, a komputer ma swobodny dostęp do sieci. Chociaż port przełącznika jest głównym punktem kontroli, przełącznik nie jest obciążony koniecznością wykonywania ciężkich prac związanych z uwierzytelnianiem. W tym celu przełączniki opierają się na centralnym serwerze uwierzytelniania (4). Ten serwer posiada dane uwierzytelniające do sprawdzania poświadczeń oraz moc obliczeniową potrzebną do sprawdzania haseł, skanów biometrycznych i innych poświadczeń dostępu. Korzystanie z centralnego serwera uwierzytelniania zamiast konieczności wykonywania całej pracy przez każdy przełącznik grupy roboczej ma trzy zalety:

OSZCZĘDNOŚĆ KOSZTÓW

Po pierwsze, jak już wspomniano, zmniejsza to koszt każdego przełączenia grupy roboczej. Jeśli firma ma wiele przełączników grup roboczych rozmieszczonych w całym budynku, bardzo ważne jest, aby nie trzeba było intensywnie przetwarzać uwierzytelniania i utrzymywać bazy danych uwierzytelniania na każdym przełączniku.

SPÓJNOŚĆ

Po drugie, użycie centralnego serwera uwierzytelniania zapewnia spójność uwierzytelniania. Sprawdzanie poświadczeń odbywa się zawsze w ten sam sposób, bez względu na to, z jakim przełącznikiem grupy roboczej łączy się atakujący. Atakujący nie może wypróbować różnych przełączników grup roboczych, dopóki nie znajdzie przełącznika z nieprawidłową bazą danych uwierzytelniania, która umożliwia atakującemu wejście.

NATYCHMIASTOWE ZMIANY

Po trzecie, centralne serwery uwierzytelniania wprowadzają natychmiastowe zmiany w kontroli dostępu. Na przykład, jeśli zwolnisz pracownika, możesz natychmiast zawiesić jego dostęp do sieci na centralnym serwerze uwierzytelniania, zamiast rekonfigurować sprawdzanie poświadczeń na wszystkich przełącznikach grupy roboczej. W 802.1X są trzy urządzenia zaangażowane w uwierzytelnianie. Komputer poszukujący dostępu jest oczywiście petentem (2), ale jakim urządzeniem jest weryfikator? Czy jest to przełącznik grupy roboczej czy centralny serwer uwierzytelniania? Oczywiście funkcja weryfikacji jest rozłożona na dwa urządzenia. Zamiast wywoływać którekolwiek z urządzeń weryfikatorem, 802.1X wywołuje przełącznik grupy roboczej jako wystawca uwierzytelnienia (3). Uwierzytelnianie centralne

Serwer nazywany jest po prostu centralnym serwerem uwierzytelniającym (4).

TEST XCVI

a. Dlaczego 802.1X nazywa się kontrolą dostępu opartą na portach?

b. Gdzie jest wykonywana ciężka praca związana z uwierzytelnianiem?

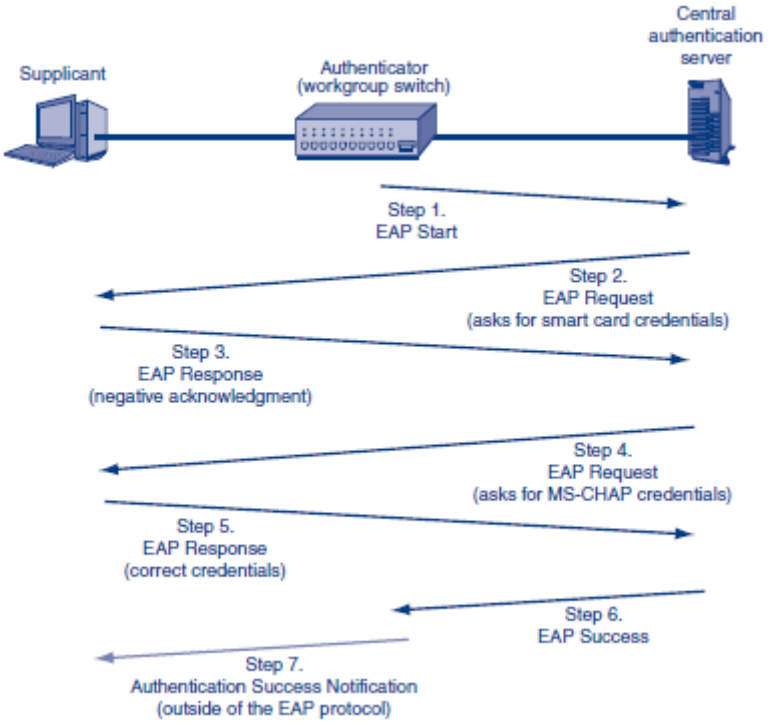
c. Jakie są trzy zalety korzystania z centralnego serwera uwierzytelniania?

d. Które urządzenie jest weryfikatorem? Wyjaśniać. (Podchwytliwe pytanie.)

e. Które urządzenie nazywa się wystawcą uwierzytelnienia?

Rozszerzalny protokół uwierzytelniania (EAP)

Rysunek pokazuje, że 802.1X opiera się na innym protokole, Extensible Authentication Protocol (EAP), do zarządzania specyfiką interakcji uwierzytelniania. Rysunek przedstawia proste okno dialogowe uwierzytelniania przy użyciu protokołu EAP.



OBSŁUGA EAP

Przełączniki Ethernet mogą wykrywać, kiedy host łączy się z jednym ze swoich portów. Gdy przełącznik wykryje połączenie, wysyła komunikat EAP Start do serwera RADIUS (Krok 1). To rozpoczyna sesję EAP. Centralny serwer uwierzytelniania wysyła do klienta komunikat żądania EAP. Ten komunikat zawiera pole wskazujące, że ten komunikat żądania EAP wymaga poświadczeń karty inteligentnej (Krok 2). Suplikant nie może używać uwierzytelniania kartą inteligentną, więc odsyła komunikat odpowiedzi EAP, który zawiera potwierdzenie negatywne (Krok 3). Te wiadomości przechodzą między serwerem uwierzytelniającym a suplikantem. Przełącznik uwierzytelniający jedynie przekazuje wiadomość. Nazywa się to operacją tranzytową. Po niepowodzeniu pierwszego żądania EAP, centralny serwer uwierzytelniania wysyła kolejną wiadomość żądania EAP, tym razem z kodem wskazującym, że życzy sobie poświadczeń MS-CHAP (Krok 4). Ten komunikat żądania zawiera komunikat wezwania, którego używa MS-CHAP, jak widzieliśmy w rozdziale 3. Tym razem suplikant spełnia żądanie. Wysyła z powrotem wiadomość odpowiedzi EAP zawierającą ciąg odpowiedzi MS-CHAP (Krok 5). Ponownie, przełącznik uwierzytelnienia jedynie przekazuje wiadomość. Centralny serwer uwierzytelniania ocenia ciąg i odsyła komunikat EAP Success, jeśli suplikant jest uwierzytelniony lub komunikat EAP Failure, jeśli suplikant nie jest uwierzytelniony (Krok 6). Ta wiadomość trafia do osoby uwierzytelniającej, a nie bezpośrednio do suplikanta. Sposób, w jaki uwierzytelniający powiadamia klienta (Krok 7) jest poza zakresem EAP.

ROZCIĄGLIWOŚĆ

EAP nazywa się rozszerzalnym, ponieważ łatwo jest dodać do EAP nowe metody uwierzytelniania. Struktura wiadomości EAP w ogóle się nie zmienia po dodaniu nowej metody uwierzytelniania. Nowy kod opcji jest po prostu dodawany do listy metod. Po zdefiniowaniu nowego kodu uwierzytelniającego wnioskodawca i weryfikator muszą wdrożyć nową metodę, zanim będą mogli z niej skorzystać. Jednak działanie uwierzytelniania nie ulega zmianie. Uwierzytelniający jedynie przechodzi przez komunikaty EAP Request i EAP Response zajmujące się nowym trybem uwierzytelniania. Operacja tranzytowa oznacza, że gdy wiele przełączników grup roboczych w firmie zaimplementuje EAP, nie ma potrzeby

ich uaktualniania za każdym razem, gdy pojawiają się nowe metody uwierzytelniania, a inne stają się przestarzałe. Firma ma wiele przełączników grup roboczych, więc te oszczędności kosztów dla uwierzytelniaczy są bardzo ważne.

TEST XCVII

a. Jak rozpoczyna się sesja EAP?

b. Jakie typy wiadomości zawierają żądania informacji uwierzytelniających i odpowiedzi na te żądania?

c. Opisz, w jaki sposób centralny serwer uwierzytelniania informuje osobę uwierzytelniającą, że suplikant jest akceptowalny.

d. W jaki sposób osoba uwierzytelniająca przekazuje te informacje petentowi?

e. W jakim sensie EAP jest rozszerzalny?

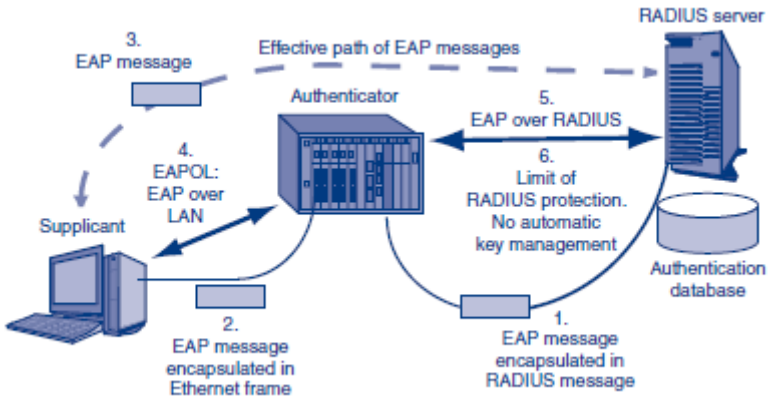
f. Po dodaniu nowej metody uwierzytelniania, jakie oprogramowanie urządzenia należy zmienić, aby korzystać z nowej metody?

g. Dlaczego nie ma potrzeby zmiany działania modułu uwierzytelniającego po dodaniu nowej metody uwierzytelniania EAP lub porzuceniu starego trybu uwierzytelniania EAP?

h. Dlaczego ta wolność od konieczności zmiany zmiany jest korzystna?

Serwery RADIUS

Większość centralnych serwerów uwierzytelniania jest zarządzana przez standard RADIUS. RADIUS to protokół klient/serwer, w którym stroną uwierzytelniającą jest klient, a centralnym uwierzytelnianiem jest serwer. Rysunek ilustruje zależność między EAP i RADIUS.



PROMIEŃ I EAP

Protokół RADIUS zapewnia uwierzytelnianie, ale wykracza poza to. Zapewnia również autoryzację, co oznacza, że może określać ograniczenia w takich kwestiach, jak z jakimi serwerami może się łączyć uwierzytelniony suplikant, do jakich katalogów suplikant może uzyskać dostęp na tych serwerach oraz co użytkownicy mogą w tych katalogach robić (odczytywać pliki, modyfikować pliki itp. .). RADIUS zapewnia również opcjonalny audyt połączeń, dzięki czemu firma może później sprawdzić, do jakiej grupy roboczej podłączony jest konkretny komputer i jak długo był on podłączony. Chociaż RADIUS ma swoje własne metody komunikacji uwierzytelniania, Rysunek pokazuje, że EAP over RADIUS określa, jak używać EAP zamiast natywnego uwierzytelniania RADIUS, gdy RADIUS zarządza komunikacją

między uwierzytelniającym a centralnym serwerem uwierzytelniania. Innymi słowy, EAP jest używany tylko w pierwszym A (uwierzytelnianie) w AAA (uwierzytelnianie, autoryzacja i audyt, omówiony dokładniej w rozdziale 5).

TEST XCVIII

a. Jaki standard stosuje większość centralnych serwerów uwierzytelniania?

b. W jaki sposób EAP i RADIUS są powiązane pod względem funkcjonalności?

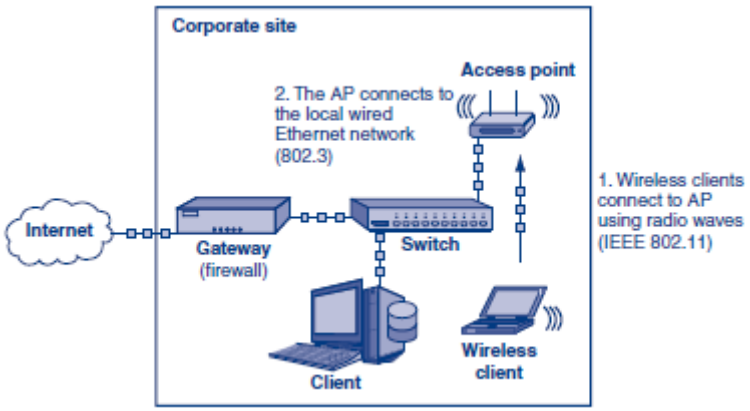
c. Jakiej metody uwierzytelniania używa RADIUS?

BEZPIECZEŃSTWO BEZPRZEWODOWE

Jak wspomniano na początku, sieci Ethernet LAN nie są jedynym rodzajem sieci, które wymagają bezpieczeństwa. W rzeczywistości bezprzewodowe sieci LAN (WLAN) mają do rozważenia więcej kwestii związanych z bezpieczeństwem niż przewodowe sieci LAN. Na przykład sieci bezprzewodowe mogą zostać zaatakowane przez hakerów drive-by, którzy nie muszą nawet wchodzić do budynku, aby uzyskać dostęp do sieci LAN. Mogą siedzieć po drugiej stronie ulicy lub w sąsiednim budynku i mieć łatwy dostęp do sieci wewnętrznej bez wzbudzania podejrzeń. Sieci bezprzewodowe stały się niemal wszechobecne, ponieważ są szybsze, łatwiejsze i tańsze w konfiguracji niż tradycyjne sieci przewodowe. Oferują również większą mobilność, produktywność i funkcjonalność. Korzyści płynące z sieci bezprzewodowych zachęciły do powszechnego przyjęcia w korporacjach. Niestety możliwość zabezpieczania sieci bezprzewodowych nie nadąża za jej szybkim rozwojem. Administratorzy sieci zauważyli nowe typy ataków na ich sieci bezprzewodowe. Musieli także wdrożyć nowe metody uwierzytelniania bezprzewodowego, standardy bezpieczeństwa i zasady bezpieczeństwa.

Ataki bezprzewodowe

Jak pokazano na rysunku,

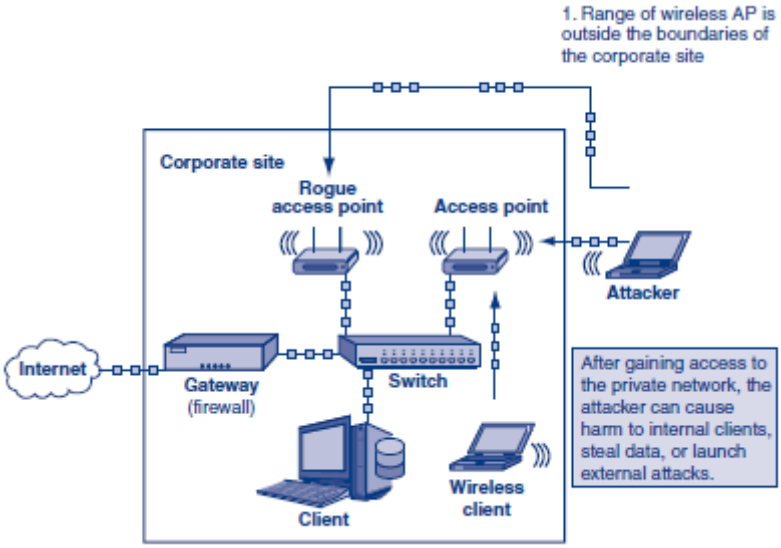


użytkownicy łączą się za pomocą fal radiowych z bezprzewodowym punktem dostępowym (AP) przy użyciu standardów 802.11, opracowanych przez grupę roboczą IEEE 802.11 (1). Punkt dostępowy łączy się następnie z lokalną siecią Ethernet (802.3) za pomocą połączenia przewodowego (2). Punkt dostępowy działa jako punkt przekaźnikowy między sieciami bezprzewodowymi i przewodowymi. Ataki bezprzewodowe koncentrują się na punkcie dostępowym. Sieci bezprzewodowe 802.11 zwykle mają zasięg od 30 do 100 metrów rozciągający się we wszystkich kierunkach od punktu dostępowego. Dzięki temu atakujący może zaatakować punkt dostępowy i sieć wewnętrzną, pozostając poza fizycznymi granicami witryny korporacyjnej. Trzy rodzaje ataków na sieć bezprzewodową, którym

przyjrzymy się, to (1) nieautoryzowany dostęp do sieci, (2) atak typu „man-in-the-middle” przy użyciu złego bliźniaka oraz (3) ataki typu „odmowa usługi” w sieci bezprzewodowej.

Nieautoryzowany dostęp do sieci

Najczęstszym atakiem na sieci bezprzewodowe jest nieautoryzowany dostęp lub łączenie się z siecią bez pozwolenia. Nieautoryzowany dostęp może wystąpić w sieciach, które mogą lub nie, mieć włączone protokoły bezpieczeństwa. To, że sieć WLAN nie jest „zablokowana”, nie oznacza, że można jej używać. Podobnie jak w domu, pozostawienie otwartych drzwi nie daje sąsiadom prawa wejścia do domu. Przed uzyskaniem dostępu do sieci należy uzyskać pozwolenie. Otwarte sieci mogą być legalnie dostępne dla każdego i często są publikowane jako takie. Można je znaleźć w miejscach publicznych, takich jak kawiarnie, kawiarnie, uniwersytety i inne przestrzenie publiczne. O ile nie zostaną opublikowane, lepiej założyć, że wszystkie inne sieci są sieciami prywatnymi, które nie zezwalają na dostęp bez wyraźnej autoryzacji. Najbardziej oczywistą formą nieautoryzowanego dostępu jest „złamanie” protokołów bezpieczeństwa bezprzewodowego w zabezpieczonej sieci. Protokoły bezpieczeństwa bezprzewodowego, omówione później, są włączane i konfigurowane w punktach dostępu bezprzewodowego. Prawidłowo skonfigurowane punkty dostępowe uwierzytelniają użytkowników, szyfrują ruch bezprzewodowy i mogą wykrywać włamania. Poważnym zagrożeniem dla sieci bezprzewodowych jest wprowadzenie nielegalnego punktu dostępowego, jak pokazano na rysunku.



Nieautoryzowane punkty dostępu to nieautoryzowane punkty dostępu skonfigurowane przez osoby lub działy z niewielkimi zabezpieczeniami lub bez nich. Nieuczciwe punkty dostępowe dają hakerowi driveby czysty dostęp do sieci, omijając starannie opracowane przez firmę zabezpieczenia sieci bezprzewodowych w legalnych punktach dostępowych.

Nielegalne punkty dostępu to nieautoryzowane punkty dostępu utworzone przez osoby lub działy.

ZAPOBIEGANIE NIEUPRAWNIONEMU DOSTĘPU

Dwa powody uniemożliwiające nieautoryzowanym użytkownikom dostęp do lokalnej sieci bezprzewodowej to (1) zapobieganie uszkodzeniom zasobów wewnętrznych oraz (2) zapobieganie szkodom zewnętrznym, które wydają się pochodzić z sieci.

Szkoda wewnętrzna. Po pierwsze, przyznanie nieautoryzowanym użytkownikom (potencjalnym napastnikom) dostępu do lokalnej sieci WLAN oznacza, że znajdują się oni w sieci lokalnej. Skutecznie

ominęły główną zaporę sieciową i wszystkie środki bezpieczeństwa, przez które musi przejść normalny ruch sieciowy. Zwiększa to prawdopodobieństwo udanego ataku. Atakujący mają większy dostęp do wewnętrznych informacji, zasobów i innych ruchów w sieci. Mogą potajemnie kraść poufne informacje, odczytywać i rejestrować ruch sieciowy, zmieniać urządzenia sieciowe lub umieszczać złośliwe oprogramowanie na docelowych klientach lub serwerach. Mogą również mieć dostęp do udziałów sieciowych, które, jak zakładano, są chronione przez zaporę. Sniffer Apacket może być używany do zbierania informacji o sieci lub danych użytkownika. Obejmuje to nazwy użytkowników w postaci zwykłego tekstu, hasła, adresy e-mail i tak dalej. Chipset bezprzewodowy na kliencie atakującego musi obsługiwać monitorowanie częstotliwości radiowych (RFMON) w celu odbierania pakietów bezprzewodowych adresowanych do innych hostów. Atakujący może odbierać pakiety w trybie rozwiązłym, co pozwala mu na odbieranie wiadomości adresowanych do innych użytkowników. Atakujący mogą nawet skupić się na sieciach bezprzewodowych celów o dużej wartości, takich jak dyrektorzy generalni, konkurenci branżowi, centra badawczo-rozwojowe, instytucje rządowe lub celebryci. Skupienie ataków elektronicznych na określonych celach o dużej wartości jest znane jako wielorybnictwo. Chociaż korporacyjna sieć bezprzewodowa prezesa może być bezpieczna, jej sieć bezprzewodowa w jej prywatnej rezydencji może nie być.

Szkoda zewnętrzna. Po drugie, ponieważ atakujący ma dostęp do Internetu z Twojej sieci wewnętrznej, wygląda na to, że jego ruch pochodzi z Twojej firmy. Atakujący wydaje się być autoryzowanym klientem. Wygląda na to, że wyrządzone ataki i szkody zostały wyrządzone przez Twoją organizację. Osoba atakująca może anonimowo pobierać, przesyłać i przechowywać nielegalne treści za pośrednictwem sieci bezprzewodowej. Co gorsza, sieć mogłaby być wykorzystana jako platforma startowa dla zewnętrznego ataku. Ponieważ źródłowy adres IP wydaje się pochodzić z sieci wewnętrznej, każdy atak można przypisać firmie. Załóżmy na przykład, że nieautoryzowany napastnik przeprowadza atak DoS na znanego dostawcę poczty online z niezabezpieczonej wewnętrznej sieci bezprzewodowej. Dostawca poczty mógłby zablokować cały zakres IP należący do korporacji. Użytkownicy wewnętrzni mogą tymczasowo (lub na stałe) utracić dostęp do swoich kont e-mail. Zasadniczo nieautoryzowany dostęp do sieci ułatwił atak z zewnątrz, a następnie wyrządził szkody w zasobach firmy.

W wiadomościach

Mężczyzna z Buffalo NY został aresztowany przez agentów federalnych za rzekome pobranie znacznej ilości pornografii dziecięcej. Agenci federalni monitorowali podejrzanego o pseudonimie „Doldrum" zalogowanego do sieci peer-to-peer. Zarejestrowali adres IP podejrzanego i uzyskali informacje o koncie podejrzanego od jego dostawcy usług internetowych. Agenci federalni wdarli się do domu o 6:20 i aresztowali podejrzanego. Skonfiskowali komputery, iPhone'a i iPada. Po trzydniowym śledztwie agenci federalni ustalili, że mężczyzna był niewinny. Okazało się, że mężczyzna nie zabezpieczył swojej sieci bezprzewodowej. Sąsiad skorzystał z bezprzewodowej sieci mężczyzny bez jego wiedzy. Rzeczywisty „Doldrum" uzyskał również dostęp do sieci peer-to-peer z kampusu SUNY-Buffalo. Tydzień później 25-letni sąsiad mężczyzny, student SUNY-Buffalo, został aresztowany i oskarżony o rozpowszechnianie pornografii dziecięcej.

TEST XCIX

a. Jaki jest najczęstszy atak na sieci bezprzewodowe? Czemu?

b. Który standard IEEE reguluje transmisję WLAN?

c. Które urządzenie działa jako przekaźnik między sieciami przewodowymi i bezprzewodowymi?

d. Jaki jest typowy zasięg sieci WLAN?

e. Jaka jest różnica między siecią otwartą a siecią prywatną?

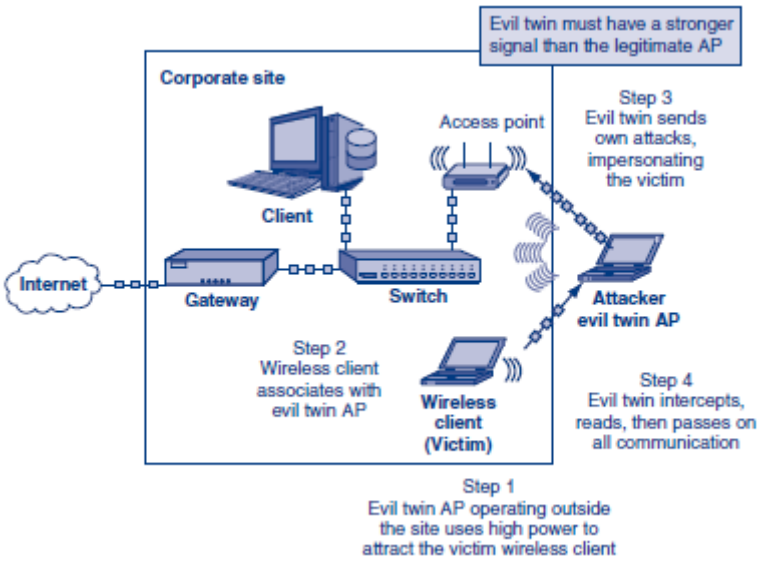
f. Kto założyłby nieuczciwy punkt dostępowy? Czemu?

g. Podaj przykłady szkód wewnętrznych i zewnętrznych spowodowanych przez nieautoryzowany dostęp bezprzewodowy.

h. Czy ponosisz odpowiedzialność, jeśli ktoś inny użyje Twojej sieci bezprzewodowej do popełnienia przestępstwa? Dlaczego lub dlaczego nie?

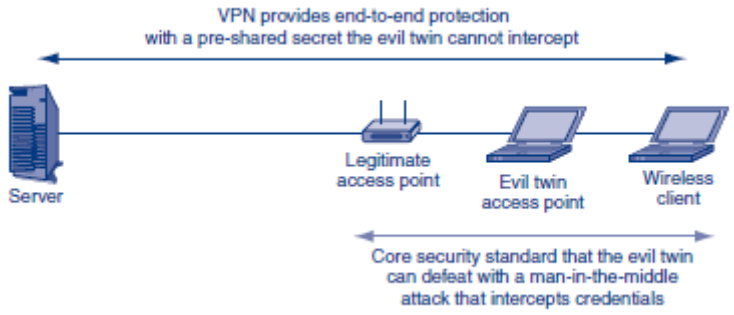
Złe podwójne punkty dostępowe

Chociaż sieci bezprzewodowe oferują silne zabezpieczenia, są podatne na ataki typu man-inthe-middle, które przechwytują wiadomości w trakcie i po konfiguracji zabezpieczeń. W bezprzewodowych sieciach LAN ataki typu man-in-the-middle wykorzystują złe bliźniacze punkty dostępowe do zmiany funkcjonalności sieci. Zły bliźniak punkt dostępowy to po prostu komputer z oprogramowaniem, które pozwala mu udawać punkt dostępowy. Jak pokazuje rysunek, osoba atakująca tworzy zły bliźniaczy punkt dostępu poza siedzibą firmy.



Atakujący ustawia wysoką moc transmisji, ponieważ klienci często łączą się z punktem dostępu, który ma najsilniejszy sygnał (Krok 1). Jeśli klient bezprzewodowy ofiary jest takim klientem, skojarzy się on ze złym bliźniaczym punktem dostępowym zamiast z jego legalnym punktem dostępowym (Krok 2). Zły bliźniak połączy się następnie z legalnym punktem dostępu w obrębie korporacyjnych ścian, udając użytkownika (Krok 3). To skutecznie stawia między klientem bezprzewodowym a uprawnionym punktem dostępu. Jest gotowy do wykonania ataku MITM. Zły bliźniaczy punkt dostępu przechwytuje cały ruch przechodzący przez niego, a następnie przekazuje ruch do miejsca docelowego (Krok 4). Początkowo przechwytuje transmisje danych uwierzytelniających i klucze. Następnie, gdy nadejdzie zaszyfrowana wiadomość, może ją odszyfrować, przeczytać, ponownie zaszyfrować i przekazać dalej. Zły bliźniak może również wysyłać własne pakiety ataków, podszywając się pod klienta ofiary. Ataki złych bliźniaczych punktów dostępowych są dość powszechne, szczególnie w publicznych hot spotach. Zabezpieczenia oferowane przez WPA i 802.11i są bez znaczenia, gdy atak MITM jest prawidłowo wykonywany przez złego bliźniaka. Aby zaradzić temu zagrożeniu, niektóre firmy wymagają, aby klienci

przychodzący za pośrednictwem zdalnego dostępu również nawiązywali połączenie VPN. Ilustruje to rysunek.



VPN używa wstępnie udostępnionego klucza tajnego, który klient i serwer wymieniają wcześniej. Dlatego ten sekret nie może być przechwycony przez złego bliźniaka.

TEST C

a. Jaki atak typu man-in-the-middle stanowi zagrożenie dla sieci WLAN 802.11?

b. Fizycznie, czym jest zły bliźniak punkt dostępowy?

c. Co się dzieje, gdy legalny suplikant wysyła dane uwierzytelniające do uprawnionego dostępu?

punkt?

d. W jakie dwa rodzaje ataków może zaangażować się zły bliźniak?

e. Czy ataki złych bliźniaków są częste?

f. Gdzie są najczęściej spotykane?

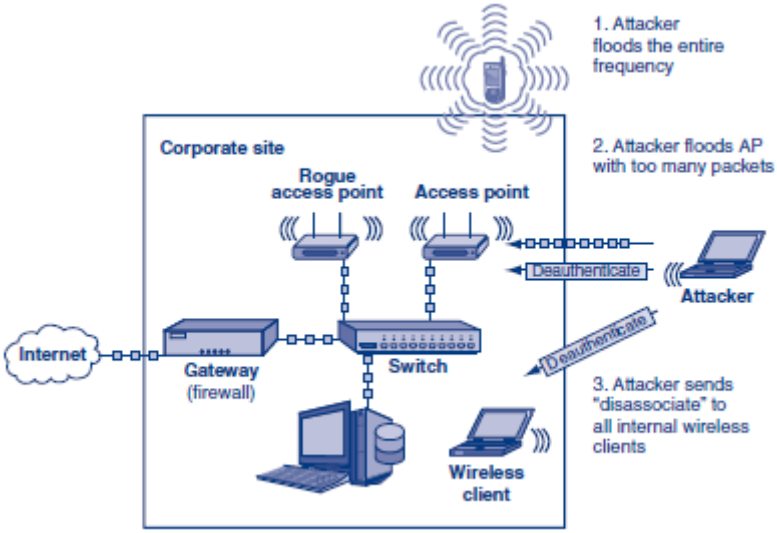
g. Jak można zaradzić niebezpieczeństwu ataków złych bliźniaków?

Bezprzewodowa odmowa usługi

Ostatnim rodzajem ataku WLAN, któremu się przyjrzymy, jest bezprzewodowy atak DoS. Podobnie jak w przypadku ataków DoS omówionych w poprzedniej sekcji, bezprzewodowe ataki DoS mają na celu wpłynięcie na dostępność sieci. Istnieje kilka sposobów, aby uniemożliwić hostom dostęp do sieci bezprzewodowej. Przyjrzymy się trzem.

ZALEW CZĘSTOTLIWOŚCI

Prymitywnym sposobem na uniemożliwienie dostępu do sieci bezprzewodowej jest zalanie całej częstotliwości transmisji. Sieci bezprzewodowe 802.11 transmitują w pasmach częstotliwości 2,4 GHz i/lub 5 GHz. Atakujący mogą modyfikować urządzenia bezprzewodowe, aby zalać te pasma częstotliwości zakłóceniami elektromagnetycznymi (EMI), znanymi również jako zakłócenia częstotliwości radiowych (RFI). Zakłócenia lub szumy uszkadzają sygnał 802.11 i sprawiają, że pakiety są nieczytelne. Rysunek 4-25 pokazuje, że atakujący mogą używać popularnych urządzeń gospodarstwa domowego, takich jak elektroniczne nianie, telefony bezprzewodowe i urządzenia Bluetooth, aby zakłócać działanie sieci 802.11.



Istnieją komercyjne urządzenia do bezprzewodowego zagłuszania, które mogą zalewać nie tylko częstotliwości 802.11, ale także częstotliwości telefonów komórkowych. Administratorzy sieci mogą używać analizatorów widma bezprzewodowego do identyfikowania powodzi DoS. Analizatory widma rejestrują wszystkie sygnały, w tym transmisje pakietowe, w danym paśmie częstotliwości radiowych. Administrator sieci może zauważyć rozległe uszkodzenia pakietów bezprzewodowych. Może to wskazywać na powódź DoS. Administrator może następnie użyć analizatora widma, aby sprawdzić, czy całe pasmo częstotliwości, w tym kanały bezprzewodowe, jest zalewane fałszywymi sygnałami. To wskazywałoby na atak DoS zalewający częstotliwość.

ZALEJ PUNKT DOSTĘPOWY

Atakujący mogą przeciążyć punkt dostępu zbyt dużym ruchem. Wszystkie hosty w sieci WLAN mają dostęp do punktu dostępowego. Jeśli atakujący nieustannie wysyła do punktu dostępowego nadmierną liczbę pakietów, dostęp do wszystkich innych hostów zostanie skutecznie odmówiony. AP wykorzystuje wszystkie jego zasoby wysyłają i odbierają pakiety atakującego. Równie skuteczną metodą zalewania byłoby wielokrotne wysyłanie bardzo dużego pliku.

WYŚLIJ POLECENIA ATAKU

Ostatnia bezprzewodowa metoda DoS, której się przyjrzymy, wykorzystuje protokoły zaimplementowane w standardzie 802.11. Atakujący wysyła polecenia ataku do klientów, punktów dostępu lub obu. Wiele z tych poleceń ataku to w rzeczywistości ramki zarządzania lub kontroli 802.11 używane do zarządzania połączeniem hostów i transmisją sygnałów. Na przykład atakujący może użyć wstrzykiwania pakietów, aby wysłać sfałszowane wiadomości deauthenticate do punktu dostępowego. Sfałszowane adresy źródłowe odpowiadałyby każdemu klientowi bezprzewodowemu w sieci WLAN. Komunikat deauthenticate mówi, że nadawca chce zakończyć uwierzytelnione połączenie. Ofiara musi ponownie uwierzytelnić się za pomocą punktu dostępowego, zanim będzie mógł się komunikować. Ciągły strumień sfałszowanych wiadomości nieuwierzytelniających może uniemożliwić klientom łączenie się z punktem dostępowym. Atakujący może również wysyłać deauthenticate wiadomości do klientów bezprzewodowych. Ten rodzaj ataku jest skuteczny, ponieważ źródło wiadomości nie jest uwierzytelnione. Innymi słowy, źródło wiadomości nie jest weryfikowane. Odpowiednikiem tego ataku w świecie rzeczywistym byłoby anulowanie wszystkich kart kredytowych twojego przyjaciela. Jeśli wystawca karty kredytowej nie zweryfikował dzwoniącego, możesz anulować czyjeś karty kredytowe. Musieliby zapisać się na inną kartę kredytową, zanim mogliby dokonać jakichkolwiek zakupów. Oprócz nieuwierzytelniania wiadomości osoba atakująca może zalewać klientów bezprzewodowych ramkami

typu request-to-send (RTS) lub clear-to-send (CTS). Ramki RTS informują innych klientów bezprzewodowych, że chcesz transmitować przez określony czas (czas trwania transmisji). Ramki CTS informują innych klientów, że otrzymałeś ramkę RTS i że nie powinni transmitować, dopóki nie upłynie wyznaczony czas. Zalew ramek CTS z długimi czasami transmisji sprawia, że inni klienci czekają. Zalew ramek RTS powoduje zalew ramek CTS. Oba wytwarzają skuteczny atak DoS na sieć bezprzewodową. Znowu te wiadomości nie są uwierzytelniane. Rzeczywistym odpowiednikiem powodzi RTS/CTS byłaby rezerwacja każdego miejsca w każdym locie konkurencyjnymi liniami lotniczymi. Żaden pasażer nie mógł latać, ponieważ wszystkie miejsca są zarezerwowane. Bez uwierzytelnienia nabywcy biletów linia lotnicza szybko zbankrutowałaby.

TEST CI

a. Jak zostałby przeprowadzony bezprzewodowy atak DoS?

b. Jakich urządzeń można użyć do zalania częstotliwości transmisji w sieci WLAN?

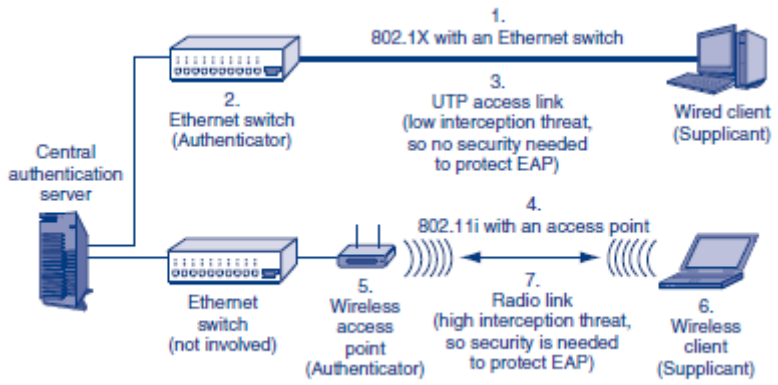
c. Jakiego urządzenia można użyć do zidentyfikowania powodzi DoS, jeśli całość częstotliwości jest zalewana przez EMI?

d. Jakiego rodzaju polecenia ataku można wysłać, aby wywołać bezprzewodowy atak DoS?

e. Co by się stało, gdyby sieć bezprzewodowa została zalana ramkami CTS?

Bezpieczeństwo bezprzewodowej sieci LAN z 802.11i

Z powodów, które zostaną omówione, 802.1X nie można zastosować bezpośrednio do bezprzewodowych sieci LAN 802.11. Musiał zostać rozszerzony, a to rozszerzenie nazwano 802.11i. Rysunek ilustruje zarówno 802.1X w przewodowej sieci LAN, jak i 802.11i dla połączenia 802.11.



W przypadku połączenia 802.11i nadal widzisz znany centralny serwer uwierzytelniania. Widzisz również suplikanta, którym jest komputer bezprzewodowy. Autoryzator zmienił się z portu przełącznika na bezprzewodowy punkt dostępowy (5), ale nie jest to zasadnicza modyfikacja.

POTRZEBA BEZPIECZEŃSTWA EAP

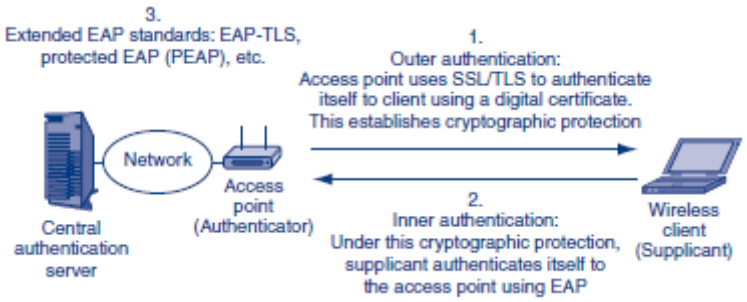
Różnica polega na komunikacji między punktem dostępowym a klientem bezprzewodowym. Extensible Authentication Protocol (EAP) to świetny protokół, ale ma poważne ograniczenie bezpieczeństwa. Zakłada, że połączenie między suplikantem a wystawcą uwierzytelnienia jest bezpieczne. Oczywiście nie ma wyraźnego zabezpieczenia w połączeniu UTP między komputerem a przełącznikiem Ethernet, ale praktyczne ryzyko, że ktoś podepnie linię między gniazdkiem ściennym a przełącznikiem, jest niewielkie, więc potrzeba EAP dla bezpieczeństwa w sieci przewodowej można zignorować (3). Jednak w bezprzewodowych sieciach LAN EAP wymaga dodatkowego zabezpieczenia. Rysunek pokazuje, że

transmisje radiowe mogą być przechwytywane. Ze względu na nieodłączny brak bezpieczeństwa w transmisji bezprzewodowej (7), należy zwiększyć bezpieczeństwo między klientem bezprzewodowym a punktem dostępowym, w przeciwnym razie uwierzytelnianie EAP może zostać łatwo zaatakowane. Aby zapewnić to bezpieczeństwo, 802.11 Working Group udoskonaliła standard 802.1X do pracy w bezprzewodowych sieciach LAN. Ten rozszerzony standard to 802.11i.

EAP zakłada, że połączenie między suplikantem a wystawcą uwierzytelnienia jest bezpieczne. Potrzebne są dodatkowe zabezpieczenia między suplikantem a punktem dostępowym w sieciach WLAN 802.11.

DODAWANIE BEZPIECZEŃSTWA DO EAP

Ulepszenie polega na rozszerzeniu standardów EAP w celu zwiększenia bezpieczeństwa. Wszystkie rozszerzone standardy EAP zaczynają się w ten sam sposób. Jak pokazuje rysunek, wystawca uwierzytelnienia najpierw ustanawia bezpieczne połączenie SSL/TLS między wystawcą uwierzytelnienia a klientem bezprzewodowym.



W tym zewnętrznym uwierzytelnianiu punkt dostępu ma certyfikat cyfrowy, który używa do uwierzytelniania się wobec klienta bezprzewodowego. Po wdrożeniu uwierzytelniania zewnętrznego ustanawiane są zabezpieczenia między klientem bezprzewodowym a punktem dostępu, a EAP może być używany do dalszej części uwierzytelniania. Uwierzytelnianie oparte na certyfikatach cyfrowych jest bardzo silne. Wymaga instalacji certyfikatu cyfrowego w każdym punkcie dostępowym, ale firma ma ograniczoną liczbę punktów dostępowych, więc koszt instalacji certyfikatów cyfrowych nie jest wygórowany. Następnym krokiem jest uwierzytelnianie wewnętrzne, w którym klient bezprzewodowy uwierzytelnia się za pośrednictwem protokołu EAP. W przypadku uwierzytelniania wewnętrznego suplikant klienta używa protokołu EAP w ramach ochrony uwierzytelniania zewnętrznego do komunikowania się z centralnym serwerem uwierzytelniania w ramach wymiany EAP.

EAP-TLS I PEAP

Obecnie na rynku powszechne są dwa rozszerzone standardy EAP. Pierwszy to EAP-TLS. W tym standardzie uwierzytelnianie wewnętrzne również wykorzystuje TLS. Wymaga to od wnioskodawcy posiadania certyfikatu cyfrowego. Jest to bardzo bezpieczne, ale wdrożenie certyfikatu cyfrowego na każdym kliencie i serwerze jest kosztowne. Drugim popularnym rozszerzonym standardem EAP jest chroniony EAP (PEAP). W przypadku uwierzytelniania wewnętrznego przy użyciu protokołu PEAP klient może użyć dowolnej metody określonej w standardzie EAP, od haseł po certyfikaty cyfrowe. PEAP odniósł sukces na rynku, ponieważ jest faworyzowany przez Microsoft i silnie wspierany przez systemy Cisco. Ponadto firmy lubią to, ponieważ mogą zastosować dowolny poziom uwierzytelniania klienta, który jest odpowiedni.

TEST CII

a. Dlaczego nie można rozszerzyć działania 802.1X przy użyciu EAP bezpośrednio na sieci WLAN?

b. Jaki standard stworzyła grupa robocza 802.3, aby rozszerzyć działanie 802.1X na sieci WLAN z zabezpieczeniami dla EAP?

c. W przypadku 802.11i rozróżnij uwierzytelnianie zewnętrzne i wewnętrzne.

d. Jakiej metody lub metod uwierzytelniania używa uwierzytelnianie zewnętrzne?

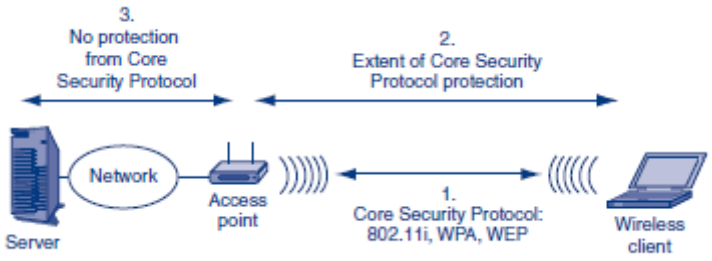
ei. Jakie dwa rozszerzone protokoły EAP są dziś popularne?

f. Rozróżnij ich opcje uwierzytelniania wewnętrznego.

g. Czy zabezpieczenia 802.11i są silne? Wyjaśniać.

Podstawowe protokoły bezpieczeństwa bezprzewodowego

W przypadku bezprzewodowych sieci LAN 802.11, Rysunek pokazuje, że podstawowe protokoły bezpieczeństwa sieci bezprzewodowej chronią komunikację między klientem bezprzewodowym a punktem dostępowym.



Nie zapewniają ochrony przez całą drogę do serwera, do którego klient chce dotrzeć.

Przewodowa ekwiwalentna prywatność (WEP)

Kiedy komitet 802.11 stworzył pierwsze wersje swoich standardów w 1997 roku, stworzył standard WEP (Wired12 Equivalent Privacy), aby zapewnić podstawowe bezpieczeństwo między bezprzewodowymi punktami dostępowymi a klientami bezprzewodowymi. Pod koniec lat 90. stało się oczywiste, że WEP był fatalnie wadliwy. Dzięki oprogramowaniu do łamania WEP, które można łatwo pobrać z Internetu, osoby atakujące mogą złamać zabezpieczenia WEP w ciągu kilku minut. Korzystanie z WEP jest gorsze niż brak zabezpieczeń, ponieważ firmy wdrażające WEP mogą myśleć, że są chronione, gdy tak nie jest. Naruszenie bezpieczeństwa TJX omówione w Rozdziale 1 było możliwe dzięki decyzji TJX o nieaktualizowaniu podstawowego standardu bezpieczeństwa WEP. Firma świadomie zdecydowała się nie uaktualniać do WPA lub 802.11i, ponieważ wierzyła, że ataki prawdopodobnie się nie zdarzą.

Łamanie WEP

WSPÓLNE KLUCZE I BEZPIECZEŃSTWO DZIAŁANIA

Po pierwsze, WEP nakazuje klucze współdzielone, co oznacza, że punkt dostępowy i wszystkie stacje, które go używają, używają tego samego klucza współdzielonego dla wszystkich zabezpieczeń kryptograficznych. Klucz współdzielony zapewnia de facto uwierzytelnianie. Jeśli stacja zna klucz współdzielony, zakłada się, że jest on prawidłowy i dlatego jest przyjmowany do sieci. Pojedynczy klucz współdzielony umożliwia również szyfrowanie wiadomości w celu zachowania poufności. Oczywiście, jeśli atakujący pozna klucz, wszystkie zabezpieczenia zostaną utracone. Sugeruje to, że firmy powinny często zmieniać klucz wspólny. Jednak WEP nie oferował automatycznego ponownego wprowadzania kluczy. W dużych firmach, które mają wiele punktów dostępu współdzielących ten sam klucz WEP,

praktyczne trudności ze zmianą klucza wszystkich oznaczają, że klucze współdzielone prawie nigdy nie są zmieniane. Ponadto, ponieważ „każdy zna" klucz, ludzie swobodnie go udostępniają, nawet jeśli im zabroniono. Co najgorsze, załóżmy, że firma zwalnia niezadowolonego pracownika. Aby być bezpiecznym, firma musi zmienić klucz w każdym punkcie dostępowym, do którego pracownik zna klucz. Będzie to również wymagało od wszystkich klientów użycia zaktualizowanego klucza w każdym punkcie dostępu. Jest to trudne, nawet jeśli klucz jest używany tylko w jednym punkcie dostępowym. Jeśli klucz jest używany w wielu punktach dostępowych lub nawet we wszystkich punktach dostępowych, zmiana klucza będzie zbyt kosztowna i będzie niewygodna dla wielu pracowników.

WYKORZYSTYWANIE SŁABOŚCI WEP

Aby znaleźć klucz WEP, hakerzy mogą użyć zautomatyzowanego oprogramowania do łamania WEP, łatwo dostępnego w Internecie. WEP określa szyfr RC4 do szyfrowania kluczem symetrycznym. Pokrótce widzieliśmy RC4 w rozdziale 3. RC4 jest bardzo wydajny, więc działał nawet z najwcześniejszymi punktami dostępowymi i bezprzewodowymi kartami sieciowymi (NIC). Niestety, jeśli atakujący odczyta dwie wiadomości zaszyfrowane tym samym kluczem za pomocą RC4, atakujący może natychmiast znaleźć klucz. W konsekwencji, WEP faktycznie szyfruje każdą ramkę kluczem na ramkę, który składa się ze współdzielonego klucza RC4 oraz 24-bitowego wektora inicjalizacji (IV), który jest inny dla każdej ramki. Nadawca losowo generuje IV. Nadawca przesyła również IV w czystym nagłówku ramki, aby odbiorca mógł się tego nauczyć. Odbiornik odszyfrowuje ramkę znanym współdzielonym kluczem plus wektor inicjujący specyficzny dla ramki. Niestety, 24-bitowe IV są zbyt krótkie. W przypadku 24-bitowego IV wiele ramek „wycieknie" kilka bitów tajnego klucza. Jeśli firma szyfruje wystarczająco duży ruch przy użyciu tego samego tajnego klucza, osoba atakująca może często obliczyć cały tajny klucz w ciągu dwóch lub trzech minut.

Perspektywiczny

Biorąc pod uwagę, jak łatwo i szybko można złamać WEP, nie ma sensu, aby dziś korporacje korzystały z WEP. W rzeczywistości daje to tylko fałszywe poczucie bezpieczeństwa, a to może być gorsze niż jego brak.

TEST CIII

a. Jaki był pierwszy podstawowy standard bezpieczeństwa sieci bezprzewodowej?

b. Jakiego algorytmu szyfrowania używa?

c. Dlaczego stałe klucze współdzielone są niepożądane?

d. Jakiego klucza na klatkę używa komputer WEP lub punkt dostępu do szyfrowania podczas transmisji?

e. Jaki błąd popełniła grupa robocza 802.11 przy wyborze długości IV?

f. Jak długo może dziś potrwać złamanie WEP?

g. Czy korporacje powinny dziś używać WEP dla bezpieczeństwa?

Zabezpieczony dostęp do sieci Wi-Fi (WPA)

Niepowodzenie WEP spowodowało zamieszanie w rozwijającej się branży WLAN. Wiele korporacji zawiesiło wdrażanie sieci WLAN lub nawet wyłączyło istniejące sieci WLAN. Doprowadziło to do wysiłków grupy roboczej 802.11, aby stworzyć standard 802.11i. Jednak powolne tempo prac rozwojowych frustrowało producentów. Zwrócili się do organizacji Wi-Fi Alliance, która zwykle poświadcza jedynie działanie urządzeń 802.11. Jeśli sprzęt jest sprzedawany z etykietą Wi-Fi na

opakowaniu, przeszedł on certyfikację zgodności operacyjnej Wi-Fi Alliance. Organizacja Wi-Fi Alliance wykorzystała wczesny projekt standardu 802.11i i stworzyła własny standard, który nazwał Wi-Fi Protected Access (WPA). Aby szybko wydobyć standard i dostosować WPA do wczesnego sprzętu, który miał ograniczoną moc obliczeniową i pamięć RAM, stowarzyszenie Wi-Fi Alliance wybrało stosunkowo słabe metody zabezpieczeń. Jak pokazuje Rysunek, WPA używa do szyfrowania stosunkowo słabego szyfru RC413 w celu zapewnienia poufności i używa jedynego umiarkowanie silnego protokołu Temporal Key Integrity Protocol (TKIP) do kluczowania i ponownego wprowadzania kluczy.

Cryptographic Characteristic	WEP	WPA	802.11i (WPA2)
Cipher for confidentiality	RC4 with a flawed implementation	RC4 with 48-bit initialization vector (IV)	AES with 128 -bit keys
Automatic rekeying	None	Temporal Key Integrity Protocol (TKIP), which has been partially cracked	AES-CCMP mode
Overall cryptographic strength	Negligible	Weaker but no complete crack to date	Extremely strong
Operates in 802.1X (enterprise) mode?	No	Yes	Yes
Operates in pre-shared key (personal) mode?	No	Yes	Yes

Chociaż nie było żadnych opublikowanych pęknięć dla WPA jako całości, przynajmniej w momencie pisania tego tekstu, TKIP został częściowo złamany, a specjaliści ds. Bezpieczeństwa nie czują się komfortowo z metodami zabezpieczeń WPA. WPA zwiększa bezpieczeństwo RC4 głównie poprzez zwiększenie IV z 24 bitów do 48 bitów. Rozszerzenie to znacznie zmniejsza wycieki, dzięki czemu RC4 jest znacznie trudniejszy do złamania, zapewniając dobre zabezpieczenie WPA zapewniające poufność. Chociaż WPA podtrzymywało rozwój branży WLAN, grupa robocza 802.11 ukończyła standard 802.11i w 2002 roku. Sojusz Wi-Fi nazwał ten nowy standard WPA2 do celów testowania interoperacyjności. Obecnie prawie wszystkie bezprzewodowe punkty dostępowe i karty interfejsów sieci bezprzewodowej obsługują standard 802.11i dzięki znacznie silniejszym zabezpieczeniom. Jednak wiele firm nadal korzysta z WPA, aby uniknąć kosztów rekonfiguracji wszystkich swoich punktów dostępowych i klientów bezprzewodowych do obsługi standardu 802.11i.

TEST CIV

a. Co skłoniło Wi-Fi Alliance do stworzenia WPA?

b. Porównaj zabezpieczenia WPA i 802.11i.

c. Jak Wi-Fi Alliance nazywa 802.11i?

d. Dlaczego pomimo słabości zabezpieczeń, wiele firm nadal używa WPA zamiast 802.11i?

Tryb klucza wstępnego (PSK)

W przypadku dużych firm konieczne jest użycie 802.11i lub WPA do wdrożenia trybu 802.1X z drogim centralnym serwerem uwierzytelniającym. Jednak w przypadku bardzo małych firm i indywidualnych gospodarstw domowych korzystanie z centralnego serwera uwierzytelniającego byłoby przesadą. W związku z tym zarówno 802.11i, jak i WPA oferują tryb inny niż 802.1X, zwany trybem klucza wstępnego (PSK). WPA, który jest oparty na wczesnej wersji roboczej 802.11i, również obejmuje ten tryb, ale nazywa go trybem osobistym. W szczególności stworzono tryb PSK/osobisty dla domów lub małych firm, które mają tylko jeden punkt dostępu. Tryb PSK/osobisty został stworzony z myślą o domach lub małych firmach, które mają tylko jeden punkt dostępu. Rysunek 4-31 pokazuje, że wszyscy klienci bezprzewodowi uwierzytelniają się w punkcie dostępowym przy użyciu wspólnego klucza

początkowego używanego przez wszystkich klientów (Krok 1). Klucze współdzielone generalnie są złe dla bezpieczeństwa, ponieważ ludzie mają tendencję do postrzegania ich jako nietajnych i oddawania ich nieautoryzowanym osobom. Ponadto, jeśli ktoś odejdzie lub zostanie zwolniony, nowy tajny klucz musi zostać zainstalowany w punkcie dostępowym i wszystkich klientach. W dużych korporacjach problemy te bywają nie do pokonania. Jednak w małych firmach i domach klucze współdzielone mogą być utrzymywane w tajemnicy. Korzystanie ze współdzielonego klucza zazwyczaj oznacza, że będzie dużo ruchu zaszyfrowanego tym samym kluczem. To znacznie ułatwia programom kryptoanalizy złamanie klucza. Gdy klucz zostanie złamany, wszystkie zabezpieczenia znikną. Aby rozwiązać ten problem, 802.11i i WPA w trybie osobistym PSK używają tylko wspólny klucz początkowy bardzo krótko - gdy klient po raz pierwszy uwierzytelnia się w punkcie dostępu (Krok 2). Po uwierzytelnieniu punkt dostępowy wysyła klientowi niewspółdzielony klucz sesji (Krok 3) do użycia podczas sesji (Krok 4). Przy zaledwie kilku wiadomościach przesłanych przy użyciu wspólnego klucza początkowego, kryptoanaliza w celu wykrycia wspólnego klucza początkowego jest praktycznie niemożliwe. Jednak tryb PSK/osobisty ma jeden poważny problem z bezpieczeństwem operacyjnym. O ile wspólny klucz początkowy nie jest złożony, kryptoanaliza klucza początkowego będzie nie tylko możliwa, ale i łatwa. W praktyce administrator lub użytkownik musi wpisać hasło do każdego klienta bezprzewodowego i punktu dostępowego. Sprzęt generuje klucz z tego hasła. Długie hasła dają silne klucze, ale jeśli hasło jest zbyt krótkie, wtedy 802.11i lub WPA w trybie PSK/osobistym będą miały bardzo słabe zabezpieczenia. Hasła muszą mieć co najmniej 20 znaków, a dłuższe hasła są lepsze. W 802.11i lub WPA w trybie PSK/osobistym hasła muszą mieć co najmniej 20 znaków.

TEST CV

a. Dlaczego tryb 802.1X nie nadaje się do domów i małych biur?

b. Jaki tryb został stworzony dla domów lub bardzo małych firm z jednym punktem dostępowym?

c. W jaki sposób użytkownicy w tym trybie uwierzytelniają się w punkcie dostępowym?

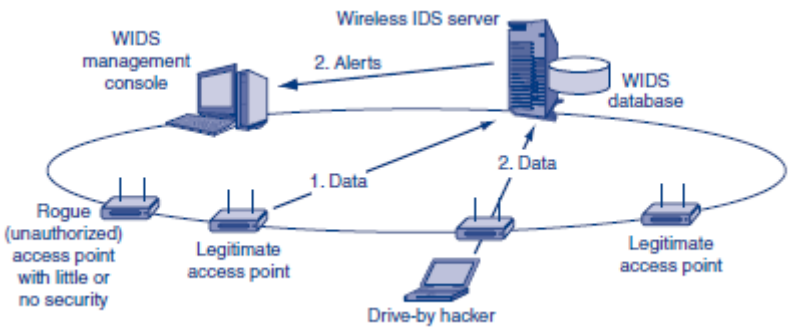
d. Dlaczego używanie wspólnego klucza początkowego nie jest niebezpieczne?

e. Jak generowane są klucze PSK/osobiste?

f. Jak długie muszą być hasła, aby zapewnić odpowiednie bezpieczeństwo?

Bezprzewodowe systemy wykrywania włamań

Firmy, które mają centralne zarządzanie wieloma punktami dostępowymi, mogą zakupić oprogramowanie do scentralizowanego bezprzewodowego systemu wykrywania włamań. Jak pokazano na rysunku, każdy punkt dostępowy staje się bezprzewodowym agentem IDS, wysyłającym odpowiednie informacje do centralnej bezprzewodowej konsoli IDS.



Konsola przesyła dane do bazy danych IDS. Sortuje również dane w bazie danych, aby znaleźć oznaki problemów. Istnieje duża szansa, że scentralizowany bezprzewodowy IDS może zidentyfikować nieuczciwe lub złe bliźniacze punkty dostępowe. Istnieją dwie alternatywy dla scentralizowanego bezprzewodowego IDS, ale żadna z nich nie jest bardzo skuteczna. Pierwszym z nich jest po prostu nie martwić się wykrywaniem włamań. Biorąc pod uwagę powszechność ataków bezprzewodowych, nie jest to rozsądne. Drugą alternatywą jest częste chodzenie po budynku z laptopem wyposażonym w bezprzewodowe oprogramowanie IDS. Wymaga to prawdopodobnie zbyt dużego nakładu pracy i nie pozwala wykryć zagrożeń pojawiających się po sprawdzeniu przez administratora bezpieczeństwa sieci bezprzewodowej części witryny pod kątem zagrożeń. Takie podejście nie jest również prawdopodobne, aby wykryć złe podwójne punkty dostępowe, które działają tylko okazjonalnie i dlatego mogą nie działać, gdy administrator sieci bezprzewodowej przeczesuje budynek w poszukiwaniu obaw.

TEST CVI

a. Jaki jest cel bezprzewodowego IDS?

b. W jaki sposób bezprzewodowe IDS uzyskują swoje dane?

c. Co to jest nieuczciwy punkt dostępowy?

d. Jakie są dwie alternatywy dla korzystania ze scentralizowanego bezprzewodowego IDS?

e. Dlaczego nie są atrakcyjne?

Fałszywe zabezpieczenia 802.11

Wiele artykułów w czasopismach dotyczących bezpieczeństwa 802.11 zawiera porady, które są obecnie powszechnie postrzegane jako oferujące jedynie fałszywe poczucie bezpieczeństwa. To są to, co mój dziadek nazywał lekarstwami na whisky. Powiedział, że ze wszystkich rzeczy, które nie leczą przeziębienia, whisky jest najbardziej popularna. Działania wycofane w tej sekcji do użytku korporacyjnego mogą wystarczyć, aby powstrzymać wścibskich sąsiadów. Jednak hakerzy drive-by z dobrym oprogramowaniem hakerskim coraz częściej wędrują po dzielnicach, aby uzyskać bezpłatny dostęp do Internetu i przeglądać komputery domowe. Ponadto te słabe „zabezpieczenia" wymagają tyle samo wysiłku lub więcej, aby skonfigurować pełne zabezpieczenia WPA lub 802.11i.

ROZSZERZONE SPEKTRUM DZIAŁANIE I BEZPIECZEŃSTWO

Wszystkie standardy bezprzewodowej sieci LAN 802.11 wykorzystują transmisję rozproszonego widma, która rozprzestrzenia sygnał w szerokim zakresie częstotliwości. Wiele osób słyszało, że wojsko wykorzystuje transmisję rozproszonego widma dla bezpieczeństwa. Jednak typy transmisji z widmem rozproszonym stosowane w 802.11 nie oferują żadnych zabezpieczeń; w rzeczywistości tryby pracy z rozproszonym widmem w sieciach WLAN 802.11 szczególnie ułatwiają stacjom znajdowanie i słyszenie się nawzajem. Użytkownicy nie powinni odrzucać hakerów, ponieważ „Mój system wykorzystuje transmisję z widmem rozproszonym, której nie można przechwycić".

WYŁĄCZANIE NADAWANIA SSID

Aby pracować z punktem dostępu, stacja musi znać identyfikator zestawu usług (SSID) punktu dostępu. Aby ułatwić stacjom znajdowanie punktów dostępu, punkty dostępu często nadają swoje identyfikatory SSID. Wyłączenie rozgłaszania SSID wydaje się oferować bezpieczeństwo. Jednak nawet jeśli rozgłaszanie identyfikatora SSID jest wyłączone, identyfikator SSID będzie nadal przesyłany w postaci przezroczystej w nagłówku każdej przesyłanej ramki. Programy sniffer nie mają problemów z

odczytaniem identyfikatorów SSID w nagłówkach ramek. Po prostu firma nie może nic zrobić, aby ukryć identyfikatory SSID przed atakującym, który ma nawet minimalne oprogramowanie hakerskie.

LISTY KONTROLI DOSTĘPU MAC

Każda karta sieciowa ma unikalny adres MAC (np. 00-1C-23-0E-1D-41). Większość punktów dostępowych można skonfigurować tak, aby obsługiwały tylko stacje znajdujące się na wstępnie zatwierdzonej liście adresów MAC. Bezprzewodowy punkt dostępowy ignoruje inne stacje. Jednak adresy MAC muszą być przesyłane w sposób jawny w każdej ramce, aby hakerzy drive-by mogli łatwo je poznać. Atakujący mogą łatwo zmienić swoje adresy MAC i wysyłać ramki, które wydają się pochodzić z jednej z zatwierdzonych stacji. Zarządzanie listami kontroli dostępu MAC to sporo pracy i nie zapewnia żadnego skutecznego zabezpieczenia.

Wdrożenie 802.11i lub WPA jest łatwiejsze

Wyłączenie rozgłaszania SSID i tworzenie list kontroli dostępu MAC są nie tylko nieskuteczne. Są czasochłonne. Włączenie 802.11i lub WPA zapewnia nie tylko pełne bezpieczeństwo (oprócz złych bliźniaczych punktów dostępowych). To także mniej pracy.

TEST CVII

a. Czy wykorzystanie transmisji z widmem rozproszonym w standardzie 802.11 zapewnia bezpieczeństwo?

b. Co to są identyfikatory SSID?

c. Czy wyłączenie rozgłaszania SSID zapewnia prawdziwe bezpieczeństwo? Wyjaśniać.

d. Co to są listy kontroli dostępu MAC?

e. Czy oferują prawdziwe bezpieczeństwo? Wyjaśniać.

WNIOSEK

Ta Część rozpoczęła się od omówienia czterech ogólnych celów, które należy wziąć pod uwagę przy tworzeniu bezpiecznego środowiska sieciowego. Cele te obejmują dostępność, poufność, funkcjonalność i kontrolę dostępu. Przyjrzeliśmy się niektórym trudnościom, z jakimi borykają się administratorzy sieci, próbując zabezpieczyć sieci. Kolejna sekcja dotyczyła ataków typu „odmowa usługi" (DoS). Chociaż firmy mogą doświadczać utraty usług, może to nie być atak DoS. Może to być wynikiem błędnego kodowania lub po prostu dramatycznego wzrostu legalnego ruchu sieciowego. Celowe ataki DoS koncentrują się na zatrzymaniu krytycznych usług lub powolnym ich degradacji w czasie. Głównymi metodami ataków DoS, które analizowaliśmy, były (1) bezpośrednie/pośrednie, (2) pośrednie, (3) odbite i (4) wysyłanie zniekształconych pakietów. Obrona przed atakami DoS obejmuje czarną dziurę, weryfikację uzgadniania TCP i ograniczanie szybkości przychodzących pakietów. Kolejnym rodzajem ataku sieciowego, który przyjrzeliśmy się, było zatrucie ARP. Dokładniej, przyjrzeliśmy się, w jaki sposób zatrucie ARP może zostać wykorzystane do przekierowania ruchu w przypadku ataku typu manin-the-middle lub całkowitego zatrzymania ruchu w przypadku ataku ARP DoS. Należy pamiętać, że zatrucie ARP wymagało od atakującego dostępu do komputera w sieci lokalnej. Przekierowywanie ruchu z wykorzystaniem ARP poisoning jest atakiem zarówno na funkcjonalność, jak i poufność sieci. Następnie przyjrzeliśmy się bezpieczeństwu przewodowych sieci LAN, które prawie zawsze korzystają z technologii Ethernet opracowanej przez Grupę Roboczą 802.3. Inna grupa robocza, 802.1, opracowała standard 802.1X, aby uniemożliwić intruzom podłączenie laptopa do gniazdka ściennego w celu uzyskania dostępu do sieci. W trybie 802.1X istnieją trzy

urządzenia. Suplikantem jest komputer klienta lub serwera łączący się z siecią. Acentralny serwer uwierzytelniania sprawdza poświadczenia. Ten centralny serwer uwierzytelniania jest zwykle zarządzany przez standard RADIUS. Przełącznik grupy roboczej Ethernet, z którym łączy się komputer kliencki lub serwer, nazywany jest wystawcą uwierzytelniającą. Dopóki komputer nie zostanie uwierzytelniony, port, z którym się łączy, jest nieautoryzowany i będzie przekazywał tylko informacje uwierzytelniające. Interakcje uwierzytelniania są regulowane przez protokół Extensible Authentication Protocol (EAP). Przyjrzeliśmy się interakcjom EAP wymaganym do uwierzytelnienia się komputera podłączonego do portu przełącznika grupy roboczej. W przypadku większości interakcji wystawca uwierzytelnienia przełączania grupy roboczej jedynie przekazuje interakcje EAP między podłączonym komputerem a centralnym serwerem uwierzytelniania. W związku z tym, gdy dodawane są nowe metody uwierzytelniania, nie trzeba wcale zmieniać wartości uwierzytelniającej. Kolejna sekcja skupiała się na atakach bezprzewodowych. Trzy rodzaje ataków na sieć bezprzewodową, które przyjrzeliśmy się, to (1) nieautoryzowany dostęp do sieci, (2) atak typu man-in-the-middle przy użyciu złego bliźniaka oraz (3) ataki typu „odmowa usługi" w sieci bezprzewodowej. Nawet jeśli firma wdroży podstawowy protokół bezpieczeństwa, taki jak WPA, problemy z bezpieczeństwem pozostają. Najlepszym sposobem radzenia sobie z zagrożeniem ze strony złych bliźniaczych punktów dostępowych jest ustanowienie sieci VPN między klientem bezprzewodowym a serwerem, z którym ostatecznie chce pracować. Ta sieć VPN może korzystać ze wstępnie współdzielonego sekretu między komputerem bezprzewodowym a komputerem, z którym chce się połączyć. Zły punkt dostępu bliźniaków nie może przechwycić wstępnie udostępnionych sekretów, ponieważ te sekrety nigdy nie są przesyłane. Początkowo grupa robocza 802.11 stworzyła podstawowy standard bezpieczeństwa WEP dla ruchu związanego z bezpieczeństwem przepływającego między komputerami bezprzewodowymi a bezprzewodowym punktem dostępowym. Ten standard był katastrofą. WEP to stara wiadomość i od dawna jest wypierany przez lepsze standardy kontroli dostępu. W 2002 roku 802.11 Working Group zakończyła prace nad standardem 802.11i, który opisuje, jak korzystać z zabezpieczeń 802.1X, w tym EAP, w bezprzewodowych sieciach LAN. Kluczową innowacją w standardzie 802.11i było zapewnienie bezpieczeństwa między klientem bezprzewodowym a punktem dostępu przed rozpoczęciem interakcji EAP. Jest to konieczne, ponieważ EAP jest łatwy do pokonania w niezabezpieczonym środowisku. Inna organizacja, Wi-Fi Alliance, opracowała standard zastępczy przed ukończeniem standardu 802.11i. W oparciu o wczesny projekt 802.11i, Alliance stworzył standard Wi-Fi Protected Access (WPA). Chociaż standard 802.11i jest już dostępny od kilku lat i używa silniejszych metod kryptograficznych niż WPA i chociaż WPA został częściowo złamany, wiele firm, które zainwestowały wcześnie w zabezpieczenia WPA, niechętnie rekonfiguruje swoje punkty dostępowe i komputery bezprzewodowe do korzystania ze standardu 802.11i. Firmy zaczynają zarządzać wszystkimi swoimi punktami dostępowymi z centralnej konsoli zarządzania. Firmy, które to robią, mogą używać bezprzewodowych systemów wykrywania włamań do lokalizowania problemów, takich jak złe podwójne punkty dostępowe i nieuczciwe punkty dostępowe, które są konfigurowane przez osoby i działy i które zwykle mają niewielkie lub żadne zabezpieczenia. Zakończyliśmy rozdział dyskusją na temat fałszywych środków bezpieczeństwa sieci bezprzewodowej, które wymagają pracy w celu skonfigurowania, ale nie zapewniają rzeczywistej ochrony przed hakerami typu drive-by, którzy mają łatwe do pobrania oprogramowanie atakujące. W kolejnych rozdziałach dotyczących kontroli dostępu (rozdział 5) i zapór sieciowych (rozdział 6) dokładniej przyjrzymy się sposobom obrony przed atakami sieciowymi przedstawionymi w tych rozdziałach.

Pytania do przemyślenia

1. Rozróżnij EAP i RADIUS pod względem funkcjonalności.

2. Dlaczego ochrona całego ruchu IP firmy przez IPsec byłaby pożądana? Podaj wiele powodów.

3. Jakich zagrożeń bezpieczeństwa sieci bezprzewodowej LAN nie zajmują się 802.11i i WPA?

4. Biorąc pod uwagę słabość komercyjnych zabezpieczeń sieci WAN, jak myślisz, dlaczego firmy nadal korzystają z technologii WAN bez dodatkowych zabezpieczeń kryptograficznych?

5. Co mogłaby zrobić firma, gdyby korzystała z komercyjnej sieci WAN i pojawiła się luka, która pozwalała atakującym łatwo znaleźć informacje o routingu, a tym samym podsłuchiwać transmisje firmowe?

6. Obecnie standard 802.1X jest stosowany głównie do bezprzewodowych sieci LAN, a nie do przewodowych sieci LAN. Jak myślisz, dlaczego tak jest?

KONTROLA DOSTĘPU

WPROWADZENIE

Kontrola dostępu

W Części 2 widzieliśmy, że firma musi opracować plan bezpieczeństwa dla każdego wrażliwego zasobu. Część tego planu bezpieczeństwa skupi się na kontroli dostępu. Atakujący, którzy nie mogą dostać się do twoich zasobów, nie mogą ich skrzywdzić. Firmy muszą planować kontrole dostępu, wdrażać wymagane kontrole i reagować, gdy kontrole zawiodą. Formalnie zdefiniowana kontrola dostępu to oparta na zasadach kontrola dostępu do systemów, danych i dialogów. Istnieje wiele sposobów kontrolowania dostępu, w tym bariery fizyczne, hasła i dane biometryczne. Wiele z tych mechanizmów kontroli dostępu korzysta z zabezpieczeń kryptograficznych, dlatego przed omówieniem kontroli dostępu omówiliśmy kryptografię. Jednak wiele technik kontroli dostępu w ogóle nie wykorzystuje kryptografii, a inne używają kryptografii tylko stycznie. Kontrola dostępu to nie tylko kryptografia.

Kontrola dostępu to oparta na zasadach kontrola dostępu do systemów, danych i dialogów.

Polityka ma kluczowe znaczenie dla kontroli dostępu. Jak omówiono w Części 2, całe bezpieczeństwo zaczyna się od opracowania polityk bezpieczeństwa dla poszczególnych zasobów. Polityki, gdy są właściwie tworzone, koordynują wszystkich i kierują wdrażaniem i nadzorem.

Uwierzytelnianie, autoryzacje i audyt

Kontrole dostępu mają trzy funkcje, które są znane pod wspólną nazwą AAA (uwierzytelnianie, autoryzacja i audyt).

Uwierzytelnianie to proces oceny tożsamości każdej osoby deklarującej posiadanie uprawnień do korzystania z zasobu. Osoba lub proces żądający dostępu jest petentem. Weryfikatorem jest osoba lub proces zapewniający przyjęcie. Suplikant uwierzytelnia siebie lub siebie przed weryfikatorem, wysyłając dane uwierzytelniające (hasło, skan odcisku palca itp.).

Autoryzacje to określone uprawnienia, które powinien posiadać dany uwierzytelniony użytkownik, biorąc pod uwagę jego uwierzytelnioną tożsamość. Na przykład Bob może mieć uprawnienia do odczytu pliku, ale nie może go zmieniać ani usuwać. Carol może nawet nie mieć uprawnień do zobaczenia nazwy pliku.

Audyt to zbieranie informacji o działaniach danej osoby w plikach dziennika. Pliki dziennika mogą być analizowane w czasie rzeczywistym lub zapisywane do późniejszej analizy. Bez audytu naruszenia zasad uwierzytelniania i autoryzacji będą prawdopodobnie szerzyły się.

Uwierzytelnianie

Większość tej części skupia się na uwierzytelnianiu, które jest najbardziej złożoną częścią kontroli dostępu AAA. Aby zostać uwierzytelnionym, musisz pokazać poświadczenia weryfikatora, które są oparte na jednym z następujących elementów:

• Co wiesz (hasło lub klucz prywatny),

• Co posiadasz (fizyczny klucz lub inteligentną kartę),

• Kim jesteś (odcisk palca) lub

• Co robisz (jak konkretnie wymawiasz hasło).

Poza hasłami

Kiedyś proste hasła wystarczały do większości potrzeb uwierzytelniania. Obecnie jednak firmy przekonują się, że muszą korzystać z coraz większej różnorodności technologii uwierzytelniania, w tym kart dostępu, tokenów, uwierzytelniania biometrycznego i uwierzytelniania kryptograficznego. Ta różnorodność metod uwierzytelniania pozwala nam wybrać taką, która ma odpowiednie mocne strony dla zagrożeń związanych z danym zasobem.

Uwierzytelnianie dwuetapowe

Coraz ważniejszą zasadą uwierzytelniania jest uwierzytelnianie dwuskładnikowe, w którym do uzyskania dostępu muszą być używane dwie różne formy uwierzytelniania. Uwierzytelnianie dwuskładnikowe zapewnia dogłębną ochronę, co, jak widzieliśmy, było podstawową zasadą planowania bezpieczeństwa w Części 2. Niektóre systemy używają nawet uwierzytelniania wieloskładnikowego, które wykorzystuje więcej niż dwie formy uwierzytelniania. Jednak uwierzytelnianie dwuskładnikowe może zapewniać znacznie słabsze uwierzytelnianie, niż wydaje się oferować. Bruce Schneier1 zauważył, że konie trojańskie i ataki typu man-in-the middle mogą podważyć siłę uwierzytelniania dwuskładnikowego.

• Po pierwsze, jeśli komputer kliencki jest zainfekowany koniem trojańskim, koń trojański może wysyłać transakcje, gdy użytkownik już uwierzytelnił się w witrynie handlu elektronicznego. Jeśli komputer użytkownika zostanie naruszony, uwierzytelnianie dwuskładnikowe nic nie znaczy.

• Po drugie, uwierzytelnianie dwuskładnikowe często można pokonać za pomocą ataku typu man-in-themiddle. Jeśli użytkownik zaloguje się na fałszywą witrynę bankową, fałszywa witryna może działać jako cichy łącznik między prawdziwą witryną bankową. Po pomyślnym uwierzytelnieniu użytkownika fałszywa strona internetowa może wykonywać własne transakcje na prawdziwej stronie internetowej.

Indywidualna i oparta na rolach kontrola dostępu

Zwykle myślimy o regułach kontroli dostępu, które mają zastosowanie do poszczególnych użytkowników i urządzeń. Jednak zawsze, gdy jest to możliwe, firmy starają się stosować kontrolę dostępu opartą na rolach (RBAC), która opiera się na rolach organizacyjnych, a nie na poszczególnych osobach. Jedną rolą może być kupujący. Ta rola może zostać przypisana kilku osobom. Chociaż logowaliby się do zasobów za pomocą własnych kont, kontrola dostępu byłaby oparta na ich rolach jako kupujących.

• Tworzenie reguł kontroli dostępu w oparciu o role jest tańsze niż przypisywanie reguł kontroli dostępu oddzielnie do poszczególnych kont nabywców, ponieważ jest mniej przydziałów do wykonania.

• Tworzenie reguł kontroli dostępu opartych na rolach zmniejsza również liczbę możliwości wystąpienia błędów.

• Wreszcie, gdy dana osoba przestaje być kupującym, może po prostu zostać usunięta z grupy kupującego. Jest to o wiele tańsze i mniej prawdopodobne, że spowoduje błędy niż przeglądanie uprawnień każdej osoby i decydowanie, które należy usunąć, gdy przestaje być kupującym.

Kontrole organizacyjne i ludzkie

Wiele technologii kontroli dostępu, które zobaczymy w tej Części, oferuje niezwykle silne zabezpieczenia. Jednak te technologie są zawsze osadzone w kontekście organizacyjnym i ludzkim. Stwarza to możliwości obejścia technologii. Na przykład, jeśli luźny lub niewyszkolony pracownik daje

oszustowi klucz prywatny do użycia podczas uwierzytelniania, siła uwierzytelniania klucza publicznego nic nie znaczy. Aby podać inny przykład, jeśli firma omyłkowo ufa partnerowi biznesowemu (ze złymi intencjami) i zapewnia mu dostęp do całego systemu, wówczas wszystkie narzędzia kontroli dostępu nic nie znaczą.

TEST CVIII

a. Wymień kontrole dostępu AAA.

b. Wyjaśnij każdy w zdaniu.

c. Jakie są cztery podstawy poświadczeń uwierzytelniających?

d. Jaka jest obietnica uwierzytelniania dwuskładnikowego?

e. Jak koń trojański może pokonać tę obietnicę?

f. Jak atak typu man-in-the-middle może pokonać tę obietnicę?

g. Co to jest RBAC? (Nie tylko to przeliteruj).

h. Dlaczego RBAC jest tańszy niż kontrola dostępu oparta na indywidualnych kontach?

i. Dlaczego jest mniej podatny na błędy? (Odpowiedź nie znajduje się konkretnie w tekście.)

j. Dlaczego technologicznie silna kontrola dostępu nie zapewnia silnej kontroli dostępu w rzeczywistych organizacjach?

Kontrole dostępu do wojskowych i narodowych organizacji bezpieczeństwa

To jest test o bezpieczeństwie korporacyjnym. W wojsku i narodowych organizacjach bezpieczeństwa pojawiają się dodatkowe względy kontroli dostępu. Korporacje zwykle stosują albo indywidualne kontrole dostępu, albo kontrole dostępu oparte na rolach. W wojskowych i narodowych organizacjach bezpieczeństwa powszechne są dwie inne formy kontroli dostępu. W obowiązkowej kontroli dostępu wydziały nie mają możliwości zmiany reguł kontroli dostępu ustalonych przez wyższe władze. W zasadzie zapewnia to bardzo silne bezpieczeństwo. W praktyce jest to trudne do utrzymania, ponieważ prawie zawsze potrzebna jest pewna elastyczność. W związku z tym organizacje zazwyczaj mogą korzystać z uznaniowej kontroli dostępu, w ramach której departament ma swobodę w przyznawaniu dostępu osobom, zgodnie ze standardami polityki ustalonymi przez wyższe władze.

Wielopoziomowe zabezpieczenia

Dokumenty i inne zasoby różnią się wrażliwością. Zazwyczaj organizacje wojskowe i bezpieczeństwa narodowego mają wielopoziomowy system bezpieczeństwa, który ocenia dokumenty według wrażliwości. Niektóre dokumenty będą całkowicie publiczne, podczas gdy inne będą poufne, ale niejawne (SBU). Poza tym istnieje kilka poziomów klasyfikacji, takich jak tajne i ściśle tajne. Zapewnienie dostępu do informacji niejawnych wymaga starannego przemyślenia. Oczywiście, jeśli ktoś nie ma poświadczenia bezpieczeństwa, nie powinno mu się pozwolić czytać ściśle tajnego dokumentu. Inne kwestie wymagają więcej przemyślenia. Na przykład, co się stanie, jeśli pojedynczy akapit z niejawnego dokumentu zostanie skopiowany do poufnego, ale niesklasyfikowanego dokumentu? Aby poradzić sobie z takimi problemami i radzić sobie z różnymi sytuacjami dostępu, organizacje stosujące wielopoziomowe zabezpieczenia muszą stosować złożone modele kontroli dostępu. Ta książka koncentruje się na bezpieczeństwie korporacyjnym, w którym tradycyjne zabezpieczenia wielopoziomowe nie działają z wielu powodów. W związku z tym nie będziemy omawiać modeli kontroli dostępu.

TEST CIX

a. Rozróżnij obowiązkową kontrolę dostępu i uznaniową kontrolę dostępu.

b. Co to jest zabezpieczenie wielopoziomowe?

c. Czym są dokumenty SBU?

d. Czy muszą być uwzględniane w kontroli dostępu?

e. Dlaczego potrzebne są modele kontroli dostępu?

DOSTĘP FIZYCZNY I BEZPIECZEŃSTWO

Wiele ataków odbywa się zdalnie za pośrednictwem sieci. Jednak atakujący mogą również wejść do budynku, podejść do komputera, a następnie go ukraść lub zhakować. Chociaż kontrola dostępu do sieci ma kluczowe znaczenie, specjaliści ds. bezpieczeństwa IT muszą rozumieć fizyczną kontrolę dostępu do budynków, stref o wysokim poziomie bezpieczeństwa w budynkach i poszczególnych komputerów. Sekcja ta zostanie oparta na Klauzuli bezpieczeństwa 9 normy ISO/IEC 27002, Bezpieczeństwo fizyczne i środowiskowe.

Ocena ryzyka

Klauzula bezpieczeństwa 9 zakłada, że analiza ryzyka została już wykonana. Specjaliści ds. bezpieczeństwa IT muszą zacząć od zrozumienia zagrożeń występujących na poziomie budynków, bezpiecznych stref wewnątrz budynków i komputerów. Bank oczywiście potrzebuje znacznie silniejszego bezpieczeństwa obwodowego niż uniwersytet, a serwerownia potrzebuje silniejszego bezpieczeństwa niż zwykła powierzchnia biurowa.

ISO/IEC 9.1: Obszary bezpieczne

Klauzula bezpieczeństwa 9 ma dwie główne kategorie bezpieczeństwa. Pierwsza z nich to 9.1, Strefy bezpieczne, która dotyczy zabezpieczania obszarów fizycznych, w tym całych budynków, pomieszczeń ze sprzętem, obszarów biurowych, obszarów dostawy i wysyłki oraz ogólnych obszarów publicznych. Główna kategoria bezpieczeństwa 9.1 ma sześć kontrolek.

OBWÓD BEZPIECZEŃSTWA FIZYCZNEGO

Ważna jest kontrola wejść do budynków. Najlepiej byłoby, gdyby istniał jeden punkt wejścia. Dodatkowo ściany oddzielające budynek od zewnątrz powinny być solidne i nie powinno być szczelin, przez które ludzie mogliby wejść. Jeśli wymagania bezpieczeństwa wymagają recepcji z personelem, powinna ona być stale obsadzana. Chociaż pojedynczy punkt wejścia ułatwia kontrolę, każdy budynek ma wyjścia awaryjne, które można otworzyć w celu ewakuacji, gdy jest to uzasadnione. Jeśli intruz ma w budynku konfederata, może on otworzyć jedne z tych drzwi, aby wpuścić napastnika. W związku z tym wyjścia awaryjne powinny być alarmowane, monitorowane (najlepiej za pomocą kamer) i często testowane. We wszystkich przypadkach przepisy bezpieczeństwa muszą być zgodne z kodami przeciwpożarowymi. Co najważniejsze, blokowanie wyjść pożarowych przed ucieczką z baru jest nielegalne.

KONTROLE WEJŚCIA FIZYCZNEGO

Operacyjnie każdy dostęp fizyczny musi być autoryzowany. (W terminologii CobiT wpis musi być uzasadniony, autoryzowany, rejestrowany i monitorowany – w tym w sytuacjach awaryjnych). Autoryzacje dostępu powinny być często przeglądane i aktualizowane. Odwiedzający powinni być

zalogowani i wylogowani oraz powinni być nadzorowani przez cały czas przebywania w budynku. Wszyscy w środku powinni nosić identyfikatory.

OBSZARY DOSTĘPU PUBLICZNEGO, DOSTAW I ZAŁADUNKU

Obszary dostaw i załadunku to wrażliwe strefy w budynku. Osoby wewnętrzne powinny mieć ograniczony dostęp do obszarów dostaw i załadunku, a osoby zajmujące się dostawami i odbiorami nie powinny mieć dostępu do budynku poza rampą dostawczą i załadunkową. Przychodzące przesyłki powinny być kontrolowane i rejestrowane. Przesyłki wychodzące należy oddzielić od przesyłek przychodzących, aby zmniejszyć ryzyko kradzieży.

ZABEZPIECZANIE BIUR, POMIESZCZEŃ I OBIEKTÓW

Niektóre obszary budynku będą szczególnie wrażliwe. Należy im zapewnić dodatkowe zabezpieczenie, ale to zabezpieczenie musi być zgodne z normami BHP. Wrażliwe obszary powinny mieć zamki z kluczami, kartami dostępu lub innymi mechanizmami ograniczającymi dostęp. Bezpieczne obszary powinny znajdować się z dala od publicznego dostępu i powinny być jak najmniej rzucające się w oczy. Wewnętrzne książki telefoniczne i książki telefoniczne zawierające wykaz tych obszarów nie powinny być publicznie dostępne.

OCHRONA PRZED ZAGROŻENIAMI ZEWNĘTRZNYMI I ŚRODOWISKOWYMI

Chociaż bezpieczeństwo IT dotyczy przede wszystkim ludzkich intruzów, bezpieczeństwo budynków jest nierozerwalnie związane również z zagrożeniami nieludzkimi. Niebezpieczne i łatwopalne materiały należy umieszczać z dala od wrażliwych obszarów, a także powinien być dostępny odpowiedni sprzęt do gaszenia pożaru. Urządzenia do reagowania w przypadku katastrof i nośniki kopii zapasowych powinny być umieszczone w bezpiecznej odległości od budynku.

ZASADY PRACY W OBSZARACH BEZPIECZNYCH

Firma powinna mieć specjalne zasady dla osób pracujących w bezpiecznych miejscach. Co najważniejsze, należy unikać pracy bez nadzoru. Jeśli nikt nie znajduje się w bezpiecznym miejscu, należy go okresowo zamykać i sprawdzać. W większości przypadków zabroniony będzie sprzęt fotograficzny, w tym aparaty w telefonach komórkowych. Nośniki danych, takie jak zapisywalne dyski oraz pamięć USB i dyski twarde, również powinny być zabronione. Te media umożliwiają teraz fizyczną penetrację atakującego do kradzieży informacji o wartości gigabajtów. Oczywiście w wielu przypadkach należy wykluczyć również nieautoryzowane komputery PC, inteligentne telefony komórkowe i inne urządzenia komputerowe. Należy przeprowadzać inspekcje osób przybywających i wychodzących w celu zapewnienia, że przepisy dotyczące urządzeń nagrywających, nośników i innych zakazanych urządzeń są skuteczne. Ludzie muszą zostać powiadomieni, że takie przeszukania będą miały miejsce, a przeszukania muszą być prowadzone zgodnie z polityką firmy, przepisami prawa i umowami związkowymi. Nie trzeba dodawać, że ograniczenia dotyczące urządzeń i nośników zapisu są niezwykle trudne do wprowadzenia w życie, chociaż firmy mogą korzystać z technologii, aby uniemożliwić podłączanie urządzeń nagrywających do komputerów lub sieci.

TEST CX

a. Dlaczego ważne jest posiadanie pojedynczego punktu wejścia do budynku?

b. Dlaczego wyjścia awaryjne są ważne?

c. Co należy z nimi zrobić?

d. Wymień cztery elementy autoryzacji wjazdu do CobiT.

e. Dlaczego bezpieczeństwo doku załadunkowego jest ważne?

f. Jakie zasady kontroli dostępu należy stosować do doków załadunkowych?

g. Jakie kroki należy podjąć, aby zmniejszyć niebezpieczeństwo szkód w środowisku?

h. Wymień zasady pracy w bezpiecznych obszarach.

Bezpieczeństwo sprzętu ISO/IEC 9.2

Główna kategoria bezpieczeństwa 9.1 dotyczy bezpieczeństwa witryny. Z kolei główna kategoria bezpieczeństwa 9.2 skupia się na bezpieczeństwie sprzętu. Posiada siedem kontrolek.

UMIESZCZENIE I OCHRONA SPRZĘTU

Wrażliwy sprzęt powinien być umieszczony (umieszczony) w bezpiecznych miejscach, aby zminimalizować dostęp. Obszary te nie powinny być narażone na uszkodzenia spowodowane dymem, awarią dopływu wody, aktami wandalizmu i innymi zagrożeniami. Lokalizacja jest synonimem lokalizacji lub umieszczania. Pochodzi od strony głównej słowa. Sprzęt powinien być ustawiony tak, aby osoby nieupoważnione nie mogły odczytać informacji na ekranach. Powinny również istnieć wytyczne dotyczące jedzenia i picia oraz dobrze monitorowane kontrole temperatury i wilgotności, które mogą być szkodliwe dla sprzętu i mediów.

NARZĘDZIA WSPIERAJĄCE

Ludzie i sprzęt potrzebują prądu, wody i HVAC (ogrzewanie, wentylacja i klimatyzacja). Te media muszą być dostarczane na odpowiednim poziomie i powinny być regularnie sprawdzane i testowane.

Szczególną uwagę należy zwrócić na zasilanie elektryczne, ponieważ utrata mocy elektrycznej może spowodować utratę dostępności lub nawet trwałe uszkodzenie. Zasilacz bezprzerwowy (UPS) ma baterię, która może zasilać sprzęt przez krótki czas po awarii. Zasilacze UPS umożliwiają uporządkowane wyłączanie podczas awarii zasilania. W przypadku dłuższych przestojów firmy mogą utrzymywać zapasowe generatory elektryczne zasilane benzyną. Zarówno zasilacze UPS, jak i generatory zapasowe powinny być regularnie sprawdzane i testowane. W przypadku generatorów rezerwowych, inspekcje powinny obejmować adekwatność zasilania paliwem.

BEZPIECZEŃSTWO OKABLOWANIA

Jeśli kable elektryczne lub sieciowe zostaną przecięte, firma utraci obsługę. Jeśli kable sieciowe są podsłuchiwane, intruz może odczytać zawartość pakietów. Tam, gdzie to możliwe, okablowanie powinno przebiegać pod ziemią lub w ścianach. Tam, gdzie nie jest to możliwe, przewody powinny być prowadzone przez kanały (najlepiej opancerzone) i nie powinny być prowadzone przez obszary publiczne. Szafy z okablowaniem, w których różne wiązki przewodów są ze sobą połączone, powinny być zamknięte i monitorowane.

BEZPIECZEŃSTWO PODCZAS KONSERWACJI SPRZĘTU POZA ZAKŁADEM

Konserwacja sprzętu jest łatwa do przeoczenia, ale ma kluczowe znaczenie dla dostępności. Sprzęt należy konserwować zgodnie ze specyfikacją dostawcy. Jeżeli konserwacja wiąże się z zabraniem sprzętu poza miejsce, nawet tymczasowo, tylko upoważnione osoby powinny mieć możliwość jego usunięcia. Sprzęt musi zostać wylogowany i ponownie zalogowany. Ponadto, gdy sprzęt ma zostać zabrany poza miejsce, wszystkie wrażliwe informacje muszą zostać usunięte.

BEZPIECZEŃSTWO SPRZĘTU POZA OBIEKTEM

Gdy sprzęt jest zabierany poza teren zakładu w celu konserwacji lub użytkowania, należy zachować szczególną ostrożność. Firma nie tylko jest pozbawiona aktywów fizycznych, ale wrażliwe dane firmy mogą być również narażone na ewentualną kradzież lub utratę. Sprzętu znajdującego się poza terenem zakładu nigdy nie należy pozostawiać bez nadzoru. Jeśli sprzęt jest przeznaczony do użytku domowego, powinny znajdować się zamykane szafki na dokumenty, a wszystkie dokumenty powinny być zamknięte na klucz, gdy nie są używane. Najlepiej, jeśli sprzęt zostanie również zablokowany. Biorąc pod uwagę znaczenie kradzieży i utraty urządzenia przenośnego, pożądane jest ubezpieczenie.

BEZPIECZNA UTYLIZACJA LUB PONOWNE UŻYCIE SPRZĘTU

Gdy sprzęt ma zostać wyrzucony, dane wrażliwe muszą zostać usunięte przed utylizacją sprzętu. Dzieje się tak, nawet jeśli sprzęt ma być ponownie wykorzystany w firmie. Jeśli sprzęt nie ma być ponownie używany, dysk twardy powinien zostać fizycznie zniszczony lub wymazany za pomocą programów do czyszczenia dysku (znanych również jako dyski typu kill), które uniemożliwiają odzyskanie danych. (Ponowne formatowanie dysku nie jest wystarczające.)

USUWANIE NIERUCHOMOŚCI

Kiedy nieruchomość jest usuwana do użytku lub utylizacji poza terenem zakładu, powinno to odbywać się wyłącznie po uzyskaniu odpowiedniego zezwolenia. Ponadto powinny istnieć ograniczenia dotyczące tego, kto może udzielić takiego upoważnienia. Zazwyczaj będą obowiązywać ograniczenia czasowe dotyczące użytkowania poza siedzibą firmy. Dodatkowo, kiedy sprzęt jest pobierany lub wyprowadzany, należy to odnotować. Zasady usuwania są często naruszane, dlatego ważne są okresowe kontrole na miejscu.

TEST CXI

a. Co to jest lokalizacja?

b. Rozróżnij zasilacze UPS i generatory elektryczne.

c. Jeśli okablowanie nie może przebiegać przez ściany, co należy zrobić, aby chronić okablowanie?

d. Co należy zrobić, aby chronić laptopy zabrane poza lokalem firmy?

ei. Jakie środki kontroli należy zastosować do konserwacji sprzętu poza zakładem?

f. Jakie środki kontroli należy zastosować w przypadku utylizacji lub ponownego użycia sprzętu?

g. Jakie kontrole należy objąć pracownikami wywożącymi sprzęt poza teren zakładu?

Inne problemy z bezpieczeństwem fizycznym

Chociaż Klauzula Bezpieczeństwa 9 normy ISO/IEC 27002 jest bardzo obszerna, istnieje kilka obszarów, które wymagają dodatkowej uwagi.

TERRORYZM

Ze względu na rosnące zagrożenia ze strony terroryzmu, ataki terrorystyczne muszą być brane pod uwagę we wszystkich kwestiach bezpieczeństwa fizycznego. Na przykład nowe budynki powinny być odsunięte od ulic i chronione za pomocą łagodnego krajobrazu wzgórza. W odpowiednich sytuacjach strażnicy mogą być uzbrojeni. Mogą być również potrzebne drzwi kuloodporne do ochrony wrażliwych obszarów.

PIGGYBACKIN

Egzekwowanie kontroli wejścia jest bardzo trudne ze względu na sztuczkę socjotechniczną o nazwie piggybacking. (Nazywa się to również tailgating.) Kiedy upoważniony użytkownik otwiera drzwi za pomocą urządzenia dostępowego, intruz może przejść przez upoważnionego użytkownika. (Często intruz podchodzi do drzwi z rękami załadowanymi papierami i bezskutecznie sięga do kieszeni po klucz). piggybacking jest trudny do wyegzekwowania. Jednak dopóki nie zostanie wyeliminowane piggybacking, fizyczne zabezpieczenie dostępu jest prawie niemożliwe. Chociaż wyeliminowanie piggybackingu jest trudne, jest to możliwe z wysiłkiem. Jeden z autorów spędził godzinę w holu jednej dużej firmy komputerowej i obserwował wchodzących pracowników. Ani jednego na drugim. Inni pracownicy po prostu tego nie zrobili i nie tolerowali.

WYPOSAŻENIE MONITORUJĄCE

ISO/IEC 27002 często odnosi się do monitorowania. Zazwyczaj dotyczy to zdalnych czujników, które są połączone przewodowo z centralnym centrum bezpieczeństwa. Zwykle to centrum bezpieczeństwa jest obsadzone przez umundurowanych strażników. Jeśli czujnik zostanie aktywowany, w centrum bezpieczeństwa włączy się alarm. Jeśli przewód do czujnika jest wyłączony, powinno to również wywołać alarm. Czasami monitoring obejmuje telewizję przemysłową (CCTV), która umożliwia pracownikom ochrony wizualną obserwację obszaru. Systemy CCTV muszą być dobierane bardzo starannie. Firma nie powinna używać systemu wykorzystującego taśmę wideo, ponieważ jakość taśmy wideo gwałtownie spada wraz z ponownym użyciem taśmy. Z kolei cyfrowe systemy CCTV, które przechowują informacje na dyskach twardych i cyfrowych taśmach zapasowych, różnią się znacznie rozdzielczością obrazu, czyli liczbą elementów obrazu na ekranie. Większość cyfrowych kamer bezpieczeństwa ma niską rozdzielczość, co sprawia, że identyfikacja obiektu staje się wątpliwa. Istnieją kamery o wysokiej rozdzielczości, ale są one nieco drogie. Ponadto kamery o wysokiej rozdzielczości wymagają więcej miejsca do przechowywania nagrań niż kamery o niskiej rozdzielczości. Aby zmniejszyć obciążenie pamięci masowej, wiele systemów nagrywa wideo tylko wtedy, gdy występuje ruch. Niektóre wykraczają poza proste wykrywanie ruchu i nagrywają wideo tylko wtedy, gdy występuje określony rodzaj ruchu, na przykład, gdy obiekt większy niż ptak porusza się po ekranie od lewej do prawej.

NURKOWANIE W ŚMIETNIKU

Ostatnim powszechnym zagrożeniem związanym z budynkami jest nurkowanie w śmietniku, w którym atakujący przechodzi przez kosze na śmieci firmy w poszukiwaniu dokumentów, taśm zapasowych, dyskietek i innych nośników informacji. Termin Dumpster jest znakiem towarowym, więc będziemy używać terminu budowanie koszy na śmieci. Kosze na śmieci budowlane powinny znajdować się w bezpiecznym i oświetlonym miejscu, najlepiej pod nadzorem telewizji przemysłowej. Obszar ten musi znajdować się na terenie firmy, ponieważ po przeniesieniu koszy na śmieci poza teren firmy ich zawartość zwykle uważana jest za opuszczoną i nie podlega ochronie prawnej.

BEZPIECZEŃSTWO KOMPUTERA STACJONARNEGO

Aby zmniejszyć niebezpieczeństwo kradzieży, poszczególne komputery stacjonarne w zwykłych obszarach biurowych można przymocować do biurka za pomocą kabla, pod warunkiem, że na biurku znajduje się coś do owinięcia kabla. Ponadto każdy komputer powinien mieć ekran logowania, który wymaga złożonego hasła i wygaszacza ekranu, aby intruz nie mógł po prostu podejść do niego i go użyć.

BEZPIECZEŃSTWO NOTEBOOKA

Bezpieczeństwo notebooków zabieranych poza teren firmy to złożony temat.

TEST CXII

a. Jakie specjalne kontrole są wymagane w przypadku zagrożeń terrorystycznych?

b. Dlaczego konieczne jest zapobieganie piggybackingowi?

c. Jaką radę dałbyś firmie w sprawie CCTV?

d. Co to jest nurkowanie w śmietniku™?

e. Jak chronić kosze na śmieci?

f. Co można zrobić, aby zmniejszyć niebezpieczeństwo kradzieży komputera stacjonarnego i nieautoryzowanego nas?

HASŁA

Istnieje wiele technologii kontroli dostępu. Niewątpliwie najczęstszym jest hasło. Na przykład, aby zalogować się na serwer, zwykle musisz znać nazwę swojego konta (która nie jest tajna) i jego tajne hasło. Nazywa się to hasłem wielokrotnego użytku, ponieważ jest używane przez tygodnie lub miesiące. Natomiast hasło jednorazowe jest używane tylko raz.

Programy do łamania haseł

Za pośrednictwem sieci osoba atakująca może próbować wielokrotnie logować się przy użyciu różnych możliwych nazw kont i haseł. Jednak taki napastnik prawie zawsze zostanie zablokowany po kilku próbach. Blokady mogą frustrować użytkowników, którzy nie mogą uzyskać dostępu do zablokowanych kont, ale blokady nie dają atakującym dostępu do ich zasobów. Jeśli jednak atakujący może fizycznie wejść na stronę, ma o wiele skuteczniejszy sposób łamania haseł — zainstalowanie na serwerze programu do łamania haseł. Programy te próbują tysiące możliwych kombinacji nazwy konta/hasła na sekundę, aż jedna zadziała. Innym sposobem na wykorzystanie komputera z dostępem fizycznym jest skopiowanie pliku hasła i złamanie go później na innym komputerze. Jest to mniej natrętne niż poświęcenie czasu na uruchomienie programu do łamania haseł na serwerze podczas włamania.

TEST CXIII

a. Co to są hasła wielokrotnego użytku?

b. Dlaczego łamanie haseł w sieci jest trudne?

c. Na jakie dwa sposoby można wykorzystać programy do łamania haseł?

d. Co jest bezpieczniejsze dla krakersa? Czemu?

Zasady dotyczące haseł

Biorąc pod uwagę dużą liczbę zagrożeń, z którymi borykają się hasła wielokrotnego użytku, firmy muszą mieć silne zasady dotyczące haseł. Dobre zasady dotyczące haseł zapobiegają wykorzystywaniu przez atakujących nieodłącznych słabości związanych z używaniem haseł wielokrotnego użytku.

W tej sekcji omówimy, w jaki sposób hasła mają być używane do kontroli dostępu. W następnej omówimy, jak wzmocnić system, tworząc silne hasła, które nie są łatwe do złamania. Specjaliści ds. bezpieczeństwa muszą przetestować zarówno sposób używania haseł, jak i siłę samych haseł. Regularne audyty sprawdzają, czy przestrzegane są zasady dotyczące haseł i czy organizacja jest chroniona.

Używanie i niewłaściwe użycie hasła

Chociaż tworzenie silnych haseł jest ważne, firma potrzebuje również zasad używania haseł i zarządzania.

NIE UŻYWAJ TEGO SAMEGO HASŁA W WIELU STRONACH

Ludzie często używają tego samego hasła w wielu witrynach. Na przykład badanie przeprowadzone przez Cyota z 2005 roku wykazało, że 44 procent ankietowanych osób używało tego samego hasła w wielu witrynach, a 37 procent klientów bankowości internetowej używało tego samego hasła w mniej bezpiecznych witrynach. Gdy hasła są używane w wielu witrynach, jeśli hasło zostanie złamane w jednej witrynie, zostanie naruszone we wszystkich witrynach. W rzeczywistości atakujący czasami zapraszają kogoś do atrakcyjnej witryny i pozwalają mu wybrać własną nazwę użytkownika i hasło. Atakujący próbują następnie wypróbować tę nazwę użytkownika i hasło w innych witrynach, których prawdopodobnie użyje ofiara. Posiadanie zasady, zgodnie z którą użytkownicy muszą używać różnych haseł w różnych witrynach, jest ważne, ale jest bardzo trudne do wyegzekwowania. Użytkownikom bardzo trudno jest zapamiętać różne hasła w różnych witrynach. Używanie różnych haseł jest nawet trudne, jeśli hasła są zapisane w księdze haseł. Aby rozwiązać ten problem, istnieją programy do zarządzania hasłami, które automatycznie zarządzają wieloma hasłami. Programy te automatycznie generują silne hasła dla każdej witryny i zapamiętują te hasła. Niestety, te obiecujące programy są nieco nieporęczne w użyciu, zwłaszcza jeśli użytkownik ma kilka różnych komputerów i musi udostępniać między nimi informacje o hasłach.

ZASADY CZASOWE HASŁA

Zasady dotyczące haseł powinny również wymagać częstej zmiany haseł. Hasła użytkowników powinny być zmieniane mniej więcej co 90 dni. W ten sposób, jeśli atakujący pozna hasło, będzie mógł z niego korzystać tylko przez ograniczony czas. Hasła kluczowe powinny być zmieniane częściej. Ponadto użytkownikom należy zabronić ponownego używania starszego hasła do konta, aby uniemożliwić użytkownikowi przechodzenie przez kilka haseł.

POLITYKI ZABRANIAJĄCE WSPÓLNE KONTA

Jedną ze szczególnie niebezpiecznych praktyk związanych z hasłami jest posiadanie kilku osób w grupie, które współdzielą jedno konto. Każda osoba będzie się logować przy użyciu tej samej nazwy konta i hasła. Współdzielone nazwy kont i hasła są złe z trzech powodów:

• Po pierwsze, wspólne hasła są rzadko zmieniane ze względu na liczbę osób, które muszą być koordynowane. Im dłużej hasło pozostaje niezmienione, tym dłużej haker może używać hasła, jeśli je złamał.

• Po drugie, ponieważ „wszyscy znają” wspólne hasło, użytkownicy prawdopodobnie rozdadzą je swobodnie osobom, które nie powinny go mieć.

• Po trzecie, co najważniejsze, jeśli konto jest używane niewłaściwie, niemożliwe będzie stwierdzenie na podstawie dzienników kontroli, który członek grupy popełnił atak, ponieważ jakikolwiek członek grupy mógł popełnić naruszenie.

Ogólnie rzecz biorąc, firmy powinny mieć jasne zasady, które zabraniają współdzielonych kont. Wszystkie systemy operacyjne i bezpieczne aplikacje umożliwiają administratorom systemów tworzenie grup z listy indywidualnych kont. Jeśli administrator systemu przydzieli grupie uprawnienia dostępu, konta poszczególnych członków grupy automatycznie dziedziczą te uprawnienia. Osoby te mogą następnie zalogować się przy użyciu własnych nazw kont i haseł. W ten sposób nie dochodzi do utraty indywidualnej tożsamości podczas logowania i kolejnych audytów.

WYŁĄCZANIE HASŁA, KTÓRE NIE SĄ WAŻNE

Wiele kont i haseł w korporacjach jest nieodpowiednich, ponieważ (1) osoba odeszła z firmy, (2) osoba ma inne stanowisko w firmie lub (3) konto było tymczasowe dla kontrahenta. International Data Corporation oszacowała, że od 30 do 60 procent wszystkich rachunków w dużych korporacjach jest nieodpowiednich. Powinny istnieć silne zasady i skuteczne procedury wyłączania kont, które stają się nieodpowiednie.

Niestety, aktualizowanie kont jest trudne. Podczas gdy do utworzenia kont prawie zawsze potrzebne są specjalne działania, jeśli nie zostaną podjęte żadne działania, konta normalnie nadal istnieją. Chociaż systemy zarządzania tożsamością obejmujące całą firmę, omówione w dalszej części tego rozdziału, mogą anulować wszystkie konta, gdy ktoś odejdzie w firmie zwykle nie ma podobnych zabezpieczeń, gdy ktoś odchodzi z zespołu projektowego lub zajmuje inne stanowisko w firmie. Jedną z opcji jest przypisanie kogoś jako właściciela logicznych grup rachunków i wymaganie od tej osoby częstego potwierdzania przydatności rachunków. Mogą być przynajmniej zobowiązani do przejrzenia list kont, które nie były ostatnio używane.

UTRACONE HASŁA

Utracone hasła powodują mniej więcej jedną czwartą do jednej trzeciej4 wszystkich wezwań do pomocy technicznej. Dlatego obsługa utraconych haseł jest dużym problemem. Jednocześnie zajmowanie się zgubionymi hasłami jest niebezpieczne.

Resetowanie hasła. Pracownicy help desku nie mogą odczytać istniejących haseł, ale zwykle mają możliwość utworzenia nowego hasła do konta. Ta akcja nazywa się, nie do końca dokładnie, resetowaniem hasła. Zwykle to hasło jest tymczasowe. Przy następnym logowaniu użytkownik musi zmienić hasło.

Niebezpieczeństwo „zagubionego hasła”

Ataki socjotechniczne. Głównym zagrożeniem związanym z socjotechniką jest to, że atakujący zadzwoni do działu pomocy, podając się za właściciela konta, i poprosi o zresetowanie hasła, zwykle wyrażając pilną potrzebę i autorytet. Pracownik pomocy technicznej Aharried może ulec presji i zresetować hasło do konta. Następnie atakujący skutecznie kontrolowałby konto. Ponadto właściwy właściciel konta zostałby zablokowany. Kolejny atak socjotechniczny mający na celu uzyskanie hasła użytkownika ma miejsce, gdy atakujący dzwoni do właściwego właściciela konta przez telefon. Atakujący twierdzi, że jest administratorem i potrzebuje pomocy użytkownika. Atakujący po prostu prosi użytkownika o podanie hasła, twierdząc, że jest to część audytu. Jeśli użytkownik złapie i odmówi ujawnienia hasła, osoba atakująca będzie twierdzić, że użytkownik pomyślnie przeszedł audyt. Istnieje wiele wariacji na ten temat i są one niestety dość skuteczne.

Automatyczne resetowanie hasła. Resetowanie hasła jest bardzo drogie. Na przykład firma WellPoint otrzymywała 14 000 telefonów każdego miesiąca od pracowników, którzy zgubili swoje hasła.5 Koszty pracy działu pomocy technicznej związane z resetem wynosiły co najmniej 25 USD i mogły sięgać nawet 200 USD, jeśli pracownik miał dostęp do wielu systemów. Aby obniżyć koszty resetowania haseł, WellPoint i wiele firm korzysta teraz z automatycznych systemów resetowania haseł. Aby skorzystać z takiego systemu, pracownik loguje się do systemu resetowania hasła i wpisuje nazwę swojego konta. Następnie pyta się go „Gdzie się urodziłeś?” lub inne pytanie, na które pracownik odpowiedział, gdy po raz pierwszy otrzymał konto. Jeśli pracownik odpowie poprawnie, może utworzyć nowe hasło do konta. Chociaż pomysł jest prosty, trudno jest stworzyć dobre pytania dotyczące resetowania hasła, na które ludzie będą odpowiadać.

• Niektóre pytania same w sobie stanowią naruszenie bezpieczeństwa. Na przykład niektóre pytania dotyczą poufnych informacji, takich jak numer ubezpieczenia społecznego lub nazwisko panieńskie matki (które nadal wykorzystuje wiele banków do identyfikacji osób).

• Na niektóre pytania może odpowiedzieć napastnik, który przeprowadził małe rozeznanie, np. „W jakim mieście się urodziłeś?" lub „Jak ma na imię twój zwierzak?"

• W przypadku niektórych pytań badany nie będzie w stanie zapamiętać odpowiedzi. Na przykład w pytaniu „Kto był twoim ulubionym nauczycielem w liceum?" zapamiętanie pierwotnie udzielonej odpowiedzi może być trudne dla kogoś, kto miał kilku ulubionych nauczycieli w liceum.

• W przypadku niektórych pytań problem z pisownią może stanowić problem, na przykład „Jak miał na imię twój ulubiony nauczyciel w szkole średniej?"

Ogólnie rzecz biorąc, dobrze jest zadać kilka rozsądnych pytań, które nie proszą o podanie poufnych informacji i na które nie można uzyskać odpowiedzi poprzez badanie partii, a następnie poprosić osobę o wybranie jednego lub więcej pytań, na które ma odpowiedzieć.

W wiadomościach

We wrześniu 2008 r. haker o imieniu „Rubico" użył funkcji resetowania hasła, aby uzyskać dostęp do prywatnego konta pocztowego Yahoo! kandydatki na wiceprezydenta Sarah Palin. Rubico był w rzeczywistości studentem na Uniwersytecie Tennessee o nazwisku David Kernell. Kernell wykorzystała adres e-mail Palin, datę urodzenia, kod pocztowy i miejsce, w którym poznała swojego męża - Wasillę High-, aby zresetować hasło Palin i uzyskać dostęp do jej konta e-mail. Kernell próbował użyć usługi proxy do zatarcia swoich śladów. Jednak dostawca proxy przekazał FBI wszystkie niezbędne informacje w dzienniku, a Kernell został zidentyfikowany jako główny podejrzany. Kernell został skazany 30 kwietnia 2010 r. za przewidywane utrudnianie wymiaru sprawiedliwości poprzez niszczenie akt i nieautoryzowany dostęp do komputera. Kernell został skazany na rok i jeden dzień aresztu oraz trzy lata w zawieszeniu.

Czy resetowanie hasła jest bezpieczne? Chociaż resetowanie haseł jest faktem w życiu firmy, stanowi poważne zagrożenie bezpieczeństwa. Łańcuch zabezpieczeń jest tak silny, jak jego najsłabsze ogniwo, a resetowanie hasła jest potencjalnie najsłabszym ogniwem w używaniu haseł – zwłaszcza samoobsługowego resetowania hasła. Jednym z kontrowersyjnych sposobów na zwiększenie bezpieczeństwa haseł jest całkowite wyeliminowanie samoobsługowego resetowania haseł w przypadku kont o wyższym poziomie bezpieczeństwa. Zwiększy to koszty pomocy technicznej, ale zmniejszenie ryzyka może być dobrze uzasadnione. W rzeczywistości w przypadku kont wysokiego ryzyka resetowanie hasła do pomocy technicznej przez telefon może być zabronione. Jeśli zgubisz kod PIN do bankomatu, zazwyczaj musisz udać się do oddziału banku i okazać dowód tożsamości przed otrzymaniem nowego kodu PIN. Ponadto być może będziesz musiał poczekać kilka dni, aż centrala banku zatwierdzi zmieniony kod PIN. Wygoda jest dobra, ale może być konieczne ograniczenie resetowania hasła, gdy zagrożenia bezpieczeństwa są wysokie.

TEST CXIV

a. Dlaczego używanie tego samego hasła w wielu witrynach jest problemem?

b. Dlaczego trudno jest wymusić politykę używania innego hasła w każdej witrynie?

c. Dlaczego zasady dotyczące czasu trwania hasła są ważne?

d. Co to jest resetowanie hasła?

e. Dlaczego resetowanie hasła jest niebezpieczne?

f. Jak można zautomatyzować resetowanie hasła?

g. Dlaczego tworzenie pytań dotyczących resetowania hasła jest trudne?

h. Jak można postępować z resetowaniem hasła w środowiskach wysokiego ryzyka?

SIŁA HASŁA

Dla korporacji ważne jest, aby miały zasady, które wymagają silnych haseł. Na przykład zasady firmy mogą wymagać, aby hasła miały następującą długość i złożoność:

• Mieć co najmniej osiem znaków.

• Miej co najmniej jedną zmianę przypadku, nie na początku hasła.

• Mieć co najmniej jedną cyfrę (od 0 do 9), nie na końcu hasła.

• Mieć co najmniej jeden znak niealfanumeryczny, nie na końcu hasła.

Przykładem hasła, które pasuje do wszystkich tych zasad, jest tri6#Vial. Ma dziewięć znaków. Chociaż używa głównie małych liter, pękanie metodą brute-force nie będzie działać z powodu cyfry (6), specjalnego symbolu (#) i dużej litery (V). Przydatne może być również tworzenie haseł z długich fraz ze złożonymi kombinacjami znaków. Na przykład „W 1492 r. Kolumb żeglował po błękitnym oceanie" może podać hasło „i1492, Cstob" (jeśli dozwolony jest przecinek).

KONTROLA HASŁA

Nazwy użytkowników i hasła są głównym celem hakerów. Wszystkie hasła muszą być przechowywane przy użyciu bezpiecznego algorytmu haszującego i regularnie testowane, aby upewnić się, że nie można ich łatwo złamać. Ważne jest, aby zawsze uzyskać pozwolenie przed uruchomieniem programu do łamania haseł na komputerach firmy. Podczas gdy systemy operacyjne automatycznie mieszają i przechowują hasło, aplikacje internetowe i witryny handlu elektronicznego tego nie robią. Na przykład w 2009 r. hakerzy wykorzystali dobrze znaną lukę w zabezpieczeniach SQL do kradzieży 32 milionów haseł z serwisu RockYou.com. RockYou przechowywał wszystkie nazwy użytkowników, hasła i dane partnerów w przejrzysty sposób. RockYou wysyłał użytkownikom hasła w postaci zwykłego tekstu za pośrednictwem poczty e-mail. Poniższa tabela przedstawia statystyki dla dwudziestu najczęściej używanych haseł dla trzech różnych stron internetowych, w tym RockYou. Gawker Media utraciło informacje o około 748 502 kontach użytkowników z zaszyfrowanymi hasłami. Hotmail stracił 9 843 nazw użytkowników i haseł w wyniku podejrzenia o phishing10. W każdym przypadku nazwy użytkowników i hasła zostały skradzione, a następnie udostępnione publicznie. Konta użytkowników ze wspólnymi hasłami stanowiły znaczną liczbę wszystkich kont. W rozdziale 7 omówimy bardziej szczegółowo, jak zabezpieczyć hosta przed tymi atakami, tworząc silne hasła, skróty i odpowiednio je testując. Wyjaśni również, jak działa proces łamania haseł. Ogólnie rzecz biorąc, bezpieczniej jest założyć, że dane konta hasła Twojej firmy zostaną skradzione i podjąć środki zapobiegawcze. Regularna kontrola haseł może uniemożliwić atakującym łatwe złamanie skradzionych skrótów haseł.

TEST CXV

a. Jakie są zalecane zasady dotyczące długości i złożoności haseł w tekście?

b. W jaki sposób można wykorzystać programy do łamania haseł do egzekwowania polityki siły haseł?

c. Co należy zrobić przed uruchomieniem programu do łamania haseł na komputerach firmy w celu sprawdzenia słabych haseł?

Koniec haseł?

Chociaż hasła są szeroko stosowane, wśród specjalistów ds. bezpieczeństwa panuje prawie całkowita zgoda, że hasła nie są już bezpieczne. Rosnąca moc komputerów sprawiła, że proste hasła można tak szybko złamać, że bezpieczne są tylko najdłuższe i najbardziej złożone hasła. Jednak gdy użytkownicy są zmuszeni do używania bardzo długich i skomplikowanych haseł, zwykle zapisują je lub obchodzą ich siłę w inny sposób. Hasła prawdopodobnie zostaną wycofane w dość niedalekiej przyszłości. Wiele firm już w dużej mierze je wycofało, a wiele innych wkrótce to zrobi. Zaczniemy teraz przyglądać się alternatywnym technologiom uwierzytelniania, które mogą być używane przez firmy w świecie post-hasła.

TEST CXVI

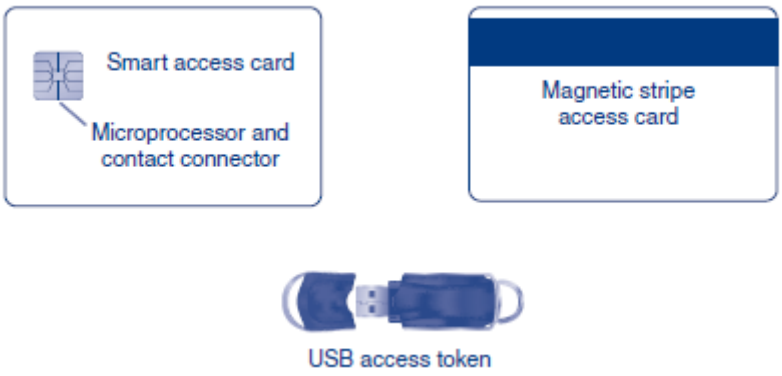
Jaka jest prawdopodobna przyszłość haseł?

KARTY DOSTĘPU I TOKENY

Jednym ze sposobów zastąpienia haseł wielokrotnego użytku jest noszenie małych urządzeń fizycznych w celu ich uwierzytelnienia. Te fizyczne urządzenia zazwyczaj dzielą się na dwie kategorie – karty dostępu i tokeny.

Karty dostępu

Rysunek pokazuje, że karta dostępu to plastikowa karta, która zwykle ma rozmiar karty kredytowej lub debetowej. Zwykle osoba, która chce uzyskać dostęp do drzwi lub komputera, wsuwa kartę dostępu przez czytnik lub wkłada ją do czytnika. To jest dokładnie to, co robisz, gdy używasz karty kredytowej lub debetowej w sklepie detalicznym.



KARTY Z PASKIEM MAGNETYCZNYM

Najprostsze karty dostępu wykorzystują paski magnetyczne, takie jak te na kartach kredytowych. Paski magnetyczne mogą przechowywać dane uwierzytelniające o osobie. Jeśli niedawno podróżowałeś, wiesz, że karty z paskiem magnetycznym są często używane do uzyskania dostępu do pokoju hotelowego.

KARTY INTELIGENTNE

Karta inteligentna wygląda jak karta z paskiem magnetycznym, ale ma wbudowany mikroprocesor i pamięć. Dzięki temu karty inteligentne mogą wykonywać przetwarzanie w celu bardziej zaawansowanego uwierzytelniania. Na przykład może wykonać szyfrowanie kluczem publicznym w celu uwierzytelniania typu wyzwanie/odpowiedź, szyfrując wiadomość wyzwania za pomocą klucza prywatnego użytkownika. Karty inteligentne mogą również podawać informacje w różny sposób do różnych aplikacji. Podczas gdy karty z paskiem magnetycznym są pasywne, zawierają tylko dane, karty inteligentne są aktywne.

KOSZTY CZYTNIKA KART

Problemem zarówno w przypadku kart dostępu z paskiem magnetycznym, jak i kart dostępu do kart inteligentnych jest koszt i dostępność czytników kart. Chociaż pojedyncze czytniki nie są drogie, instalacja wielu z nich jest łącznie bardzo kosztowna. Ponadto, jeśli ktoś potrzebuje skorzystać z komputera, który nie ma czytnika kart, nie może tego zrobić, jeśli uwierzytelnianie karty dostępu jest obowiązkowe.

Tokeny

Aby zagrać na automacie, wkładasz żeton do slotu na monety. Żeton reprezentuje monetę. Ogólnie rzecz biorąc, token to coś, co reprezentuje coś innego. Token uwierzytelniający reprezentuje osobę, która chce zostać uwierzytelniona. Token to coś, co reprezentuje coś innego. Token uwierzytelniający reprezentuje osobę, która chce zostać uwierzytelniona.

TOKENY JEDNORAZOWYCH HASEŁ

Token z jednorazowym hasłem to niewielkie urządzenie z wyświetlaczem, na którym często zmienia się liczba. Użytkownicy muszą wpisać aktualny numer do zamków kluczy lub do swoich komputerów. Korzystanie z hasła jednorazowego pozwala uniknąć konieczności używania haseł wielokrotnego użytku, które, jak widzieliśmy wcześniej, często są łatwe do pokonania.

Tokeny USB

Token AUSB to po prostu małe urządzenie, które podłącza się do portu USB komputera w celu identyfikacji właściciela. Tokeny USB zapewniają wiele zabezpieczeń kart inteligentnych bez konieczności zakupu czytnika kart inteligentnych na każdym komputerze.

Tokeny dostępu zbliżeniowego

Problemem zarówno z kartami dostępowymi, jak i tokenami USB jest konieczność fizycznego kontaktu z czytnikiem lub portem USB. Nową alternatywą jest token zbliżeniowy, który zawiera mały znacznik identyfikatora częstotliwości radiowej (RFID). Gdy petent zbliża się do komputera lub drzwi, nadajnik radiowy przy komputerze lub drzwiach wysyła sygnał radiowy. Moc tego sygnału radiowego jest częściowo pochłaniana przez tag RFID, który wykorzystuje tę moc do przesyłania informacji identyfikacyjnych zawartych w tagu. Z tokenem zbliżeniowym osoba może po prostu podejść do komputera lub drzwi i zostać wpuszczona.

Rozwiązanie problemu utraty i kradzieży

Chociaż urządzenia dostępu fizycznego mogą zwiększyć bezpieczeństwo, należy nimi zarządzać ostrożnie ze względu na ich częste zgubienie i kradzież. Znalazca lub złodziej może być w stanie użyć urządzenia dostępowego, aby uzyskać nieautoryzowany dostęp.

ANULOWANIE URZĄDZENIA FIZYCZNEGO

Jedną z odpowiedzi na kradzież i utratę jest wyłączenie zhakowanych urządzeń. Na przykład w hotelach, jeśli zgubisz kartę dostępu do pokoju, pracownik recepcji wyłączy dostęp starej karty do wszystkich zamków. Pracownik przekaże Ci wtedy nową kartę do Twojego pokoju. Nowa karta będzie miała nowy kod dostępu. Anulowanie wymaga zainstalowania okablowania z centrum bezpieczeństwa do poszczególnych urządzeń weryfikacyjnych. Jednak utrata urządzeń dostępowych jest tak powszechna, że aktywne radzenie sobie z utraconymi urządzeniami dostępowymi jest obowiązkowe. (Zabezpieczenia urządzenia dostępowego zwykle wymagają również połączeń w celu rejestrowania zdarzeń dostępu do celów audytu). Jak szybkie musi być anulowanie? Jest to kwestia analizy ryzyka, która równoważy koszt szybszego anulowania z kosztem włamań, które mogą mieć miejsce w czasie przed anulowaniem.

UWIERZYTELNIANIE DWUCZYNNIKOWE

Uwierzytelnianie dwuskładnikowe, które pokrótce omówiliśmy wcześniej, wymaga użycia dwóch różnych metod uwierzytelniania. Urządzenie dostępowe byłoby tylko jedną z tych metod. Jak zauważono na początku tego rozdziału, uwierzytelnianie dwuskładnikowe ma ograniczenia, ale nadal jest przydatne w wielu przypadkach.

Kody PIN. Niektóre firmy wymagają od pracowników wpisywania osobistych numerów identyfikacyjnych (PIN) podczas korzystania z fizycznych urządzeń dostępowych. Zazwyczaj te kody PIN mają tylko cztery do sześciu cyfr. Hasła muszą być długie, ponieważ osoby atakujące mogą przeprowadzać miliony porównań na sekundę. Jednak ludzie muszą wprowadzać kody PIN ręcznie, więc atakujący mogą wprowadzać kod PIN tylko co sekundę lub dwie. Ponadto osoba stojąca nad drzwiami dostępowymi i próbująca wielu kodów PIN byłaby bardzo widoczna, a zatem podatna na wykrycie. Mimo to firma powinna zakazać łatwych do odgadnięcia kodów PIN, takich jak 1111, 2222, 1234, ostatnich czterech cyfr numeru ubezpieczenia społecznego użytkownika lub ważnej daty osobistej w formacie miesiąc/dzień, takiej jak urodziny lub rocznica ślubu wnioskodawcy. Firmy powinny agresywnie zabronić zapisywania PIN-u na karcie lub w portfelu, którym dana osoba ma przy sobie kartę. Takie praktyki negują zalety uwierzytelniania dwuskładnikowego.

Inne formy uwierzytelniania dwuskładnikowego.

Istnieje wiele innych sposobów uwierzytelniania dwuskładnikowego. Na przykład karta inteligentna może zawierać odcisk palca właściciela urządzenia dostępowego. Osoba korzystająca z fizycznego urządzenia dostępowego musiałaby również przesunąć palcem po skanerze linii papilarnych, aby sprawdzić, czy jest uprawnionym użytkownikiem urządzenia.

TEST CXVII

a. Rozróżnij karty z paskiem magnetycznym i karty inteligentne.

b. Co to są tokeny z jednorazowym hasłem?

Cc. Czym są tokeny USB?

d. Jaka jest przewaga tokenów USB w porównaniu z kartami?

e. Jaka jest atrakcyjność tokenów zbliżeniowych?

a. Dlaczego ważne jest, aby wyłączyć zgubione lub skradzione urządzenia dostępowe?

b. Podaj przykład uwierzytelniania dwuskładnikowego, o którym nie wspomniano w tekście.

c. Co to jest PIN?

d. Dlaczego kody PIN mogą być krótkie — tylko cztery do sześciu cyfr — podczas gdy hasła muszą być znacznie dłuższe?

UWIERZYTELNIANIE BIOMETRYCZNE

Biometria

Zapominamy hasła. Tracimy karty dostępu. Jednak pomimo żartów o zostawieniu głowy w domu, zawsze zabieramy ze sobą nasze ciała. Umożliwia to uwierzytelnianie biometryczne, które opiera się na pomiarach biologicznych (bio) (metrykach). Uwierzytelnianie biometryczne opiera się na tym, czym jesteś (odcisk palca, wzór tęczówki, twarz, geometria dłoni itp.) lub na czymś, co robisz (pisanie, pisanie, chodzenie itp.). Główną obietnicą biometrii jest uczynienie przestarzałych haseł wielokrotnego użytku.

Główną obietnicą biometrii jest uczynienie przestarzałych haseł wielokrotnego użytku.

TEST CXVIII

a. Co to jest uwierzytelnianie biometryczne?

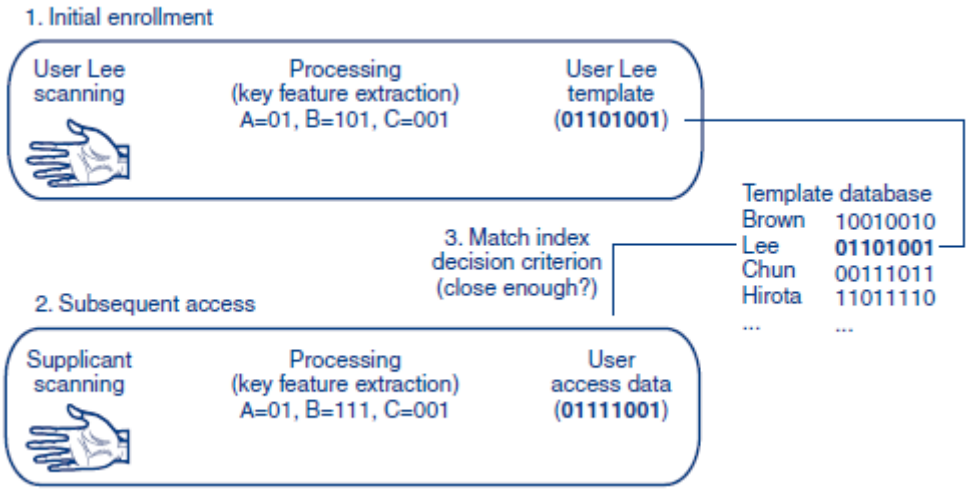
b. Na jakich dwóch rzeczach w tobie opiera się uwierzytelnianie biometryczne?

c. Jaka jest główna obietnica biometrii?

Systemy biometryczne

ZAPISY WSTĘPNE

Rysunek przedstawia biometryczny system uwierzytelniania. Każdy użytkownik musi najpierw zostać zarejestrowany w systemie.



Rejestracja składa się z trzech etapów:

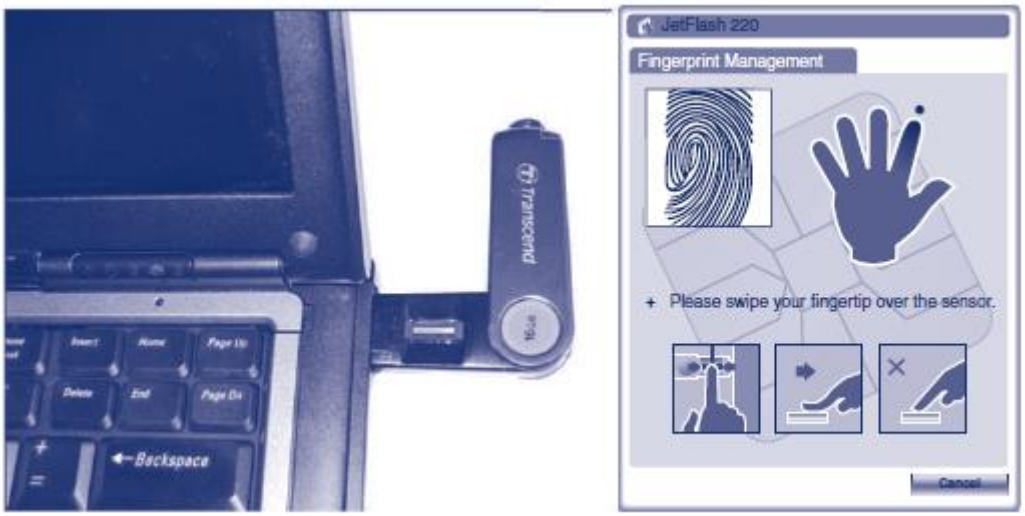
• Krok 1 Czytnik skanuje dane biometryczne każdej osoby. To skanowanie rejestracji tworzy zbyt dużo danych do wykorzystania. Ponadto dane skanowania będą się różnić za każdym razem, gdy użytkownik będzie skanowany.

• Krok 2 Czytnik przetwarza następnie zeskanowane dane rejestracji, aby wyodrębnić kilka kluczowych cech z masy zeskanowanych danych. Tych kilka kluczowych funkcji, a nie cały zestaw zeskanowanych danych, zostanie w przyszłości wykorzystanych do identyfikacji lub weryfikacji użytkownika.

• Krok 3 Czytnik w końcu wysyła dane kluczowej cechy do bazy danych, która przechowuje dane kluczowej cechy jako szablon użytkownika.

Dlaczego nie użyć całych skanów zamiast kluczowych funkcji? Problem polega na tym, że całe skany nie są zbyt przydatne w postaci surowej. Jeśli dana osoba przesuwa palcem pod różnymi kątami, surowe pliki skanów będą bardzo różne, ale kluczowe cechy, takie jak względne położenie pętli, łuków i zwojów w odciskach palców, będą takie same lub prawie takie same bez względu na to, jak palec jest skanowany.

Rysunek przedstawia proces rejestracji czytnika linii papilarnych w Transcend JetFlash.



Proces jest przyjazny dla użytkownika i zajmuje około trzech minut. Aby zakończyć proces, użytkownik musi czterokrotnie przesunąć ten sam palec i wprowadzić hasło.

KOLEJNE PRÓBY DOSTĘPU

Gdy użytkownicy później chcą zostać uwierzytelnieni, są ponownie skanowani. Czytelnik przetwarza te informacje ze skanowania suplikanta, aby stworzyć kluczowe funkcje. Te kluczowe cechy stają się danymi dostępowymi użytkownika. System centralny dopasowuje dane dostępowe użytkownika do szablonu osoby w bazie danych.

AKCEPTACJA LUB ODRZUCENIE

Gdy system otrzymuje dane dostępowe, oblicza indeks dopasowania, który jest różnicą między kluczowymi funkcjami skanowania a szablonem. Nigdy nie ma idealnego dopasowania, ponieważ skanowanie nigdy nie działa dwa razy dokładnie w ten sam sposób. Jeśli błąd jest mniejszy niż wartość zwana kryterium decyzyjnym, kandydat jest akceptowany jako dopasowanie. Jeśli nie, wnioskodawca jest odrzucany jako dopasowanie.

TEST CXIX

a. Opisz trzy akcje skanera w procesie rejestracji.

b. Jakie są kluczowe cechy?

c. Dlaczego są konieczne?

d. Co serwer robi z kluczowymi funkcjami utworzonymi przez skanowanie rejestracji?

e. Co to jest szablon?

f. Co to są dane dostępowe użytkownika?

g. Co to są wskaźniki dopasowania i jak są powiązane z kryteriami decyzyjnymi?

Błędy biometryczne

Kontrola dostępu wymaga dużej dokładności. Niestety pojawia się wiele pytań dotyczących wiarygodności różnych rodzajów uwierzytelniania biometrycznego. Jedną z kwestii jest poziom błędu, który odnosi się do dokładności, gdy petent nie próbuje oszukać systemu. Inną kwestią dotyczącą dokładności jest wskaźnik oszustw, czyli prawdopodobieństwo, że oszust będzie w stanie oszukać system, jeśli spróbuje. Na razie skupimy się na wskaźnikach błędów.

Uwaga: Poniższy materiał jest trudny do opanowania, ponieważ istnieje kilka powiązanych pojęć, które łatwo pomylić. Zwolnij podczas studiowania tej części i porównuj to, co czytasz, z tym, co już przeczytałeś.

FAŁSZYWY STOPIEŃ AKCEPTACJI

Akceptacja oznacza dopasowanie osoby do określonego szablonu. Jak właśnie widzieliśmy, fałszywa akceptacja to dopasowanie do szablonu, którego nie należy robić. Wskaźnik fałszywych akceptacji jako procent wszystkich prób dostępu nazywa się fałszywą akceptacją stawki (FAR). Akceptacja oznacza dopasowanie osoby do określonego szablonu. Fałszywa akceptacja to dopasowanie do szablonu, którego nie należy wykonywać. Fałszywe akceptacje mają różne implikacje dla różnych zastosowań, na przykład w dostępie do drzwi lub komputera w porównaniu z listami obserwacyjnymi terrorystów.

• W przypadku dostępu do komputera lub drzwi fałszywa akceptacja oznacza, że oszust jest dopasowany do legalnego szablonu i tym samym otrzymuje dostęp. W konsekwencji oszust może dostać się do środka (nawet bez próby oszustwa). To poważne naruszenie bezpieczeństwa.

• W przypadku dopasowywania terrorystów do listy obserwacyjnej, fałszywa akceptacja oznacza nieprawidłowe dopasowanie osoby do listy, innymi słowy, nieprawidłowe etykietowanie niewinnej osoby jako terrorysty. Będzie to niedogodnością dla osoby błędnie dopasowanej, ale nie jest to awaria bezpieczeństwa. Jeśli jednak jest zbyt wiele fałszywych akceptacji, reklamacje mogą wymusić wyłączenie systemu.

• Z kolei w przypadku dostępu na liście obserwacyjnej do pomieszczenia ze sprzętem fałszywe akceptacje stanowią problem z bezpieczeństwem, podczas gdy fałszywe odrzucenia są jedynie niewygodne. Wskaźnik fałszywych akceptacji jako procent wszystkich prób dostępu nazywany jest wskaźnikiem fałszywych akceptacji (FAR).

FAŁSZYWY STOPIEŃ ODRZUCENIA

W przypadku fałszywego odrzucenia z kolei wnioskodawca jest błędnie odrzucany jako dopasowanie do wzorca, podczas gdy wnioskodawca powinien zostać zaakceptowany jako dopasowanie. Współczynnik fałszywych odrzuceń (FRR) jest więc prawdopodobieństwem, że system odrzuci osobę, która powinna być dopasowana do szablonu. Współczynnik fałszywych odrzuceń (FRR) to prawdopodobieństwo, że system odrzuci osobę, która powinna być dopasowana do szablonu. Należy

zauważyć, że fałszywe odrzucenia, takie jak fałszywe akceptacje, mają różne konsekwencje dla różnych zastosowań dostępu do drzwi lub komputera w porównaniu z listami obserwacyjnymi terrorystów.

• Na przykład w przypadku dostępu do komputera fałszywe odrzucenie oznacza odmowę dostępu uprawnionemu użytkownikowi. Chociaż niekoniecznie jest to złe z punktu widzenia bezpieczeństwa, wysoki FRR dla dostępu do komputera lub drzwi może prowadzić do dużego niezadowolenia użytkownika, a to może zabić system.

• W przypadku list obserwacyjnych fałszywe odrzucenie oznacza, że osoba, która powinna zostać zidentyfikowana jako znajdująca się na liście obserwacyjnej, nie znajduje się na liście obserwacyjnej. Jeśli jest to lista obserwowanych terrorystów, oznacza to, że terrorysta pozostaje niezidentyfikowany. To poważne naruszenie bezpieczeństwa. Jeśli jest to lista obserwacyjna dostępu do drzwi do pomieszczenia ze sprzętem, to jest to tylko niedogodność

CO JEST GORSZE?

Co jest zatem gorsze - fałszywa akceptacja czy fałszywe odrzucenie? To zależy od kontekstu. W przypadku dostępu do drzwi lub serwera fałszywa akceptacja umożliwia atakującemu wejście i stanowi poważne naruszenie. Fałszywe odrzucenie to po prostu niedogodność. Jednak w przypadku dopasowywania listy obserwacyjnej terrorystów fałszywe odrzucenie (niedopasowanie atakującego do szablonu listy obserwacyjnej) jest poważnym naruszeniem bezpieczeństwa. Z kolei fałszywa akceptacja to tylko uciążliwość

ROSZCZENIA DOSTAWCY

Niestety twierdzenia dostawców dotyczące FAR i FRR mogą być mylące. Zwykle opierają się na wyidealizowanych sytuacjach, które nie są reprezentatywne dla rzeczywistych warunków. Na przykład widzieliśmy, że współczynnik fałszywej akceptacji wzrasta wraz ze wzrostem liczby szablonów, ponieważ istnieje małe prawdopodobieństwo fałszywej akceptacji dla każdego szablonu. Aby to wykorzystać, dostawcy mogą opierać szacunki FAR na bazach danych zawierających tylko kilka szablonów. Ponadto dostawcy rejestrują użytkowników w idealnych okolicznościach i mają idealne sytuacje do próby uzyskania dostępu. Na przykład w rozpoznawaniu twarzy osoby testowane mogą być bardzo dobrze oświetlone i wyczekiwać zarówno rejestracji, jak i prób dostępu – warunków, które prawdopodobnie nie wystąpią w prawdziwym świecie. Może to spowodować, że zgłoszony przez dostawcę odsetek fałszywych odrzuceń będzie niższy niż w praktyce.

NIEPOWODZENIE ZAPISU

Jest inny rodzaj błędu, niepowodzenie rejestracji (FTE). Dzieje się tak, jeśli system nie zarejestruje użytkownika. Na przykład w przypadku uwierzytelniania odcisków palców niektórzy ludzie nie mają dobrze zdefiniowanych odcisków palców z powodu wieku, lat pracy budowlanej, długiej obsługi dokumentów biurowych lub z innych powodów. W niektórych przypadkach może to sprawić, że system uwierzytelniania odcisków palców będzie bezużyteczny.

TEST CXX

a. Czym jest dopasowanie w biometrii?

b. Rozróżnij fałszywe akceptacje i fałszywe odrzucenia.

c. Czym są współczynniki fałszywych akceptacji (FAR) i współczynniki fałszywych odrzuceń (FRR)?

d. W przypadku dostępu do komputera, dlaczego fałszywa akceptacja jest zła?

e. Dlaczego fałszywe odrzucenie jest złe?

f. Co jest gorsze z punktu widzenia bezpieczeństwa?

g. Co jest gorsze z punktu widzenia akceptacji użytkownika?

a. Czym jest fałszywa akceptacja w przypadku list obserwacyjnych przestępców?

b. W przypadku list obserwacyjnych przestępców, co jest gorsze z punktu widzenia bezpieczeństwa, fałszywa akceptacja czy fałszywe odrzucenie? Wyjaśniać.

c. Na listach obserwacyjnych osób, którym należy wpuścić do pokoju, co jest gorsze z punktu widzenia bezpieczeństwa, fałszywa akceptacja czy fałszywe odrzucenie? Wyjaśniać.

Czym jest brak rejestracji?

Listy weryfikacyjne, identyfikacyjne i obserwacyjne

WERYFIKACJA

Uwierzytelnianie biometryczne ma jeden z trzech możliwych celów. W trakcie weryfikacji, petent twierdzi, że jest konkretną osobą, a wyzwaniem jest zmierzenie biometrycznych danych dostępowych petenta względem szablonu osoby, za którą się podaje. Kiedy logujesz się na serwer za pomocą nazwy użytkownika i hasła, jest to weryfikacja.

Podczas weryfikacji weryfikator ustala, czy petent jest konkretną osobą.

Za każdym razem, gdy próbuje się dopasować, istnieje niebezpieczeństwo fałszywego dopasowania, co oznacza, że dane szablonu mogą pasować do danych dostępowych wnioskodawcy, gdy nie powinno być dopasowania. To niebezpieczeństwo jest zwykle niewielkie, a ponieważ weryfikacja dopasowuje dane dostępowe tylko do jednego szablonu, istnieje tylko jedna szansa na fałszywe dopasowanie. Na przykład, jeśli prawdopodobieństwo fałszywej akceptacji wynosi jeden do tysiąca, to prawdopodobieństwo fałszywej akceptacji wynosi jeden do tysiąca, ponieważ podjęto tylko jedną próbę dopasowania. Wskaźnik fałszywej akceptacji (FAR) wynosi 0,1 procent.

IDENTYFIKACJA

Natomiast przy identyfikacji, petent nie twierdzi, że jest konkretną osobą. Zadaniem systemu jest identyfikacja petenta, czyli ustalenie, kim on jest.

Podczas identyfikacji weryfikator określa tożsamość wnioskodawcy.

Podczas identyfikacji biometryczne dane dostępowe wnioskodawcy muszą być dopasowane do szablonów wszystkich osób, których szablon jest przechowywany w systemie. Jeśli system nie znajdzie dopasowań, odrzuca petenta.

Podczas identyfikacji system dokonuje wielu dopasowań między dostępem wnioskodawcy i szablonem w systemie. Z każdym dopasowaniem istnieje niewielkie niebezpieczeństwo fałszywego dopasowania (fałszywa akceptacja). Biorąc pod uwagę wiele dopasowań wymaganych w porównaniu do identyfikacji przy pojedynczym dopasowaniu wymaganym podczas weryfikacji szansa na fałszywe dopasowanie jest dużo wyższe w identyfikacji niż w weryfikacji.

Załóżmy na przykład, że prawdopodobieństwo fałszywego dopasowania na szablon wynosi 1/1000. Załóżmy również, że w bazie danych jest 500 szablonów. Wtedy będzie 500 prób dopasowania, a FAR wyniesie 1/1000 razy 500, czyli 50 procent. To jest 500 razy fałszywy wskaźnik akceptacji do weryfikacji.

Z drugiej strony identyfikacja uwalnia użytkowników od konieczności wpisywania swoich nazwisk lub nazw kont. Identyfikacja jest najlepsza w przypadku kontroli dostępu do drzwi i innych sytuacji w których tożsamości nie może złożyć wnioskodawca.

LISTY OBSERWACJI

Ograniczoną, ale coraz ważniejszą formą identyfikacji jest lista obserwacyjna, która identyfikuje osobę jako członka grupy. Na przykład dopasowania mogą być wykonane na podstawie szablonów osób znajdujących się na liście obserwacyjnej terrorystów. Lub, dopasowania mogą być wykonane przeciwko członkom zespołu naprawczego, którzy powinni mieć możliwość wejścia do pomieszczenia. Dopasowanie listy obserwowanych zapewnia więcej porównań danych dostępowych z szablonami niż weryfikacja i dlatego jest bardziej podatny na fałszywe akceptacje. Jednak dopasowanie listy obserwowanych sprawia, że mniej porównań niż pełna identyfikacja, dzięki czemu jest mniej podatny na fałszywe akceptacje.

TEST CXXI

a. Rozróżnij weryfikację i identyfikację.

b. Co wymaga więcej dopasowań do szablonów?

c. Co jest bardziej prawdopodobne, aby wygenerować fałszywą akceptację? Czemu?

d. Porównaj identyfikację z dopasowaniem do listy obserwacyjnej.

e. Co jest bardziej prawdopodobne, aby wygenerować fałszywe dopasowanie? Czemu?

a. Załóżmy, że prawdopodobieństwo fałszywej akceptacji wynosi jeden na milion, w bazie danych znajduje się 10 000 tożsamości oraz że istnieje lista obserwacyjna obejmująca 100 osób. Jaki będzie FAR do weryfikacji?

b. Do identyfikacji?

c. Do listy obserwacyjnej?

Oszustwo biometryczne

Chociaż błędy są poważnym problemem, oszustwo jest jeszcze bardziej kłopotliwe. System biometryczny o niskim poziomie błędów jest bezużyteczny, jeśli można go skutecznie oszukać przy rozsądnym wysiłku. W oszustwie atakujący celowo próbuje oszukać system. Na przykład, wiele skanerów linii papilarnych może zostać oszukanych, jeśli przeciwnik podniesie ukryty (obecny, ale niewidoczny) odcisk palca ze szkła, umieści go na żelatynowym palcu i umieści fałszywy palec na skanerze linii papilarnych.

W oszustwie atakujący celowo próbuje oszukać system.

W dopasowaniu listy obserwacyjnej z systemem kamer monitorujących na lotnisku napastnik może wejść na lotnisko, trzymać głowę opuszczoną i nosić kapelusz z rondem, aby oszukać algorytm dopasowujący. Wskaźniki oszustw biometrycznych w świecie rzeczywistym są w dużej mierze nieznane, z wyjątkiem skanerów linii papilarnych, w przypadku których oszustwa często działają przy użyciu nieskomplikowanych metod. Na szczęście dla wielu aktywów oszustwo nie jest kwestią krytyczną. Na przykład zwykła osoba bez poufnych informacji na komputerze przenośnym prawdopodobnie nie spotka się z wyrafinowanym napastnikiem. W przypadku notebooków bez poufnych informacji, czytniki linii papilarnych istnieją głównie po to, by eliminować hasła, które są zbyt słabe i zbyt często zapisywane przez użytkowników.

TEST CXXII

a. Rozróżnij wskaźniki błędów i oszustwa w biometrii.

b. Dlaczego skanowanie linii papilarnych, które jest często oszukiwane, może być dopuszczalne do wprowadzenia do szafki na materiały eksploatacyjne?

c. Kiedy to może nie wystarczyć?

Metody biometryczne

ROZPOZNAWANIE ODCISKÓW PALCÓW

Dzięki filmom kryminalnym prawie każdy zna rozpoznawanie odcisków palców. Technologia rozpoznawania odcisków palców jest dobrze rozwinięta i niedroga. Skanery linii papilarnych są na tyle tanie, że można je dodać do komputerów, a nawet małych urządzeń przenośnych. Ze względu na niski koszt skanery linii papilarnych stanowią większość całego rynku biometrycznego. Niestety, technologię rozpoznawania odcisków palców często łatwo oszukać. W 2002 roku naukowcy byli w stanie pokonać 80 procent systemów rozpoznawania odcisków palców, tworząc żelatynowy palec z ukrytego odcisku (tj. niewidocznego odcisku pozostawionego na szkle lub innym przedmiocie). Czytniki linii papilarnych, które mogą lepiej wykrywać oszustwa, wykorzystują takie pomiary, jak pomiar pojemności skóry, a nawet częstości tętna. Jednak tego typu czytniki linii papilarnych są drogie i dlatego są rzadziej stosowane. Biorąc pod uwagę, że skanery linii papilarnych można oszukać, zauważyliśmy, że powinny być używane tylko w zastosowaniach, w których istnieje niewielkie ryzyko poważnego oszustwa. Przykładem może być zalogowanie się do komputera osobistego, który nie zawiera poufnych informacji.

ROZPOZNAWANIE TĘCZÓWKI

Tęczówka to kolorowa część twojego oka. Irysy są znacznie bardziej złożone i indywidualne niż odciski palców. W rzeczywistości rozpoznawanie tęczówki jest najdokładniejszą formą uwierzytelniania biometrycznego z bardzo niskimi wartościami FAR. Ogólnie rzecz biorąc, skanowanie tęczówki oka jest dziś złotym standardem w uwierzytelnianiu biometrycznym. Niestety, podobnie jak złoto, jest drogi.

Skanery tęczówki mogą odczytywać wzory tęczówki z odległości kilku centymetrów do metra. W filmach skanowanie tęczówki jest zwykle pokazywane jako czerwona wiązka laserowa świecąca w oko petenta. To kompletna bzdura. Dzięki skanerom tęczówki ludzie po prostu patrzą w zwykłe kamery. Zazwyczaj istnieje mały monitor telewizyjny, który pomaga petentowi upewnić się, że patrzy bezpośrednio w kamerę.

ROZPOZNAWANIE TWARZY

Rysy twarzy można odczytać z odległości kilku metrów. Dzięki temu rozpoznawanie twarzy jest przydatne do kontroli dostępu do drzwi. Jednak rozpoznawanie twarzy jest bardzo czułe na różnice w oświetleniu między skanowanym obrazem zapisanym na komputerze a sytuacją, w której skan jest wykonywany. Jest również umiarkowanie wrażliwy na zmiany w rysach twarzy, takie jak zarost, i często jest bardzo wrażliwy na oszustwa ze strony ludzi odwracających twarze od aparatu. Jedyną istotną zaletą rozpoznawania twarzy jest to, że można go używać potajemnie, to znaczy bez wiedzy osoby badanej. To sprawia, że wydaje się to dobre dla kamer monitorujących szukających przestępców i terrorystów. Jednak jego wysoki poziom błędów i łatwość, z jaką można go oszukać, sprawiają, że jest wysoce podejrzany w przypadku list obserwacyjnych przestępców i terrorystów.

GEOMETRIA DŁONI

Geometria ludzkiej dłoni, w tym długość i szerokość palca, szerokość dłoni i inne cechy, jest dość łatwa do zmierzenia i jest używana głównie w kontroli dostępu do drzwi ze względu na rozmiar skanerów geometrii dłoni. Użytkownik po prostu kładzie rękę na skanerze wielkości podręcznika.

ROZPOZNAWANIE GŁOSU

Odciski palców, tęczówka, twarz, geometria dłoni i rozpoznawanie żył to przykłady tego, czym jesteś. Natomiast rozpoznawanie głosu opiera się na czymś, co robisz, a mianowicie mówieniu. Niestety rozpoznawanie głosu jest łatwo oszukane przez nagrania. Ponadto wysokie wskaźniki fałszywych odrzuceń sprawiają, że rozpoznawanie głosu jest frustrujące dla użytkowników.

INNE FORMY UWIERZYTELNIANIA BIOMETRYCZNEGO

Istnieje wiele innych form uwierzytelniania biometrycznego – rozpoznawanie żył w dłoni, rozpoznawanie naciśnięć klawiszy (wpisywanie tempa między poziomami), rozpoznawanie podpisów pisemnych i rozpoznawanie chodu (sposób chodzenia), żeby wymienić tylko kilka. Jednak geometria odcisków palców, tęczówki, twarzy i dłoni są obecnie najczęściej używanymi rodzajami uwierzytelniania biometrycznego, a rozpoznawanie odcisków palców jest dominujące.

TEST CXXIII

a. Jaka jest zaleta rozpoznawania odcisków palców?

b. Jakie są wady?

c. Do jakiego rodzaju zastosowania wystarczy rozpoznawanie odcisków palców?

D. Jaka jest zaleta rozpoznawania tęczówki?

e. Jakie są wady?

f. Czy skanowanie tęczówki wystrzeliwuje światło w twoje oko?

a. Jaka jest zaleta rozpoznawania twarzy?

b. Co znaczy potajemny?

c. Gdzie jest używane rozpoznawanie geometrii dłoni?

d. Jakie są wady rozpoznawania głosu?

e. Jakie są najczęściej używane formy uwierzytelniania biometrycznego?

f. Jaka jest najczęściej stosowana forma biometrii?

UWIERZYTELNIANIE KRYPTOGRAFICZNE

W Części 3 przyjrzeliśmy się uwierzytelnianiu kryptograficznemu w kontekście systemów kryptograficznych. Uwierzytelnianie kryptograficzne to złoty standard uwierzytelniania. Jest to najbezpieczniejsza forma uwierzytelniania, jeśli zostanie prawidłowo zaimplementowana. Podobnie jak złoto, jest to również najdroższa forma uwierzytelniania. Rozdział 3 zawiera kilka kluczowych punktów:

• W systemach kryptograficznych istnieją dwie formy uwierzytelniania – uwierzytelnianie początkowe na początku dialogów oraz uwierzytelnianie wiadomość po wiadomości z podpisami elektronicznymi dla wszystkich wiadomości w dialogu.

• Przyjrzeliśmy się MS-CHAP pod kątem początkowego uwierzytelniania przy użyciu haseł.

• Następnie przyjrzeliśmy się dwóm formom podpisów elektronicznych. Kody uwierzytelniania wiadomości z haszowanym kluczem (HMAC) są szybkie i niedrogie, ale brakuje im niezaprzeczalności.

• Podpisy cyfrowe wykorzystują szyfrowanie kluczem publicznym i certyfikaty cyfrowe, aby zapewnić niezwykle silne, ale powolne uwierzytelnianie.

• Chociaż w rozdziale 3 tego nie omówiono, uwierzytelnianie kluczem publicznym za pomocą certyfikatów cyfrowych jest również przydatne do wstępnego uwierzytelniania.

Infrastruktury klucza publicznego

Korzystanie z uwierzytelniania klucza publicznego za pomocą certyfikatów cyfrowych wymaga od organizacji ustanowienia infrastruktury klucza publicznego (PKI) w celu tworzenia i zarządzania parami klucz publiczny-prywatny oraz certyfikatami cyfrowymi. Rysunek 5-18 ilustruje funkcje PKI.

FIRMA JAKO JEDNOSTKA CERTYFIKUJĄCA

Jak zauważono w Części 3, urzędy certyfikacji (CA) zarządzają certyfikatami cyfrowymi. W rozdziale zauważono również, że CA nie są regulowane, a to rodzi pytania o zaufanie. Jeśli jednak firmy działają jako własne CA, mają kontrolę nad zaufaniem do całej swojej infrastruktury klucza publicznego. Z drugiej strony bycie urzędem certyfikacji jest dość drogie ze względu na wymaganą pracę.

TWORZENIE PARY KLUCZ PUBLICZNY-KLUCZ PRYWATNY

Po pierwsze, PKI potrzebuje sposobu na generowanie par klucz publiczny-prywatny dla serwerów i klientów innych niż PKI. Zwykle robi to klient lub serwer inny niż PKI, a nie serwer PKI. Klient lub serwer generuje parę klucz prywatny-klucz publiczny, a następnie wysyła klucz publiczny do urzędu certyfikacji. Ta transmisja może być wykonana jawnie, ponieważ klucze publiczne nie są tajne. Klucz prywatny, który jest tajny, w ogóle nie jest przesyłany.

DYSTRYBUCJA CERTYFIKATÓW CYFROWYCH

Oczywiście infrastruktura PKI musi być w stanie dystrybuować klucze publiczne w certyfikatach cyfrowych.

AKCEPTACJA CERTYFIKATÓW CYFROWYCH

Może się to wydawać podejrzane, ale pamiętaj, że certyfikaty cyfrowe mają własne podpisy cyfrowe podpisane (zaszyfrowane) kluczem prywatnym serwera PKI. Podpisy cyfrowe zapewniają integralność wiadomości oraz uwierzytelnianie. W konsekwencji oszust nie może zmienić nazwy prawdziwej partii i zastąpić jej własnym imieniem.

Przyjęcie certyfikatu cyfrowego od petenta jest bezpieczne, nawet jeśli petent jest oszustem. Certyfikat cyfrowy posiada własny podpis cyfrowy, który zapewnia integralność. Oznacza to, że nadawca nie może go zmienić.

STAN COFNIĘCIA CERTYFIKATU

Jak omówiono w Części 3, certyfikaty cyfrowe mogą zostać unieważnione przed datą wygaśnięcia wskazaną w certyfikacie cyfrowym. W związku z tym serwery PKI muszą obsługiwać pobieranie list odwołania certyfikatów (CRL) i odpowiadać na zapytania protokołu OCSP (Online Certificate Status Protocol).

APROWIZACJA

Skupiamy się na technologii PKI. Jeszcze droższe są koszty pracy związane z udostępnianiem — akceptacją kluczy publicznych i dostarczaniem użytkownikom nowych certyfikatów cyfrowych.

Na drugim końcu cyklu życia certyfikatu cyfrowego pracownicy muszą mieć dobre procedury terminacji certyfikatów cyfrowych, a przełożeni pracowników i dział kadr muszą również prawidłowo i rzetelnie obsługiwać terminację certyfikatów cyfrowych.

PROBLEM UWIERZYTELNIANIA PRIME

Chociaż technologia może być bardzo skuteczna, dobra technologia nic nie znaczy, jeśli cały system nie jest dobrze zarządzany. Muszą istnieć silne procedury, które muszą być egzekwowane i kontrolowane. Najpoważniejszym problemem jest podstawowy problem z uwierzytelnianiem, który mówi, że dopóki osoby nie zostaną dokładnie sprawdzone przed dopuszczeniem do systemu, oszuści mogą po prostu zapisać się poprzez socjotechnikę. Udostępnianie jest najbardziej ryzykownym aspektem infrastruktury klucza publicznego, ponieważ jeśli oszust może nakłonić personel PKI do zarejestrowania go, wszystkie zabezpieczenia techniczne są automatycznie omijane. Muszą istnieć silne procedury określające, kto może zgłosić kogoś do włączenia, kto może to zatwierdzić (zawsze ktoś inny), jaka identyfikacja jest wymagana i jak postępować z wyjątkami. Procedury te muszą być starannie egzekwowane i kontrolowane.

TEST CXXIV

a. Jaka jest najsilniejsza forma uwierzytelniania?

b. Wymień funkcje infrastruktury PKI.

c. Czy firma może być własnym urzędem certyfikacji?

d Jaka jest z tego korzyść?

e. Kto tworzy parę klucz prywatny-klucz publiczny komputera?

f. Jak urzędy certyfikacji rozpowszechniają klucze publiczne?

g. Co to jest aprowizacja?

h. Jaki jest główny problem z uwierzytelnianiem?

i. Co można zrobić, aby zmniejszyć to ryzyko?

ZEZWOLENIE

Kontrola dostępu składa się z trzech elementów, które nazwaliśmy uwierzytelnianiem AAA, autoryzacją i audytem. Do tej pory przyglądaliśmy się tylko uwierzytelnianiu. Jednak znajomość tożsamości partnera komunikacji nie wystarczy. Należy również zdefiniować konkretne uprawnienia (uprawnienia) strony komunikującej się. Nie każdy, kto jest uwierzytelniony, może robić cokolwiek zechce w każdym katalogu. (Aby podać analogię, prawdopodobnie nie pozwoliłbyś niektórym osobom, które znasz, aby prowadziły Twój samochód).

Zasada najmniejszych uprawnień

W uprawnieniach planistycznych ważne jest przestrzeganie zasady najmniejszych uprawnień. Oznacza to, że każda osoba powinna uzyskać tylko te uprawnienia, których bezwzględnie potrzebuje do wykonywania swojej pracy. Jeśli początkowe przypisanie uprawnień jest zbyt wąskie, w razie potrzeby można przyznać dodatkowe uprawnienia. Zasada najmniejszych uprawnień polega na tym, że każda osoba powinna uzyskać tylko te uprawnienia, których bezwzględnie potrzebuje do wykonywania

swojej pracy. Aby podać przykład, załóżmy, że system ma uprawnienia A, B, C, D, E i F, a dana osoba potrzebuje uprawnień A, C i E. Załóżmy, że osobie przyznano tylko te uprawnienia, których potrzebuje. Wtedy osoba otrzyma A, C i E. A co jeśli popełni błąd i osoba otrzyma tylko A i C? Odpowiedź brzmi, że E można dodać później. Osoba będzie niedogodności do czasu dostarczenia E, ale bezpieczeństwo nie zostanie naruszone. Przypisanie najmniejszych uprawnień oznacza, że system ma tendencję do bezpiecznej awarii, nie dając każdemu użytkownikowi zbyt wielu uprawnień w przypadku popełnienia błędu. Odwrotnym podejściem jest nadanie każdemu użytkownikowi albo pełnych uprawnień, albo szerokich uprawnień. W ten sposób użytkownik zawsze lub prawie zawsze będzie miał uprawnienia, których potrzebuje do wykonywania swojej pracy. Możliwe jest wówczas odebranie uprawnień, których użytkownik nie potrzebuje. Jednak bardzo łatwo zapomnieć o cofnięciu pozwolenia, które pozwala użytkownikowi na podjęcie działań powodujących poważne szkody. Kontynuując poprzedni przykład, załóżmy, że dana osoba otrzymuje uprawnienia od A do F, a B i D są odbierane. Tutaj popełniono błąd. Uprawnienie F nie zostało usunięte. Dopóki błąd nie zostanie wykryty i naprawiony, osoba będzie miała uprawnienia F i może być w stanie podejmować działania sprzeczne z bezpieczeństwem. To jest naruszenie bezpieczeństwa. Po prostu zaczynając od najmniejszych uprawnień, a następnie dodając uprawnienia, ponieważ potrzebne, rzadko będą powodować problemy z bezpieczeństwem. Jednak rozpoczynanie od rozległych uprawnień, a następnie ich zmniejszanie, ma znacznie większą szansę na stworzenie poważnych problemów z bezpieczeństwem.

TEST CXXV

a. Dlaczego autoryzacje są potrzebne po uwierzytelnieniu osoby?

b. Jaka jest inna nazwa autoryzacji?

c. Jaka jest zasada najmniejszych uprawnień?

d. Dlaczego jest to dobry sposób na przypisanie początkowych uprawnień?

e. Co jest złego w przypisywaniu wszystkich uprawnień, a następnie odbieraniu uprawnień, których użytkownik nie potrzebuje?

f. Co oznacza bezpieczna awaria w systemie bezpieczeństwa?

AUDYT

Trzecie A w AAA to audyt. Pierwsze A, uwierzytelnienie, identyfikuje osobę lub program. Drugie A, autoryzacje, określa, co ta osoba lub program może robić. Wreszcie audyt rejestruje i analizuje, co faktycznie zrobiła osoba lub program. Jeśli czynności związane z uwierzytelnianiem i autoryzacją nie są często kontrolowane, niewłaściwe zachowanie może trwać bardzo długo.

Zezwolenia określają, co ta osoba lub program może robić. Rejestry audytu i analizy tego, co faktycznie zrobiła osoba lub program;

Logowanie

Kamery bezpieczeństwa rejestrują wizualne obrazy tego, co robią ludzie. W podobny sposób rejestrowanie rejestruje akcje, które właściciel konta podejmuje na zasobie. Aby podać tylko kilka przykładów, system rejestrowania serwera może gromadzić dane o takich zdarzeniach, jak udane logowanie, nieudane logowanie, usuwanie plików, tworzenie plików, drukowanie plików i tak dalej. Informacje te są przechowywane w pliku dziennika wraz z tożsamością osoby lub procesu, który podjął działanie. Później administrator systemu może odczytać plik dziennika, aby wyszukać podejrzane wzorce lub dowiedzieć się, kto popełnił czyn, którego nie powinien.

Odczytywanie dziennika

Dopóki logi nie są badane, są bezużyteczne. Pliki dziennika stają się formą „pamięci tylko do zapisu". Niestety odczytanie logów jest trudne i czasochłonne. W konsekwencji są często ignorowane.

REGULARNY ODCZYT DZIENNIKA

Ważne jest, aby regularnie czytać pliki dziennika. W zależności od wrażliwości zdarzeń, które rejestruje plik, może to oznaczać codziennie lub nawet kilka razy dziennie.

OKRESOWE AUDYTY ZEWNĘTRZNE WPISÓW PLIKU LOGÓW

Oprócz regularnego czytania pliki dziennika powinny być okresowo sprawdzane zewnętrznie. Audyt zewnętrzny sprawdza losowo wybrane wpisy w dzienniku i określa, czy odczyt dziennika został wykonany prawidłowo.

AUTOMATYCZNE ALERTY

Czytanie plików dziennika mówi tylko o przeszłości. W idealnym przypadku systemy rejestrowania powinny mieć aktywne funkcje odczytu dzienników, które wysyłają do administratora zabezpieczeń alerty w czasie rzeczywistym o określonych typach zdarzeń.

TEST CXXVI

a. Co to jest audyt?

b. Dlaczego jest to konieczne?

c. Dlaczego czytanie dzienników jest ważne?

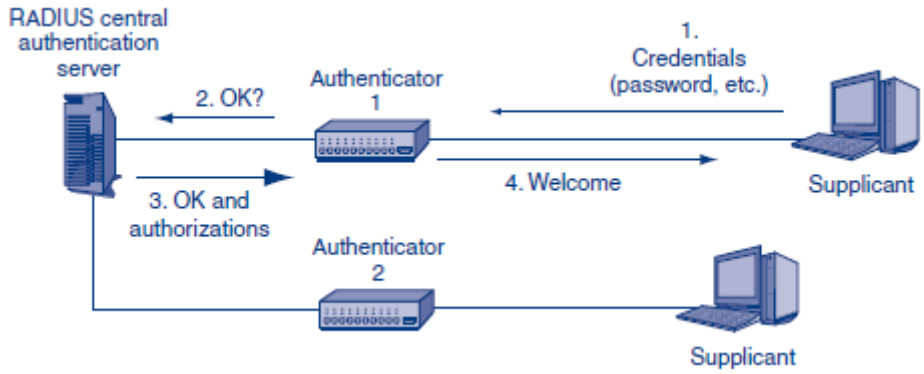
d. Jakie są trzy rodzaje działań, które należy wykonać na dziennikach?

e. Dlaczego pożądane są automatyczne alerty?

CENTRALNE SERWERY UWIERZYTELNIANIA

Potrzeba scentralizowanego uwierzytelniania

Większość firm ma setki lub tysiące serwerów. Poszczególni pracownicy mogą potrzebować dostępu i autoryzacji dla kilkunastu lub więcej serwerów. Firmy zaspokajają tę potrzebę, korzystając z centralnych serwerów uwierzytelniania. Centralne serwery uwierzytelniania obniżają koszty, zapewniają spójność uwierzytelniania bez względu na to, gdzie użytkownik lub atakujący wchodzi do sieci i umożliwiają natychmiastowe wprowadzanie zmian w całej firmie. Najczęściej stosowanym standardem dla centralnych serwerów uwierzytelniających jest RADIUS. Rysunek przedstawia podstawowe elementy centralnego uwierzytelniania RADIUS.



Gdy używany jest centralny serwer uwierzytelniający, urządzenie, z którym łączy się suplikant, nazywane jest uwierzytelniającym. Gdy suplikant wysyła poświadczenia do dowolnego podmiotu uwierzytelniającego, uwierzytelniający przekazuje je do centralnego serwera uwierzytelniania. Serwer uwierzytelniania sprawdza poświadczenia i wysyła wiadomość z powrotem do wystawcy uwierzytelnienia. Ten komunikat informuje osobę uwierzytelniającą, czy poświadczenia suplikanta zostały zweryfikowane. Na podstawie tych informacji osoba uwierzytelniająca albo przyjąć lub odrzucić petenta.

TEST CXXVII

a. Jakie są trzy urządzenia w centralnym uwierzytelnianiu przy użyciu serwerów RADIUS?

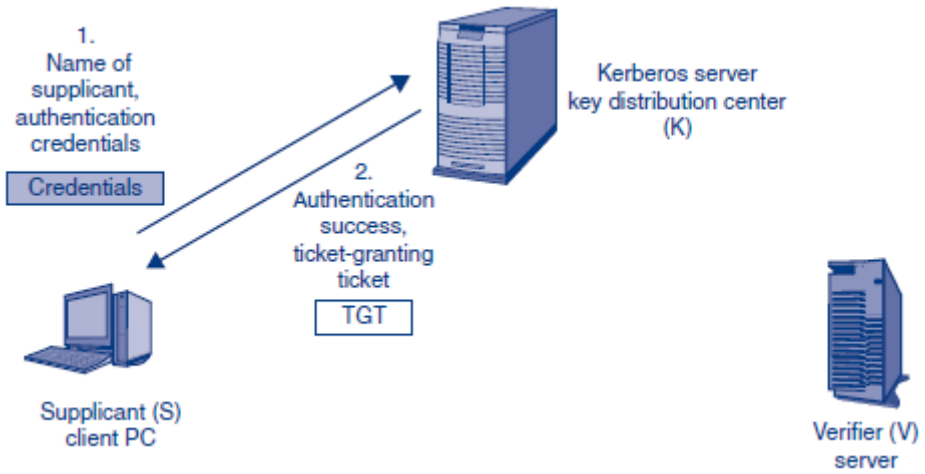
b. Jaka jest rola uwierzytelniającego?

c. Jaka jest rola centralnego serwera uwierzytelniania?

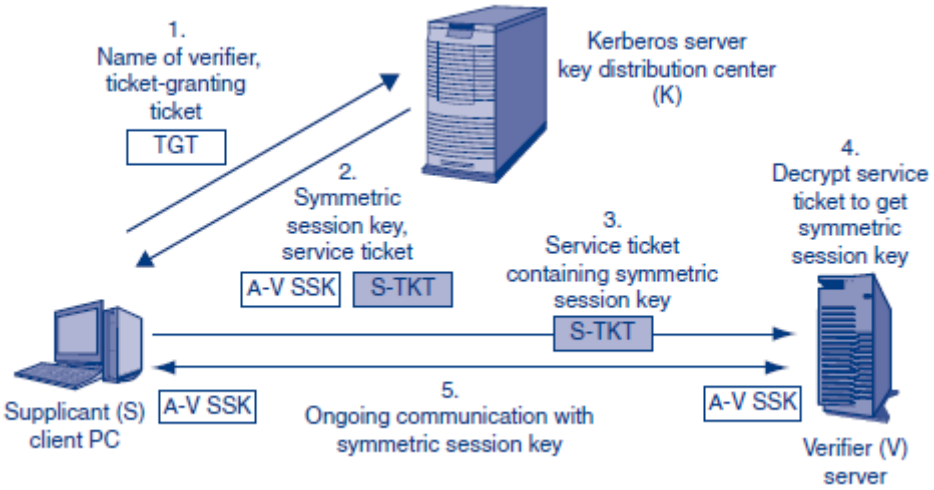
Kerberos

Chociaż RADIUS jest prawdopodobnie najpopularniejszym standardem centralnego serwera uwierzytelniającego, Kerberos16 jest również ważny, w dużej mierze dlatego, że Microsoft używa go do łączenia hostów, jak zobaczymy w następnej sekcji. W rzeczywistości Kerberos to coś więcej niż centralny serwer uwierzytelniania. Dostarcza również informacje o kluczu stronom, które muszą się ze sobą komunikować, a także może dostarczać informacje dotyczące autoryzacji. (RADIUS również może to zrobić.)

Rysunek pokazuje, że gdy host chce połączyć się z innym hostem, najpierw loguje się do serwera Kerberos.



Jeśli uda mu się zalogować, otrzymuje bilet przyznania biletu (TGT). To jak zdobycie bransoletki na nadgarstek, gdy wchodzisz na koncert lub wydarzenie sportowe. Dzięki temu wrócisz później bez konieczności pokazywania oryginalnych poświadczeń uwierzytelniających. Następnie uwierzytelniony suplikant (S) chce skomunikować się z hostem weryfikatora (V). Rysunek pokazuje, że S łączy się z serwerem Kerberos.



W tym procesie S wysyła swój bilet przyznający bilet do serwera Kerberos, aby udowodnić, że został już uwierzytelniony. Jeśli serwer Kerberos zezwala na połączenie z weryfikatorem, wysyła bilet usługi do S, który wysyła bilet usługi do V. Weryfikator ma klucz symetryczny, który udostępnia tylko serwerowi Kerberos. Używa tego wspólnego klucza do odszyfrowania biletu usługi wysłanego przez serwer Kerberos. Odszyfrowany bilet do usługi zawiera klucz sesji, którego S używa do komunikacji z V. Może również zawierać listę uprawnień, które S powinien mieć na V.

Gdy serwer Kerberos wysyła bilet usługi do S, wysyła również klucz sesji z V zaszyfrowanym kluczem, który współużytkują tylko suplikant i serwer Kerberos. S używa tego współdzielonego klucza do odszyfrowania symetrycznego klucza sesji za pomocą V. Teraz, gdy oba hosty mają ten sam symetryczny klucz sesji, mogą zacząć komunikować się tam iz powrotem, szyfrując swoją transmisję w celu zachowania poufności za pomocą klucza sesji. Jeśli śledziłeś to uważnie, niewątpliwie pytasz: „Hej, skąd V wie, że S nie jest oszustem?” Odpowiedź jest taka, że jeśli inny host, powiedzmy X, przechwyci bilet usługi i wyśle go do V, X nie będzie znał symetrycznego klucza sesji. Nie będzie w stanie komunikować się z V za pomocą tego klucza. W konsekwencji nie ma potrzeby wyraźnego informowania V, że S jest uwierzytelniony i ma uprawnienia do konwersacji. V po prostu zachowuje się tak, jakby tak było, a jeśli tak nie jest, komunikacja się zepsuje. Innymi słowy słowa, system zawodzi bezpiecznie.

TEST XXVIII

a. W Kerberos należy rozróżnić między biletem przyznającym bilet a biletem usługi.

b. Jakie informacje daje bilet serwisowy weryfikatorowi?

c. W jaki sposób petent otrzymuje symetryczny klucz sesji?

d. Czy weryfikator został wyraźnie powiadomiony, że wnioskodawca został uwierzytelniony? Wyjaśnij.

SERWERY KATALOGOWE

RADIUS, Kerberos i inne centralne serwery uwierzytelniania usprawniają centralizację, ale w większości dużych firm pozostają dwa problemy.

• Po pierwsze, większość dużych firm korzysta z wielu serwerów RADIUS, Kerberos i innych centralnych serwerów uwierzytelniania.

• Ponadto większość dużych firm podjęła strategiczną decyzję o wykorzystaniu serwerów katalogowych jako miejsca centralnego przechowywania danych w firmie.

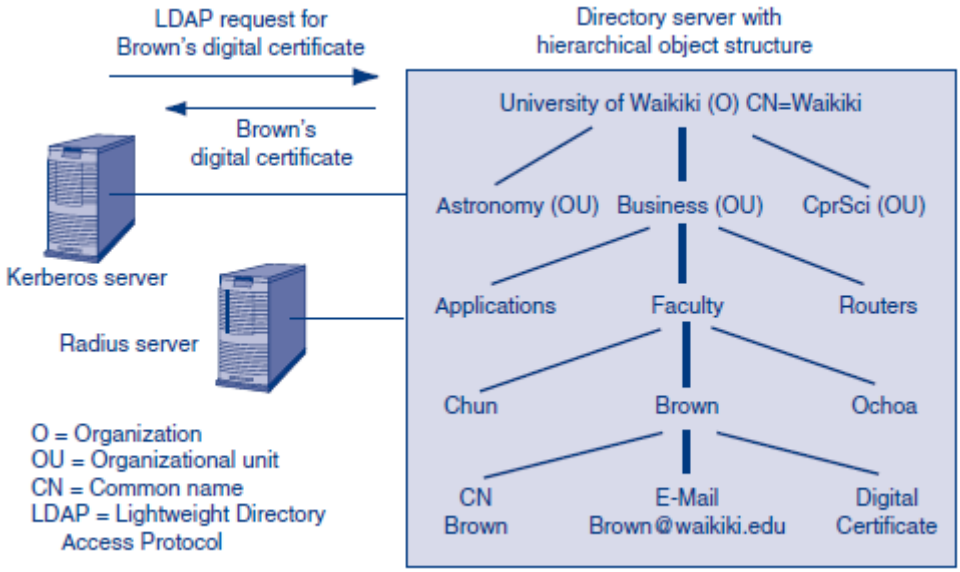
Co to są serwery katalogowe?

Serwery katalogowe to centralne repozytoria informacji o ludziach, sprzęcie, oprogramowaniu i bazach danych. Serwery katalogowe przechowują informacje dotyczące uwierzytelniania, autoryzacji i inspekcji wymagane do zapewnienia bezpieczeństwa. Jednak serwery katalogowe nie ograniczają się do informacji o zabezpieczeniach. Przechowują informacje o konfiguracjach hostów, informacje kontaktowe pracowników, takie jak numery telefonów, oraz wiele ogólnych informacji.

Informacje o zabezpieczeniach to tylko jeden aspekt informacji o serwerze katalogowym.

Hierarchiczna organizacja danych

Kursy bazodanowe zwykle koncentrują się na relacyjnych bazach danych. Relacyjne bazy danych są dobre, gdy liczba dostępów i aktualizacji jest równa. Jeśli jednak dostępów jest znacznie więcej niż aktualizacji, jak w przypadku serwerów katalogowych, hierarchiczna organizacja bazy danych może być lepsza. Jak ilustruje Rysunek, serwery katalogowe wykorzystują hierarchiczną organizację bazy danych.



Schemat bazy danych serwera katalogów jest hierarchiczną kolekcją obiektów (węzłów).

• Obiektem najwyższego poziomu jest organizacja (O). To jest nazwa organizacji. Na rysunku jest to Uniwersytet Waikiki. Nazwa zwyczajowa (CN) to skrótowy sposób odwoływania się do tego węzła.

• Poniżej poziomu organizacji znajduje się kilka obiektów jednostek organizacyjnych (OU). Na rysunku trzy jednostki organizacyjne to astronomia, biznes i informatyka. Prawdopodobnie istnieje kilka innych jednostek organizacyjnych, których nie pokazano na rysunku. Zazwyczaj zarządzanie danymi OU jest przynajmniej częściowo delegowane do jednostki organizacyjnej.

• W strukturze hierarchicznej może występować kilka poziomów jednostek organizacyjnych, ale ten serwer katalogowy ma tylko jeden poziom jednostki organizacyjnej.

• Następny poziom składa się z większej liczby węzłów. W tym przypadku węzły to aplikacje, członkowie wydziału i routery. Podkreśla to, że serwery katalogowe nie ograniczają się do informacji o ludziach.

• Pod wydziałem znajduje się wiele obiektów ludzi. Jeden z nich jest dla Browna. Brown ma podwęzły dla nazwy pospolitej (Charlene Brown), adresu e-mail i certyfikatu cyfrowego.

TEST CXXIX

a. Jak zorganizowane są informacje na serwerach katalogowych?

b. Jakie są dwa najwyższe poziomy organizacji?

c. Czy serwery katalogowe przechowują tylko informacje o osobach?

Lekki protokół dostępu do danych

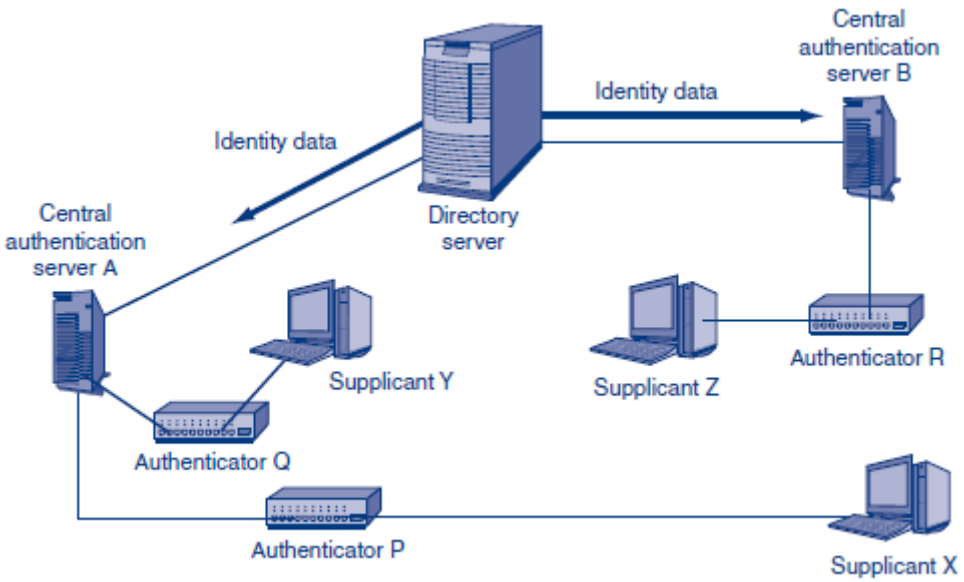
Serwery uwierzytelniania komunikują się z serwerami katalogowymi za pomocą protokołu LDAP (Lightweight Directory Access Protocol). W większości przypadków protokół LDAP służy do pobierania danych z serwera katalogów. Można go jednak również użyć do aktualizacji informacji na serwerze katalogowym. Prawie wszystkie serwery katalogowe obsługują protokół LDAP. Należy zauważyć, że protokół LDAP nie reguluje wewnętrznych operacji komunikacji tylko serwera katalogów między serwerami katalogów a innymi urządzeniami, w tym serwerami uwierzytelniania.

TEST CXXX

Jaki jest cel LDAP?

Użycie przez serwery uwierzytelniające

Z punktu widzenia bezpieczeństwa serwery katalogowe są ważne, ponieważ są używane przez centralne serwery uwierzytelniania, takie jak serwery RADIUS i serwery Kerberos. Rysunek pokazuje, że serwer katalogowy może dostarczyć informacje uwierzytelniające do wielu serwerów uwierzytelniających.



Tak jak serwery uwierzytelniania są cenne, ponieważ centralizują informacje dotyczące uwierzytelniania, katalogi zapewniają wyższy poziom centralizacji firmom, które mają wiele centralnych serwerów uwierzytelniania.

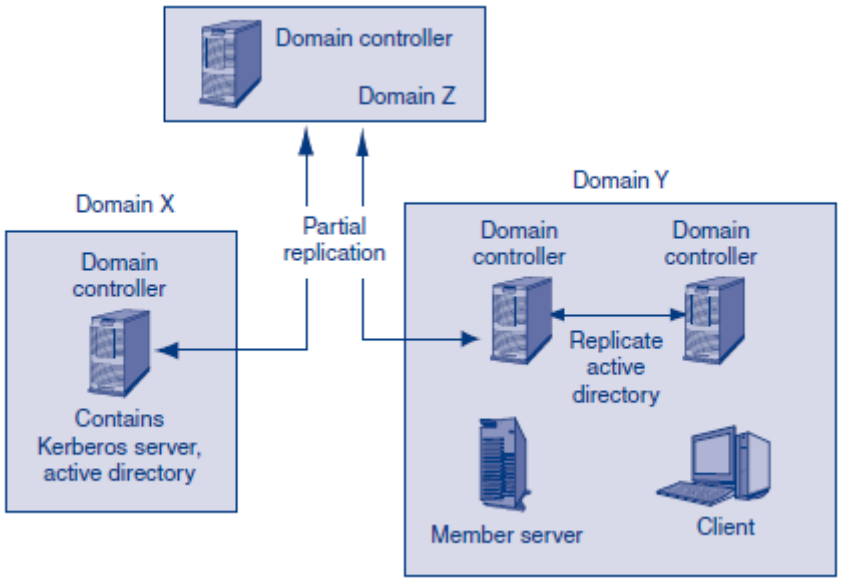
CXXXI

a. W jaki sposób centralne serwery uwierzytelniające często uzyskują informacje uwierzytelniające?

b. Jaka jest z tego korzyść?

Active Directory

Produkt serwera katalogowego firmy Microsoft nazywa się Active Directory (AD). Biorąc pod uwagę powszechne stosowanie produktów firmy Microsoft w korporacjach, specjaliści ds. bezpieczeństwa powinni rozumieć AD. Rysunek przedstawia firmę z kilkoma serwerami Active Directory.



DOMENY ACTIVE DIRECTORY

Jak pokazuje powyższy rysunek, firmy zwykle dzielą swoje zasoby na wiele domen Active Directory. Domeny AD to zazwyczaj jednostki organizacyjne. Na przykład na uniwersytecie domeną może być pojedyncza szkoła lub kolegium. Zasobami domeny zazwyczaj zarządza jednostka organizacyjna. Domeny AD mogą odpowiadać domenom DNS, ale nie muszą.

Kontrolery domeny.

Na rysunku Domena X ma jeden serwer kontrolera domeny, który kontroluje zasoby w domenie. Kontroler domeny ma zarówno bazę danych Active Directory, jak i program serwera uwierzytelniania Kerberos. W związku z tym obsługuje uwierzytelnianie i wyszukiwanie AD w domenie.

Domeny z wieloma kontrolerami.

Domena Y ma dwa kontrolery domeny. Oba serwery mają zsynchronizowane bazy danych AD, więc każdy z nich może obsłużyć żądanie usługi Active Directory LDAP. Posiadanie dwóch (lub więcej) kontrolerów domeny zapewnia niezawodność w przypadku awarii lub pomyślnego ataku. Drzewa. Domeny AD mogą być zorganizowane w hierarchie zwane drzewami. Hierarchia na rysunku ma trzy domeny. Jednak drzewa mogą mieć wiele domen.

Lasy. Wyobraź sobie proste drzewo z wieloma domenami. Niektóre korporacje mają również wiele drzew. Mogą łączyć ze sobą wiele drzew w las.

Replikacja. W domenie zachodzi całkowita replikacja między kontrolerami domeny. A co z replikacją w drzewach? Odpowiedź jest taka, że kontrolery domeny często replikują część swojej bazy danych AD na kontrolery domeny na następnym wyższym poziomie, ale zwykle nie replikują wszystkich danych. Replikacja między domenami na tym samym poziomie i między lasami jest zwykle jeszcze bardziej selektywna. Na szczęście AD jest bogata w narzędzia do określania replikacji w określonych domenach. Oczywiście to samo bogactwo wymaga silnej kontroli politycznej, aby uniknąć chaosu i bezpieczeństwa szwajcarskiego sera.

TEST CXXXII

a. Co to jest produkt serwera katalogowego firmy Microsoft?

b. Jaka jest najmniejsza jednostka organizacyjna w Active Directory?

c. Jakie dwie rzeczy zawiera kontroler domeny?

d. Czy domena może mieć wiele kontrolerów domeny?

ei. Jaka jest zaleta posiadania wielu kontrolerów domeny?

f. W jakie większe struktury zorganizowane są domeny?

g. W jaką większą strukturę można zorganizować drzewa?

h. Opisz replikację między kontrolerami domeny w jednej domenie AD.

i. Opisz replikację między kontrolerem domeny w jednej domenie a kontrolerem domeny w domenie nadrzędnej.

Zaufanie

Zaufanie oznacza, że jeden serwer katalogowy przyjmie informacje od innego. Możliwych jest kilka rodzajów zaufania.

Zaufanie oznacza, że jeden serwer katalogowy będzie akceptował informacje od innego

• Zaufanie może być wzajemne (dwukierunkowe). Możliwe jest jednak również zaufanie jednokierunkowe, w którym jeden serwer katalogów ufa drugiemu, ale to zaufanie nie jest odwzajemnione.

• Czasami zaufanie jest przechodnie. Oznacza to, że jeśli serwer katalogów X ufa serwerowi katalogów Y, a serwer katalogów Y ufa serwerowi Z, serwer katalogów X automatycznie ufa serwerowi katalogów Z.

• Jeśli natomiast serwer Directory Server X ufa serwerowi Directory Server Y, a serwer Directory Server Y ufa serwerowi Directory Server Z, ale serwer Directory Server X nie ufa automatycznie serwerowi Directory Server Z, to zaufanie jest nieprzechodnie.

Kontrolując kierunkowość i przechodniość zaufania, firma może stworzyć odpowiednie relacje zaufania między swoimi serwerami katalogowymi. Istnieje jednak wiele możliwych relacji zaufania, więc ustanowienie relacji zaufania jest trudnym zadaniem, a błędy mogą prowadzić do luk w zabezpieczeniach. Ważną zasadą rządzącą przyznawaniem trustów jest to, że bezpieczniej jest początkowo obdarzać zbyt małym zaufaniem niż zbyt dużym zaufaniem.

TEST CXXXIII

a. Rozróżnij wzajemne i jednokierunkowe zaufanie między domenami AD.

b. Rozróżnij zaufanie przechodnie i nieprzechodnie.

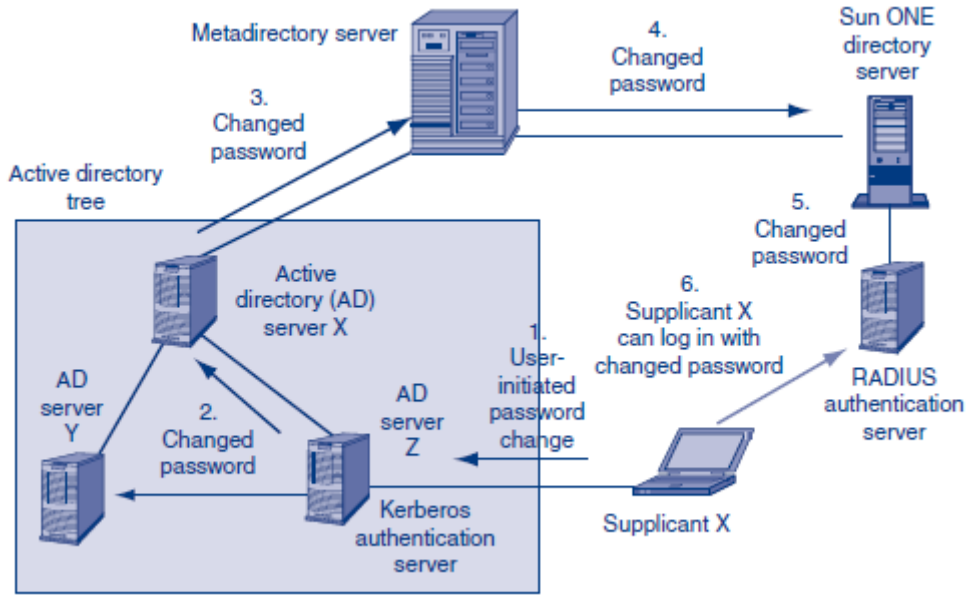
c. Jaką zasadą powinny kierować się firmy przy dokonywaniu cesji powierniczych?

ZARZĄDZANIE PEŁNĄ TOŻSAMOŚCIĄ

Centralne serwery uwierzytelniania i serwery katalogowe to tylko dwa kroki, które organizacje podejmują w celu zarządzania tożsamościami swoich użytkowników i zasobami technicznymi.

Inne serwery katalogowe i metakatalogi

W idealnym świecie firma miałaby tylko jedną rodzinę serwerów katalogowych. Zamiast tego firmy zazwyczaj mają kilka typów serwerów katalogowych, jak pokazuje Rysunek.



Inne popularne typy serwerów katalogowych to Novell eDirectory i serwery katalogowe Sun ONE dla systemu Solaris (wersja systemu Unix firmy Sun). Aby połączyć ze sobą te różne serwery katalogów, firma na rysunku posiada serwer metakatalogów. Serwer metakatalogów umożliwia serwerom katalogowym wymianę informacji i synchronizację usług na różne sposoby. Niestety te wymiany i synchronizacje są dziś ograniczone. Najczęściej, gdy użytkownik resetuje hasło na jednym serwerze katalogowym, serwer metakatalogu przekazuje resetowanie hasła do innych serwerów katalogowych.

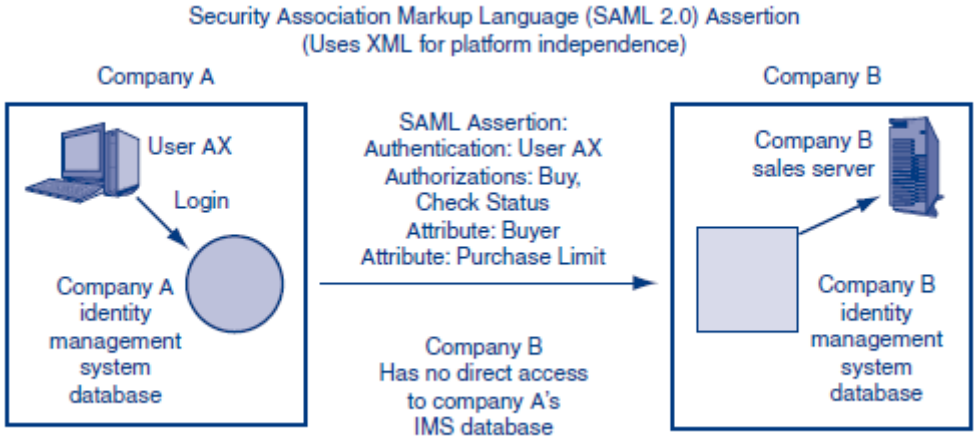
TEST CXXXIV

a. Dlaczego potrzebne są serwery metakatalogów?

b. Co robią serwery metakatalogów?

Zarządzanie tożsamością federacyjną

W firmach zaufanie jest złożone. Sytuacja między firmami jest jeszcze bardziej złożona. Między firmami mówimy o uwierzytelnianiu sfederowanym, autoryzacji i audycie lub, częściej, o zarządzaniu tożsamością federacyjną. Rysunek ilustruje federacyjne zarządzanie tożsamością.



W takim przypadku Pracownik Dave najpierw loguje się do serwera zarządzania tożsamością Firmy A i jest uwierzytelniany w tym procesie. Pracownik Dave jest kupującym w Firmie A. Ma limit zakupów w wysokości 10 000 USD. Dave prosi serwer federacyjnego zarządzania tożsamością w Firmie A o skontaktowanie się z serwerem sprzedaży w Firmie B, aby mógł zakupić materiały eksploatacyjne w Firmie B. Serwer federacyjnego zarządzania tożsamością w Firmie A wysyła potwierdzenie do swojego odpowiednika w Firmie B. oświadczenie, które Firma B powinna uznać za prawdziwe, jeśli Firma B ufa Firmie A. Stwierdzenie to może składać się z trzech głównych elementów.

Zapewnienie to stwierdzenie, które Firma B powinna uznać za prawdziwe, jeśli Firma B ufa Firmie A.

Zarządzanie tożsamością

Rozpoczęliśmy tę dyskusję od uwierzytelniania, autoryzacji i audytu. Gdy przeszliśmy do bardziej wyrafinowanych tematów, zaczął pojawiać się termin zarządzanie tożsamością. Teraz nadszedł czas, aby być bardziej precyzyjnym w rozmowach o zarządzaniu tożsamością. Formalnie zarządzanie tożsamością to oparte na zasadach zarządzanie wszystkimi informacjami wymaganymi do uzyskania dostępu do systemów korporacyjnych przez ludzi, komputery, programy lub inne zasoby.

Zarządzanie tożsamością to scentralizowane, oparte na zasadach, zarządzanie wszystkimi informacjami wymaganymi do uzyskania dostępu do systemów korporacyjnych przez ludzi, komputery, programy lub inne zasoby.

KORZYŚCI Z ZARZĄDZANIA TOŻSAMOŚCIĄ

Zarządzanie tożsamościami może obniżyć koszty, zmniejszając ilość nadmiarowej pracy potrzebnej do zarządzania dostępem użytkowników, w tym aprowizacji, wycofywania aprowizacji, resetowania haseł i wielu innych zadań. Zarządzanie tożsamościami wymusza spójność, zezwalając na pojedynczą zmianę na serwerze zarządzania tożsamością w celu dodania, zmiany lub usunięcia uprawnień dostępu pracownika na wszystkich serwerach w organizacji. Ponadto system zarządzania tożsamością umożliwia scentralizowany audyt wszystkich uprawnień dostępu pracowników w całej firmie. Potencjalną korzyścią z zarządzania tożsamością jest jednokrotne logowanie (SSO). Podczas logowania jednokrotnego użytkownik uwierzytelni się raz w systemie zarządzania tożsamością. Od tego momentu, gdy użytkownik prosi o dostęp do określonego serwera, nie ma potrzeby dodatkowego logowania. Niestety pełne logowanie jednokrotne w całej firmie jest prawie niemożliwe. Chociaż jednokrotne logowanie jest dobrym celem długoterminowym, ograniczone logowanie to wszystko, co dziś mogą osiągnąć firmy. W przypadku ograniczonego logowania pracownik może zalogować się raz i otrzymywać usługi z kilku serwerów, ale nie ze wszystkich serwerów. Zazwyczaj skrócone logowanie

daje typowemu użytkownikowi dostęp do poczty e-mail i większości innych usług, których będzie potrzebował, więc logowanie się do innych serwerów zwykle nie jest zbyt uciążliwe. Innym powodem rosnącego znaczenia zarządzania tożsamością jest to, że wiele systemów zgodności (omówionych w rozdziale 2) wymaga silnej kontroli dostępu, która prawdopodobnie będzie skuteczna tylko przy silnym zarządzaniu tożsamością.

CO TO JEST TOŻSAMOŚĆ?

Chociaż tożsamość może wydawać się prostym pojęciem, w praktyce jest wysoce kontekstowa. Wszyscy mamy tożsamość rodzinną, tożsamość zawodową i tożsamość w szkole. Każda tożsamość zawiera pewne informacje o nas, ale nie zawiera innych informacji. Ze względu na te czynniki zdefiniujemy tożsamość jako zbiór atrybutów dotyczących osoby lub zasobu nieludzkiego, które muszą zostać ujawnione w określonym kontekście. Mówimy „musi być", ponieważ podstawową zasadą jest minimalna tożsamość danych – nieujawnianie większej ilości informacji o osobie lub zasobie niż jest to konieczne do określonego celu. W przeciwnym razie atakujący mogą uzyskać informacje, niż nie powinni.

Tożsamość to zestaw atrybutów dotyczących osoby lub zasobu nieludzkiego, które muszą zostać ujawnione w określonym kontekście.

ZARZĄDZANIE TOŻSAMOŚCIĄ

Przyjrzeliśmy się przede wszystkim technologiom zarządzania tożsamością, ale praca i zarządzanie to najbardziej złożone aspekty zarządzania tożsamością. Wymienimy tylko kilka aspektów zarządzania tożsamością, które zarządza tożsamościami od ich kreacji do ich usunięcia.

• Wstępne sprawdzanie poświadczeń - przywołaj problem z uwierzytelnianiem podstawowym z wcześniejszego rozdziału. O ile poświadczenia pracowników nie zostaną bardzo dokładnie sprawdzone na początku zatrudnienia, późniejsze środki bezpieczeństwa będą bez znaczenia.

• Definiowanie tożsamości - jak już omówiono, ilość informacji, które należy podać w określonych okolicznościach, powinna być ograniczona. Uważne projektowanie tożsamości dla każdej sytuacji ma kluczowe znaczenie dla bezpieczeństwa.

• Relacje oparte na zaufaniu - Widzieliśmy wcześniej, że istnieje wiele rodzajów relacji opartych na zaufaniu. Właściwe relacje zaufania są również niezbędne dla dobrego bezpieczeństwa.

• Provisioning - autoryzacje i uwierzytelnianie muszą być dostarczane ostrożnie, a następnie zmieniane za każdym razem, gdy zmieniają się role lub inne warunki. To może być ogromne zadanie. Konto może wymagać ponownej aprowizacji, gdy nastąpią zmiany, a ostatecznie wyrejestrowania, gdy nie jest to już właściwe.

• Decentralizacja - najlepiej, aby tożsamościami zarządzali ludzie najbliżej sytuacji. Oczywiście należy zachować właściwy rozdział i zasady; dlatego decentralizacja musi być starannie planowana i zarządzana.

• Funkcje samoobsługi - w przypadku niewrażliwych informacji użytkownicy mogą samodzielnie aktualizować dane. Na przykład, jeśli ktoś zmieni swój stan cywilny i jeśli nie ma to wpływu na bezpieczeństwo, powinien mieć możliwość zrobienia tego samodzielnie w systemie zarządzania tożsamością, najlepiej za pośrednictwem portalu internetowego.

TEST CXXXV

a. Co to jest zarządzanie tożsamością?

b. Jakie są korzyści z zarządzania tożsamością?

c. Co to jest logowanie jednokrotne?

d. Dlaczego pełne logowanie jednokrotne jest generalnie niemożliwe?

e. Co to jest skrócone logowanie?

f. Czym jest tożsamość?

g. Dlaczego podawanie minimalnych danych dotyczących tożsamości jest ważną zasadą?

a. Co to jest aprowizowanie, ponowne aprowizowanie i wyrejestrowywanie w zarządzaniu tożsamością?

b. Dlaczego pożądane jest zarządzanie zdecentralizowane?

c. Dlaczego pożądane są funkcje samoobsługowe?

d. Jakie zmiany należy wprowadzić poprzez funkcje samoobsługowe?

Zaufanie i ryzyko

Wiele osób czuje się niekomfortowo z ideą zaufania. W związku z tym często bardziej przydatne jest myślenie w kategoriach ryzyka niż zaufania. Ilekroć mamy do czynienia z innymi, wiąże się to z ryzykiem. Musimy jednak zaakceptować to ryzyko, jeśli mamy pracować z innymi. Jak zauważono w rozdziale 2, bezpieczeństwo to tak naprawdę zarządzanie ryzykiem. Celem zabezpieczenia jest ograniczenie ryzyka do akceptowalnego poziomu, a nie całkowite wyeliminowanie ryzyka. Zarządzanie tożsamością na różnych poziomach siły przynosi różne stopnie redukcji ryzyka. Firma musi zrównoważyć te ograniczenia ryzyka z kwotą, jaką zarządzanie tożsamością będzie kosztować, aby wdrożyć w całym cyklu życia. Rozważając ryzyko, firma musi brać pod uwagę możliwe przyszłe przedsięwzięcia, a nie tylko te obecne. Jednym z czynników, które należy wziąć pod uwagę, myśląc o zarządzaniu tożsamością i ryzyku, jest to, że silny system zarządzania tożsamością może pozwolić na nowe przedsięwzięcia, które byłyby zbyt ryzykowne bez silnego zarządzania tożsamością.

TEST CXXXVI

a. W jakim sensie zarządzanie tożsamością jest tak naprawdę tylko kolejną formą zarządzania ryzykiem?

b. Jak zarządzanie tożsamością może zmniejszyć ryzyko?

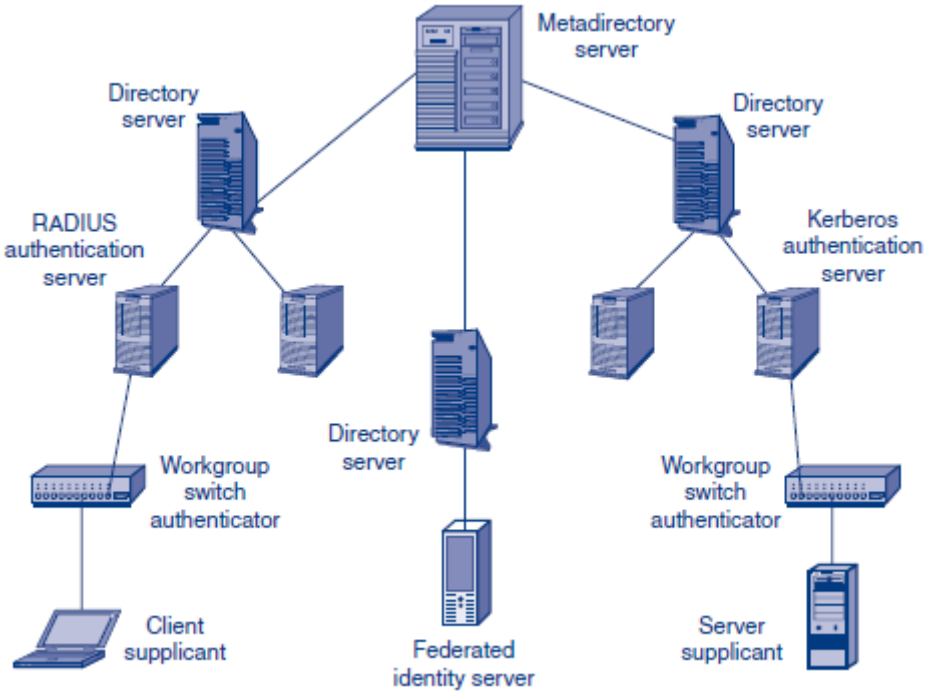
c. Ile firmy powinny wydać na zarządzanie tożsamością?

WNIOSEK

Kontrola dostępu to oparta na zasadach kontrola dostępu do systemów, danych i dialogów. Bezpieczeństwo dostępu zaczyna się od fizycznego zabezpieczenia budynku. Ważne jest, aby kontrolować dostęp i wejścia do budynku za pomocą strażników i urządzeń monitorujących. Ważna jest również kontrola nad drzwiami wewnętrznymi prowadzącymi do wrażliwych części budynku. Ważne jest, aby mieć kontrolę nad usuwaniem, aby napastnicy nie mogli nurkować w Dumpste w poszukiwaniu informacji. Bezpieczeństwo fizyczne musi obejmować pomieszczenia ze sprzętem komputerowym, komputery stacjonarne i urządzenia mobilne, a nawet wymienne nośniki pamięci. Hasła wielokrotnego użytku zapewniają niski poziom uwierzytelniania, ale są znane ludziom i są wbudowane w komputerowe systemy operacyjne. Jeśli atakujący zdoła ukraść plik z hasłami, może uruchomić na nim program do łamania haseł. Jeśli złamią hasło do konta root lub mogą podnieść swoje

uprawnienia do uprawnień konta root, napastnicy będą „właścicielami” maszyny. Firmy potrzebują silnych zasad dotyczących haseł, aby zapewnić, że hasła są długie (co najmniej osiem znaków) i złożone (w tym litery z dużymi literami, cyfry i inne znaki z klawiatury). W szczególności nie powinny być zwykłymi słowami ani niewielkimi odmianami popularnych słów. Firma musi również opracować system resetowania haseł w przypadku zgubionych haseł. Aby obniżyć koszty, firma może korzystać z automatycznego resetowania hasła, ale należy to robić bardzo ostrożnie.

Karty dostępu i tokeny fizyczne ograniczają dostęp do osób posiadających urządzenia fizyczne. Tokeny dostępu zbliżeniowego można nawet odczytać na odległość, gdy osoba zbliża się do zasobu. Urządzenia fizyczne mogą zostać zgubione lub skradzione, dlatego większość firm wymaga uwierzytelniania dwuskładnikowego, w którym użytkownik musi wprowadzić kod PIN lub użyć innego rodzaju uwierzytelniania wraz z urządzeniem fizycznym. Uwierzytelnianie biometryczne wykorzystuje pomiary ciała lub działania do uwierzytelniania osób. Auser musi najpierw zarejestrować się w systemie. Z danych skanowania jego rejestracji wyodrębnia się kilka kluczowych funkcji i przechowuje je w bazie danych uwierzytelniania jako szablon osoby. W przypadku późniejszych prób dostępu dane każdego skanowania dostępu są ponownie redukowane do kilku kluczowych funkcji, a te kluczowe funkcje są porównywane z szablonem użytkownika. Uwierzytelnianie biometryczne daje obietnicę wyeliminowania użycia haseł wielokrotnego użytku. Niestety, niepewne poziomy błędów i podatność na oszustwa pozostają głównymi problemami. W przypadku fałszywej akceptacji osoba jest błędnie zadeklarowana jako dopasowanie do szablonu w bazie danych uwierzytelnień. W przypadku fałszywego odrzucenia osoba, która powinna zostać zadeklarowana jako dopasowanie do szablonu, nie jest uważana za dopasowanie. Innym zestawem ważnych rozróżnień w biometrii są różnice między weryfikacją (uwierzytelnianiem osoby, która twierdzi, że ma określoną tożsamość), identyfikacją (określanie tożsamości osoby) i członkostwem na liście obserwacyjnej. Skanowanie linii papilarnych dominuje obecnie w biometrii; zapewnia niedrogie uwierzytelnianie o niskim poziomie bezpieczeństwa. Skanowanie tęczówki dominuje w przypadku aplikacji o wysokim poziomie bezpieczeństwa. Skanowanie twarzy budzi kontrowersje. Pozwala na potajemną identyfikację, ale ma bardzo wysoki wskaźniki błędów i wskaźniki oszustw. Uwierzytelnianie kryptograficzne wykorzystuje certyfikaty cyfrowe. Uwierzytelnianie kryptograficzne wymaga od firmy stworzenia infrastruktury klucza publicznego (PKI). Większość firm staje się własnym urzędem certyfikacji. Autoryzacje to uprawnienia, które należy nadać uwierzytelnionym podmiotom. Autoryzacja powinna być zgodna z zasadą najmniejszych uprawnień – nadanie każdemu podmiotowi minimalnych uprawnień wymaganych do pracy. Inspekcja jest niezbędna do wykrycia działań sprzecznych z zasadami. Zdarzenia dostępu do kluczy powinny być rejestrowane i regularnie odczytywane. Należy również przeprowadzać okresowe audyty zewnętrzne, a także pożądane są alerty w czasie rzeczywistym. Firmy mają wielu użytkowników i serwerów, a większość użytkowników potrzebuje uprawnień dostępu do wielu serwerów. Jeśli uprawnienia są przydzielane niezależnie na różnych serwerach, może to powodować wiele problemów. Zarządzanie tożsamościami centralizuje uprawnienia dostępu. Żadna firma nie ma pełnego zarządzania tożsamością, ale firmy zmierzają w tym kierunku. Jak pokazuje Rysunek, pierwszym krokiem jest użycie scentralizowanych serwerów uwierzytelniania.



Kolejne kroki to użycie serwerów katalogów i wielu typów katalogów połączonych przez serwery metakatalogów. Przyjrzeliśmy się szczegółowo usłudze Active Directory, która jest produktem serwera katalogowego firmy Microsoft. Wreszcie, federacyjne zarządzanie tożsamością pozwala na różne firmy, które ufają sobie nawzajem, wymieniają między sobą twierdzenia dotyczące tożsamości pracowników, ale nie przeglądają nawzajem swoich baz danych identyfikacyjnych. Tożsamości to złożone rzeczy. Tożsamość to zestaw atrybutów dotyczących osoby lub zasobu nieludzkiego, które muszą zostać ujawnione w określonym kontekście. Ze względów bezpieczeństwa ważne jest ograniczenie ujawnianych informacji do minimum wymaganego w danym kontekście. Pracownicy będą mieli wiele różnych tożsamości, ponieważ mają do czynienia z różnymi kontekstami, ale w scentralizowanej bazie danych zarządzania tożsamościami będzie tylko jeden zestaw danych tożsamości dla każdej osoby.

Jedną z potencjalnych korzyści związanych z zarządzaniem tożsamością jest jednokrotne logowanie, które umożliwia każdemu pracę z dowolnym zasobem po uprzednim zalogowaniu się do centralnego serwera uwierzytelniania. W praktyce firmy mogą zapewnić jedynie ograniczone logowanie, w którym wstępne uwierzytelnienie może zapewnić dostęp do ograniczonej grupy zasobów. Chociaż specjaliści ds. bezpieczeństwa zwykle mówią o ochronie AAA w kategoriach zaufania, należy pamiętać, że zaufanie to tylko kolejny sposób patrzenia na analizę ryzyka. Lepsze zabezpieczenia AAA zmniejszają ryzyko kontaktów z osobą lub organizacją. Ponadto bardzo silne zabezpieczenia AAA mogą pozwolić firmie na podjęcie pewnych działań, które byłyby zbyt ryzykowne bez bardzo silnych zabezpieczeń AAA. Jednocześnie korzyści płynące z ograniczenia ryzyka należy zestawić z kosztem ochrony AAA potrzebnej do osiągnięcia tych korzyści.

Pytania do przemyślenia

1. Hasła wielokrotnego użytku zapewniają słabe bezpieczeństwo. Jak myślisz, co powstrzymuje ich zastąpienie innymi podejściami?

2. Utwórz dwa dobre pytania dotyczące resetowania hasła. Dla każdego wyjaśnij, dlaczego uważasz, że to dobre pytanie.

3. Ktoś mówi, że chce chronić swój komputer stacjonarny przed atakiem typu walk-up za pomocą hasła lub haseł. Daj im radę i uzasadnienie twojej rady. To nie jest bardzo krótka odpowiedź.

4. (a) Podaj dwie sytuacje, w których ryzyko oszustwa jest wysokie. (b) Podaj dwie sytuacje, w których ryzyko oszustwa jest niskie.

5. Twój znajomy chce zabezpieczyć swój komputer stacjonarny za pomocą skanowania linii papilarnych lub ochrony dostępu hasłem. Przekaż swojemu przyjacielowi informacje, które powinien znać, aby podjąć decyzję. Rozważ alternatywy. To nie jest bardzo krótka odpowiedź.

6. Co oznaczają FRR, gdy skanowanie linii papilarnych służy do zabezpieczenia komputera przed atakami typu walk-up? Co może generować wysokie FRR? Czy możesz wymyślić sposób na zmniejszenie tego problemu podczas skanowania odcisków palców?

7. Niektóre lotniska instalują systemy rozpoznawania twarzy w celu identyfikacji terrorystów i przestępców. Około jedna na milion osób przechodzi przez lotnisko jest terrorystą. Załóżmy, że FAR wynosi około 1 procent. FRR wynosi około 30 proc. Czy ten system będzie sprawny? Wyjaśnij, używając analizy arkusza kalkulacyjnego z rozsądnymi założeniami. Wytnij i wklej analizę arkusza kalkulacyjnego do pliku pracy domowej, zamiast przekazywać ją osobno. Podaj krótki akapit zawierający wnioski.

8. Centralizacja uwierzytelniania i autoryzacji zmniejsza koszty, poprawia spójność oraz umożliwia szybkie udostępnianie i wprowadzanie zmian. Wymień technologie na drodze do większej centralizacji, zaczynając od samodzielnych uwierzytelniaczy za pośrednictwem firmowych serwerów metakatalogów.

9. Załóżmy, że prawdopodobieństwo fałszywej akceptacji wynosi 0,0001 na próbę dopasowania. Załóżmy, że baza danych zawiera 1000 szablonów. Jakie jest prawdopodobieństwo fałszywej akceptacji w przypadku weryfikacji? Jakie jest prawdopodobieństwo fałszywej akceptacji w przypadku identyfikacji? Jakie jest prawdopodobieństwo fałszywej akceptacji, jeśli istnieje lista obserwacyjna składająca się z 50 osób, którym należy przyznać dostęp do systemu?

10. Wymień co najmniej sześć tożsamości, które wymagają różnych uwierzytelniania i autoryzacji.

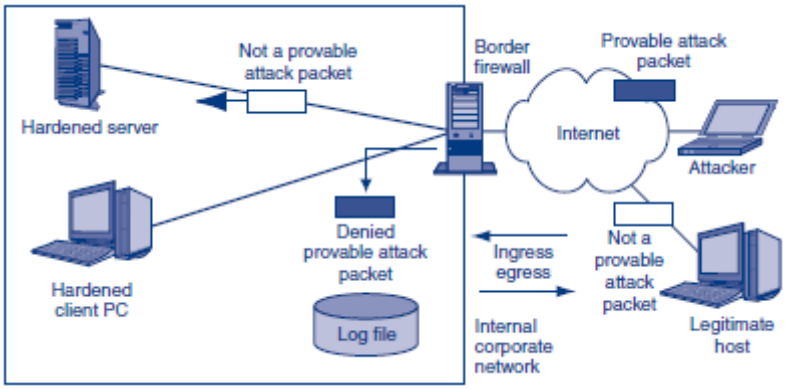
11. Twoja firma instaluje system rozpoznawania twarzy dla dostępu do drzwi. (a) Jego FRR jest znacznie gorszy niż roszczenia sprzedawcy. Co może być tego przyczyną? (b) FRR systemu wzrasta z czasem. Co może być tego przyczyną?

FIREWALLE

WPROWADZENIE

Podstawowa obsługa zapory

Rysunek pokazuje, że zapora bada każdy przechodzący przez nią pakiet.



Jeśli pakiet jest możliwym do udowodnienia pakietem ataku, zapora odrzuca pakiet. Jeśli pakiet nie jest możliwym do udowodnienia pakietem ataku, zapora przekazuje pakiet do miejsca docelowego. W firewallach nazywa się to decyzją typu pass/deny. Należy zauważyć, że zapora przepuszcza wszystkie pakiety, które nie są możliwymi do udowodnienia pakietami ataku. Oznacza to, że przepuszcza każdy prawdziwy pakiet ataku, który nie jest możliwym do udowodnienia pakietem ataku. Umożliwi to pakietom ataku dotarcie do swoich celów. W związku z tym ważne jest, aby wzmocnić hosty, aby chronić je przed pakietami ataków, których zapora nie odrzuca. Hartowanie obejmuje szereg zabezpieczeń, które zobaczymy w kolejnych rozdziałach. Oprócz odrzucania możliwych do udowodnienia pakietów ataków, zapory zwykle zapisują informacje o każdym odrzuconym pakiecie w pliku dziennika. Ten proces nazywa się rejestrowaniem. Administrator zapory powinien przeglądać ten plik dziennika codziennie lub nawet częściej, aby zrozumieć rodzaje ataków, których doświadcza firma. Nawet jeśli zapora odrzuca wiele pakietów od konkretnego atakującego, może nie odrzucać ich wszystkich. Administrator zapory może zmienić konfigurację zapory tak, aby odrzucała wszystkie pakiety z adresu IP napastnika lub może podjąć inne działania. Zapora pokazana na rysunku 6-1 jest zaporą graniczną. Znajduje się na granicy między witryną firmową a zewnętrznym Internetem. Zobaczymy później, że wiele firm ma również wewnętrzne zapory sieciowe, które filtrują ruch przechodzący między różnymi częściami sieci wewnętrznej witryny. Podczas filtrowania ruchu przychodzącego zapora bada pakiety wchodzące do sieci z zewnątrz, zazwyczaj z Internetu. Celem filtrowania ruchu przychodzącego jest zapobieganie przedostawaniu się pakietów ataku do sieci wewnętrznej firmy. Filtrowanie przychodzące jest tym, o czym myśli większość ludzi, gdy słyszą termin filtrowanie zapory. W filtrowaniu ruchu wychodzącego zapora filtruje pakiety wychodzące z sieci. Zapobiega to opuszczaniu sieci przez odpowiedzi na pakiety sondujące. (Omówiliśmy pakiety sondujące w rozdziale 1.) Zapobiega również atakom zainfekowanych hostów firmy na inne firmy. (Dzięki temu firma jest dobrym sąsiadem; może również zapobiegać procesom sądowym). Filtrowanie ruchu wychodzącego może nawet uniemożliwić pracownikom i zaatakowanym hostom wysyłanie plików zawierających własność intelektualną firmy poza firmę.

TEST CXXXVII

a. Co to jest decyzja o przyznaniu/odrzuceniu?

b. Jaki typ pakietu odrzuca i rejestruje zapora?

c. Co robi zapora z pakietami, które podejrzewa (ale nie mogą udowodnić) są pakietami ataku?

d. Dlaczego zapora rejestruje informacje o odrzuconych pakietach?

e. Rozróżnij zapory graniczne i zapory wewnętrzne.

f. Rozróżnij filtrowanie przychodzące i wychodzące.

Strategia i technologia bezpieczeństwa

Wielka chińska zapora sieciowa

Wielka chińska zapora ogniowa to kompleksowy system filtrowania, który może blokować, filtrować i przekierowywać cały ruch internetowy przychodzący, wychodzący i wewnątrz Chin. Chińska Republika Ludowa (ChRL) uruchomiła Wielką Chińską Zaporę Sieciową, oficjalnie znaną jako Projekt Złota Tarcza, w 1998 r. w odpowiedzi na obawy, że Internet pozwoli na zdobycie władzy wywrotowym frakcjom politycznym. Rozpoczęła działalność w 2002 roku, a przez lata pojawiły się dodatkowe komponenty.

FILTROWANIE I MONITOROWANIE

Great Firewall of China jest zarządzany przez Ministerstwo Bezpieczeństwa Publicznego i działa w 31 prowincjach i miastach. Ruch można blokować, filtrować i przekierowywać na wiele sposobów. Niektóre z metod, które zostały użyte w projekcie Golden Shield, obejmują blokowanie adresów IP (lub blokowanie adresów IP), blokowanie adresów URL, blokowanie nazw hostów, zatruwanie DNS w celu filtrowania i przekierowywania oraz skanowanie ruchu w poszukiwaniu określonych „zabronionych" słów kluczowych. Wielka chińska zapora ogniowa również ewoluuje w czasie i prawdopodobnie będzie miała większą funkcjonalność w przyszłości. Oprócz zarządzania ruchem internetowym, projekt Złota Tarcza obejmuje również wiele innych w pełni zintegrowanych systemów bezpieczeństwa IT. Obejmują one między innymi systemy nadzoru wideo, systemy bezpieczeństwa sieci, systemy rozpoznawania twarzy, systemy zarządzania populacją, systemy dochodzeniowe i zintegrowane systemy biznesowe. Pełna zdolność tych systemów nie jest znana. Poniższy rysunek przedstawia dwa wyszukiwania filmów związanych z „Falun Gong" przy użyciu zarówno Google.hk (Hong Kong), jak i najlepszej chińskiej wyszukiwarki Baidu. Falun Gong to ruch duchowy, który został zakazany przez Komunistyczną Partię Chin (CPC) w 1999 roku. Wyszukiwania na serwerach Google w Hongkongu zwracają liczne filmy i artykuły o Falun Gong. Wyszukiwania z użyciem Baidu nie zwracają żadnych filmów, a jedynie ostrzeżenie, że „wyniki wyszukiwania mogą być niezgodne z odpowiednimi przepisami . . ". Wyniki wyszukiwania zwracają również tylko te artykuły, które wspierają stanowisko CPC. Jak na ironię, zrzut ekranu z wynikami wyszukiwania z Baidu.com nie mógł zostać użyty w tej książce. Baidu.com nie odpowie na prośbę o użycie zrzutu ekranu z wynikami wyszukiwania, które są materiałem chronionym prawem autorskim. Ironia polega na tym, że szacunkowo jedna piąta całego ruchu w Baidu jest generowana przez użytkowników poszukujących nielegalnego pobierania muzyki. Baidu czerpie korzyści z praw autorskich obowiązujących poza Chinami, ale pozwala na zawieszenie tych praw w samych Chinach. Z drugiej strony Google ma stałą politykę, zgodnie z którą dowolny niezmieniony zrzut ekranu może zostać użyty w dowolnej publikacji. Google aktywnie usuwa również treści naruszające prawa autorskie.

CO JEST ZABLOKOWANE?

Biała księga zatytułowana Internet w Chinach została wydana w 2010 roku przez Biuro Informacyjne Rady Państwa Chin. W tej białej księdze przedstawiono politykę dotyczącą korzystania z Internetu. Poniżej znajduje się lista treści, które Chiny uznają za nielegalne i mogą być blokowane lub filtrowane. Decyzja Stałego Komitetu Narodowego Kongresu Ludowego ds. Ochrony Bezpieczeństwa w Internecie,

Regulaminu Telekomunikacji Chińskiej Republiki Ludowej oraz środków dotyczących administrowania informacjami internetowymi. Usługi przewidują, że żadna organizacja ani osoba nie może wytwarzać, powielać, ogłaszać ani rozpowszechniać informacji o następującej treści:

• Sprzeczność z kardynalnymi zasadami określonymi w Konstytucji

• Zagrażające bezpieczeństwu państwa

• Ujawnianie tajemnic państwowych

• Obalanie władzy państwowej

• Zagrożenie zjednoczenia narodowego

• Niszczenie honoru i interesów państwowych

• podżeganie do nienawiści etnicznej

• Dyskryminacja

• Zagrażanie jedności etnicznej

• Zagrażanie państwowej polityce religijnej

• Propagowanie heretyckich lub przesądnych idei

• Rozsiewać plotki

• Zakłócanie porządku i stabilności społecznej

• Rozpowszechnianie nieprzyzwoitości

• Pornografia

• Hazard

• Przemoc

• Brutalność i terror

• Podżeganie do przestępstwa

• Upokarzanie lub oczernianie innych

• Naruszenie praw i interesów innych osób

• Inne treści zabronione przez prawo i przepisy administracyjne

Wiele stron internetowych może należeć do jednej lub wielu z tych kategorii. Wiadomości, media, sieci społecznościowe, blogi, organizacje polityczne i organizacje praw człowieka to tylko kilka rodzajów blokowanych witryn. Dosłowne blokowanie stron internetowych było włączane i wyłączane. Na przykład The New York Times zaczął być blokowany dla użytkowników w Chinach kontynentalnych pod koniec 2008 roku. Później został odblokowany. W tym samym czasie BBC, Voice of America i Asiaweek zostały odblokowane po wcześniejszym zablokowaniu. Youtube był blokowany mniej więcej raz w rokui. Facebook i Twitter są również obecnie zablokowane.

KTO JESZCZE FILTRUJE TREŚĆ

Wielka chińska zapora ogniowa może być jednym z bardziej agresywnych podejść do rządowej kontroli nad Internetem. Jednak Chiny nie są osamotnione w blokowaniu, filtrowaniu i monitorowaniu ruchu internetowego w jej granicach. Większość krajów stosuje jakąś formę filtrowania. Wiele krajów aktywnie próbuje uchwalić przepisy, które pozwolą na rozszerzone uprawnienia do filtrowania treści internetowych. Poniżej przedstawiamy tylko kilka przykładów filtrowania w innych znanych krajach.

Francja

16 lutego 2010 r. Francja uchwaliła ustawę o nazwie LOPPSI 2.9. Ta ustawa pozwoliłaby między innymi francuskiemu rządowi zmusić dostawców usług internetowych do blokowania niektórych stron internetowych. Witryny mogą być blokowane na mocy dekretu rządowego. W sprawie LICRA przeciwko Yahoo! francuski sąd uznał, że Yahoo! musi zablokować kupno lub sprzedaż pamiątek nazistowskich mieszkańcom Francji.

Stany Zjednoczone

29 listopada Departament Sprawiedliwości USA przejął 82 nazwy domen stron internetowych, które „zajmowały się sprzedażą i dystrybucją podrabianych towarów i nielegalnych dzieł chronionych prawem autorskim". Konfiskaty były publicznie wspierane przez Amerykańskie Stowarzyszenie Filmowe (MPAA) i Amerykańskie Stowarzyszenie Przemysłu Nagraniowego (RIAA). Amerykański senator Patrick Leahy powiedział: „Nie możemy dłużej siedzieć z boku, podczas gdy amerykańska własność intelektualna jest kradziona i sprzedawana online przy użyciu naszej własnej infrastruktury". Stany Zjednoczone również aktywnie prowadzą wykazy osób, firm, stron internetowych i podmiotów, które uważają za szkodliwe dla interesów USA. Lista Specjalnie Wyznaczonych Obywateli (SDN) jest prowadzona przez Departament Skarbu USA i zawiera listę osób i firm, w przypadku których „ich aktywa są zablokowane, a osoby z USA mają generalnie zakaz zajmowania się nimi".14 W 2008 roku angielskie biuro podróży działający w Hiszpanii miał 80 stron podróżniczych zablokowanych przez rząd USA, ponieważ organizował wakacje na Kubie

Niebezpieczeństwo przeciążenia ruchem

Co się stanie, jeśli ruch stanie się tak duży, że zapora nie będzie w stanie zbadać wszystkich przychodzących pakietów? Czy zapora przekaże pakiety, których nie może zbadać, czy też je odrzuci? Odpowiedź jest taka, że przeciążony firewall odrzuci wszystkie pakiety, których nie może przetworzyć. Jest to najbezpieczniejsze podejście, ponieważ nie przepuszcza pakietów ataku. Zapora nie działa bezpiecznie.

Jeśli zapora zostanie przeciążona ruchem, odrzuci pakiety, których nie może przetworzyć.

Jednak odrzucanie pakietów, których zapora nie może skutecznie przetworzyć, powoduje samoczynny atak typu „odmowa usługi" na firmę. Kluczowe znaczenie dla firm ma zakup zapór sieciowych o mocy obliczeniowej wystarczającej do obsługi ruchu, który będą musiały badać. Nawet jeśli zapora może obsłużyć ruch, gdy firma ją kupuje, zapora może później wyczerpać się.

• Najwyraźniej ruch prawdopodobnie wzrośnie.

• Ponadto, w miarę pojawiania się nowych zagrożeń, administrator zapory musi napisać więcej reguł filtrowania, a przetwarzanie tych dodatkowych reguł będzie wymagało więcej pracy zapory przetwarzania na pakiet.

• Co gorsza, podczas ataków DoS i intensywnych ataków polegających na skanowaniu ruch może znacznie wzrosnąć. Jeśli zapora działa dobrze przy normalnym poziomie ruchu, ale nie radzi sobie ze

skokami ruchu podczas dużych ataków, jest to bardzo słaba zapora. Zapory sieciowe muszą być w stanie filtrować ruch z prędkością łącza — to znaczy z maksymalną prędkością łączących się z nim linii.

Wraz ze wzrostem mocy obliczeniowej zapory, zapory będą mogły wykonywać coraz bardziej wyrafinowane przetwarzanie. Na przykład w dalszej części zobaczymy, że systemy zapobiegania włamaniom (IPS) mogą powstrzymać niektóre bardzo subtelne ataki, badając wszystkie warstwy w każdym pakiecie i badając złożone relacje w strumieniach pakietów. Co ważniejsze, prawdopodobnie będziemy świadkami rozwoju zapór ogniowych ujednoliconego zarządzania zagrożeniami (UTM), które obsługują tradycyjne przetwarzanie zapór ogniowych, filtrowanie antywirusowe, a nawet filtrowanie spamu. (Jak omówimy później, tradycyjne zapory ogniowe nie filtrują antywirusa ani innego złośliwego oprogramowania na poziomie aplikacji.) Oczywiście ruch również nadal rośnie, co zużyje przynajmniej część zwiększającej się mocy obliczeniowej zapór.

TEST CXXXVIII

a. Co robi zapora, jeśli nie nadąża za natężeniem ruchu?

b. Dlaczego to działanie jest dobre?

c Dlaczego to działanie jest złe?

d. Dlaczego zapora może ogólnie nadążyć za ruchem, ale nie radzi sobie z tym podczas poważnego ataku?

e. Co to będzie oznaczać dla filtrowania firewalla w miarę wzrostu mocy obliczeniowej w przyszłości?

f. Co to jest ujednolicone zarządzanie zagrożeniami (UTM)?

g. Co to znaczy, że firewall powinien działać z prędkością łącza?

Mechanizmy filtrowania zapory

Użyliśmy terminu filtrowanie, nie określając go konkretnie. Powodem tego braku precyzji jest to, że istnieje kilka metod filtrowania do badania pakietów. Metody te obejmują (1) stanowe filtrowanie inspekcji pakietów, (2) statyczne filtrowanie pakietów, (3) translację adresów sieciowych, (4) filtrowanie proxy aplikacji, (5) filtrowanie systemu zapobiegania włamaniom oraz (6) filtrowanie antywirusowe. Przyjrzymy się tym metodom filtrowania w tym rozdziale. Chociaż ważne jest, aby zrozumieć wszystkie te mechanizmy, ważne jest również, aby zrozumieć, że prawie wszystkie główne zapory graniczne wykorzystują stanową inspekcję pakietów (SPI) jako główny mechanizm inspekcji. Używają jednak niektórych innych mechanizmów filtrowania, które będziemy postrzegać jako wtórne mechanizmy filtrowania uzupełniające SPI. Prawie wszystkie główne firewalle graniczne wykorzystują stanową inspekcję pakietów (SPI) jako podstawowy mechanizm kontroli.

TEST CXXXIX

a. Czy istnieje tylko jeden mechanizm filtrowania firewalla?

b. Z jakich mechanizmów filtrowania korzystają prawie wszystkie główne firewalle graniczne?

c. Czy zapory sieciowe SPI wykonują tylko stanową inspekcję pakietów?

STATYCZNE FILTROWANIE PAKIETÓW

Najwcześniejsze firewalle graniczne wykorzystywały statyczne filtrowanie pakietów, które jest bardzo ograniczone. Obecnie statyczne filtrowanie pakietów nie jest już używane przez główne zapory

graniczne jako główny mechanizm filtrowania, ale niektórzy używają go jako mechanizmu wtórnego uzupełniającego inspekcję pakietów ze stanem.

Patrząc na pakiety pojedynczo

Statyczne filtrowanie pakietów analizuje pakiety pojedynczo, oddzielnie. Jest to poważne ograniczenie, ponieważ wiele ataków można powstrzymać jedynie poprzez zrozumienie miejsca pakietu w strumieniu pakietów.

Na przykład, jeśli host wewnętrzny wyśle segment TCP SYN do hosta zewnętrznego, host zewnętrzny odpowie prawidłowym segmentem TCP SYN/ACK. Co się stanie, jeśli statyczna zapora filtrująca pakiety odbierze segment TCP SYN/ACK przychodzący do witryny z zewnątrz? Może to być prawidłowa odpowiedź na segment TCP SYN hosta wewnętrznego. Może to jednak być również częścią ataku zainicjowanego z zewnątrz. Zewnętrzny atakujący może wysłać segment TCP SYN/ACK w nadziei, że otrzyma w odpowiedzi segment RST. Segment RST potwierdzi, że pod adresem IP znajduje się host, do którego atakujący wysłał segment TCP SYN/ACK. Statyczne filtrowanie pakietów, bez znajomości kontekstu pakietu, nie może odróżnić. Domyślnie będzie musiał przepuścić wszystkie pakiety zawierające segmenty SYN/ACK, ponieważ odrzucenie takich segmentów odcięłoby całą wewnętrznie inicjowaną komunikację. To tylko jeden przykład na to, jak badanie pakietów w izolacji oznacza, że niektórych ataków nie można powstrzymać przez statyczne filtrowanie pakietów.

Przeglądanie tylko niektórych pól w nagłówkach internetowych i transportowych

Oprócz patrzenia tylko na pakiety w izolacji, statyczne zapory filtrujące pakiety sprawdzają tylko nagłówki Internetu i warstwy transportowej, i zwykle patrzą tylko na niektóre pola w tych nagłówkach. Oznacza to również, że nie mogą powstrzymać wszystkich ataków, w tym ataków wymagających filtrowania wiadomości aplikacji lub filtrowania pól nagłówka, których nie bada statyczne filtrowanie pakietów.

Przydatność statycznego filtrowania pakietów

Chociaż istnieje wiele ataków, których statyczne filtrowanie pakietów nie może zatrzymać, istnieje wiele ataków, które może zatrzymać bardzo skutecznie. Na przykład, zapora ogniowa z filtrem pakietów statycznych może powstrzymać wiadomości echa protokołu ICMP (Internet Control Message Protocol) przed przychodzeniem do witryny z zewnątrz, ponieważ hakerzy wykorzystują te wiadomości jako sondy skanujące. Ponadto zapora statycznego filtru pakietów może zatrzymać wszystkie pakiety odpowiedzi ICMP echo w przypadku, gdy zapora przeoczyła jakiekolwiek przychodzące wiadomości echa. Statyczna zapora filtrująca pakiety może również zatrzymywać przychodzące pakiety z fałszywymi źródłowymi adresami IP. Atakujący może wysłać pakiet z zewnątrz ze źródłowym adresem IP, który powinien być używany tylko przez hosty w witrynie. Hosty wewnętrzne mogą ufać takim adresom, ponieważ są „lokalne”. Ponadto, jeśli host w witrynie wysyła pakiet wychodzący ze sfałszowanym źródłowym adresem IP, hostem wysyłającym może być zainfekowany komputer będący częścią botnetu. Aby podać inny przykład, atakujący może ustawić zarówno bity SYN, jak i FIN w nagłówku TCP. Oznacza to, że pakiet jednocześnie prosi o otwarcie i zamknięcie połączenia. To nie ma sensu. Jeśli system operacyjny hosta docelowego nie został przetestowany pod kątem tego dziwnego stanu, pakiet ten może spowodować awarię hosta docelowego lub spowodować, że host odeśle segment RST w pakiecie zawierającym źródłowy adres IP hosta docelowego.

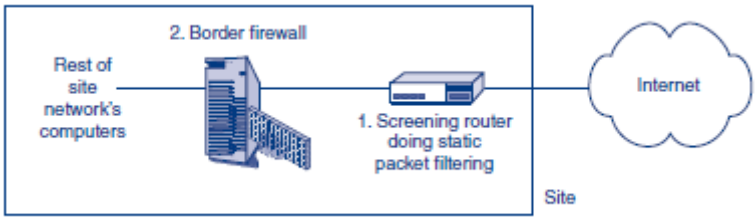
Perspektywy

Ze względu na ograniczenia związane z filtrowaniem pojedynczych pakietów w izolacji i patrzenie tylko na niektóre pola w nagłówkach Internetu i warstwy transportowej, statyczne filtrowanie pakietów

okazało się ślepym zaułkiem jako główny mechanizm filtrowania zapór granicznych. To ograniczone statyczne filtrowanie pakietów do dwóch zastosowań peryferyjnych.

• Co najważniejsze, wiele zapór typu main border używa statycznego filtrowania pakietów jako dodatkowego mechanizmu filtrowania ze względu na zdolność statycznego filtrowania pakietów do powstrzymania niektórych określonych ataków, które są trudniejsze i dlatego droższe do powstrzymania w inny sposób.

• Ponadto Rysunek pokazuje, że niektóre firmy przekształcają swoje routery graniczne w statyczne zapory filtrujące pakiety poprzez dodanie oprogramowania (a czasami pamięci RAM).



Te routery filtrujące mogą powstrzymać wiele masowych, ale prostych ataków przychodzących w celu zmniejszenia obciążenia głównej zapory granicznej. Te routery filtrujące mogą również zapewnić, że wychodzące komunikaty odpowiedzi echa ICMP i inne odpowiedzi sondujące nie zostaną przesłane do osób sondujących sieć.

TEST CXL

a. Jakie są dwa ograniczenia statycznego filtrowania pakietów? Wyjaśnij, dlaczego każde ograniczenie jest złe.

b. Z jakich dwóch powodów firmy nie stosują obecnie statycznego filtrowania pakietów jako głównego mechanizmu filtrowania w firewallach granicznych?

c. Na jakie dwa drugorzędne sposoby korporacje czasami stosują statyczne filtrowanie pakietów?

STANOWA KONTROLA PAKIETU

Podstawowa operacja

Właśnie widzieliśmy, że statyczne filtrowanie pakietów nie jest używane jako mechanizm filtrowania głównej ściany granicznej. W przeciwieństwie do tego, prawie wszystkie współczesne firewalle korporacyjne wykorzystują metodę filtrowania ze stanową inspekcją pakietów (SPI). W związku z tym w tym rozdziale przyjrzymy się bardziej szczegółowo filtrowaniu SPI.

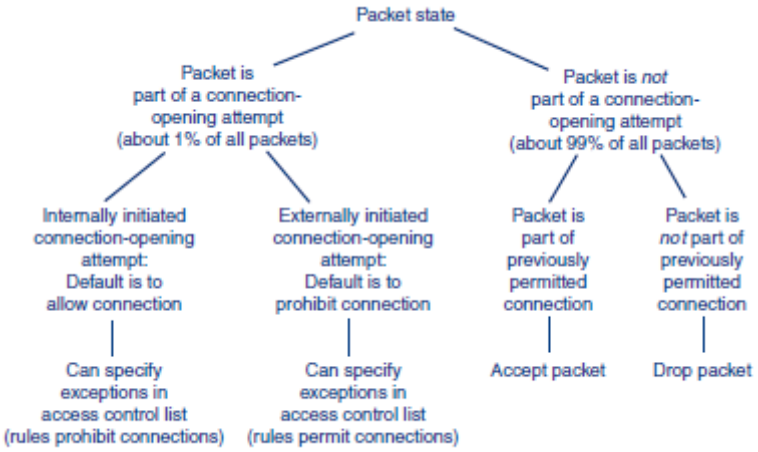
ZNAJOMOŚCI

SPI skupia się na połączeniach, które są trwałymi konwersacjami między różnymi programami na różnych komputerach. Posługując się analogią, połączenie jest jak rozmowa telefoniczna między dwojgiem ludzi.

STANY

Kiedy dzwonisz do kogoś przez telefon, istnieją dorozumiane zasady postępowania, których należy przestrzegać w różnych momentach rozmowy. Gdy osoba, do której dzwonisz, odbierze, uprzejmie jest zapytać, czy może porozmawiać. Pod koniec rozmowy niegrzecznie jest po prostu się rozłączać. W głównej fazie rozmowy niegrzecznie jest monopolizować rozmowę. Zamiast mówić o okresach, fazach

lub etapach, informatycy używają terminu stan do opisania określonego okresu czasu podczas połączenia. W rozmowach między ludźmi występuje stan otwarcia, stan ciągłej komunikacji i stan zakończenia. Pojęcie stanów ma kluczowe znaczenie dla filtrowania SPI. Rysunek ilustruje proste połączenie, w którym występują tylko dwa stany.



Stan to odrębna faza połączenia między dwoma aplikacjami.

• Po pierwsze, występuje stan otwarcia, kiedy dwie aplikacje zgadzają się na otwarcie połączenia.

• Następnie obie aplikacje przechodzą w stan trwającej komunikacji. W przypadku większości połączeń ruch jest zdominowany przez wymiany w trakcie trwającej komunikacji. Dwie aplikacje komunikują się tam i z powrotem przy użyciu tych samych numerów portów i innych warunków.

STANOWA KONTROLA PAKIETÓW W DWÓCH STANACH

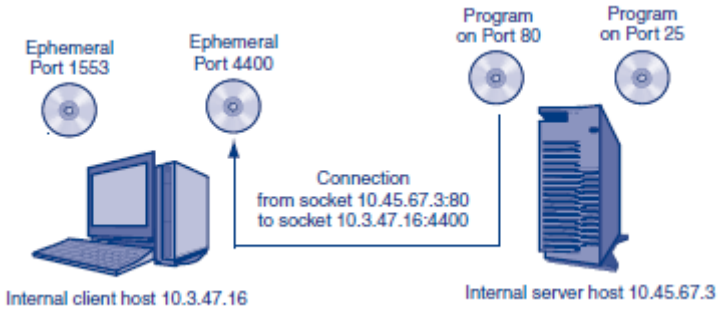
Pojęcie stanów jest ważne, ponieważ właściwe jest sprawdzanie różnych rzeczy w różnych stanach. Stateful Inspection robi dokładnie to: zmienia swoją konkretną metodę badania w zależności od stanu.

Stateful Packet Inspection (SPI) wykorzystuje różne specyficzne metody badania w zależności od stanu połączenia.

Powyższy rysunek pokazuje, że po przybyciu pakietu zapora najpierw określa, czy pakiet jest częścią próby otwarcia połączenia. Na przykład, jeśli pakiet zawiera segment TCP, próbuje otworzyć połączenie tylko wtedy, gdy ustawiony jest bit SYN. Rysunek pokazuje, że różne reguły dotyczą pakietów, które są częścią prób otwarcia połączenia i tych, które nie są. Zdecydowana większość pakietów nie jest częścią prób otwarcia połączenia. Zauważ na rysunku, że stanowa inspekcja pakietów jest prosta w przypadku pakietów, które nie próbują otworzyć połączenia. W konsekwencji prawie wszystkie pakiety są obsługiwane szybko, prosto, a zatem niedrogo. W przypadku nielicznych pakietów, które próbują otwierać połączenia, przetwarzanie zapór sieciowych inspekcji pakietów jest bardziej złożone. Na szczęście, ponieważ niewiele pakietów próbuje otworzyć połączenia, pakiety otwierające połączenie nie obciążają zapór ogniowych SPI.

REPREZENTUJĄCE POŁĄCZENIA

SPI skupia się na połączeniach między programami na różnych hostach. W sieci połączenie jest reprezentowane przez gniazdo, które wyznacza określony program (oznaczony numerem portu) na określonym komputerze (adres IP). Asocket jest zapisany jako adres IP, dwukropek i numer portu, na przykład 10.3.47.16:4400. Jak pokazuje Rysunek, połączenie jest łączem między programami na różnych komputerach. Składa się z dwóch gniazd - wewnętrznego i zewnętrznego.



TEST CXLI

a. Czym jest sta?

b. Czy większość pakietów jest częścią stanu otwarcia połączenia czy stanu trwającej komunikacji?

cC. Dlaczego odpowiedź na część b jest ważna dla wydajności inspekcji pakietów ze stanem?

d. Co to jest połączenie?

e. Jak jest reprezentowane połączenie między dwoma programami na różnych komputerach?

Pakiety, które nie próbują otwierać połączeń

W stanowej inspekcji pakietów, jak pokazano na powyższym rysunku, po nadejściu pakietu, który nie próbuje otworzyć połączenia, zapora sieciowa SPI sprawdza, czy jest częścią wcześniej zatwierdzonego połączenia.

• Jeśli jest częścią istniejącego połączenia w tabeli połączeń, pakiet jest przekazywany, zwykle bez dalszego filtrowania.

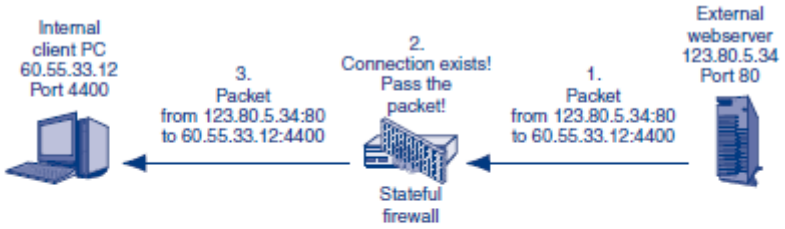
• Jeśli nie jest częścią istniejącego połączenia w tabeli połączeń, jest odrzucane i rejestrowane.

POŁĄCZENIA TCP

Załóżmy na przykład, że pakiet przychodzący z zewnątrz nie próbuje otworzyć połączenia (krok 1 na rysunku). Pakiet ma adres źródłowy IP 123.80.5.34, numer portu źródłowego TCP 80, adres docelowy IP 60.55.33.12 i numer portu docelowego TCP 4400. Jest to zgodne z połączeniem w pierwszym wierszu. Dlatego pakiet jest częścią zatwierdzonego połączenia. Zapora przekazuje pakiet.

POŁĄCZENIA UDP I ICMP

Chociaż protokoły ICMP i UDP są bezpołączeniowe, zapory sieciowe SPI mogą obsługiwać protokoły ICMP i UDP. Na przykład w przypadku ICMP istnieją interakcje typu echo-echo. Jeśli nadejdzie komunikat ICMP echo, jest to traktowane jako próba otwarcia połączenia. Wiadomość z odpowiedzią echa nie. Niektóre interakcje UDP można również obsługiwać w podobny sposób. Rysunek przedstawia wiersz reprezentujący połączenie UDP. Przepuszcza kolejne pakiety pasujące do tego połączenia.



Connection table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	4400	123.80.5.34	80	OK
UDP	60.55.33.5	3660	1.8.33.4	161	OK

2. Match

PRÓBY ATAKU

Załóżmy, że host atakującego wysyła pakiet ze źródłowym adresem IP 10.5.3.4 (sfałszowanym adresem IP) i docelowym portem TCP 80. Nie jest to próba otwarcia połączenia. (Flaga SYN nie jest ustawiona w segmencie TCP.) Na rysunku 6-8 widzimy, że ten pakiet nie pasuje do żadnego wiersza w tabeli połączeń. Zapora odrzuca i rejestruje pakiet.

PERSPEKTYWY

Widzieliśmy, że w przypadku pakietów, które nie próbują otworzyć połączenia i dlatego wydają się być częścią stanu trwającej komunikacji, przetwarzanie SPI jest bardzo proste. Jeśli połączenie znajduje się w tabeli połączeń, przekaż pakiet; jeśli nie, odrzuć pakiet. Chociaż podstawowe przetwarzanie SPI dla bieżącej komunikacji jest tak proste, możliwe jest również wbudowanie dodatkowego filtrowania w przetwarzanie. Dodatkowe filtrowanie zwiększa pracę, a tym samym koszt zapory sieciowej SPI. Jest to jednak uzasadnione.

TEST CXLII

a. Podaj prostą, stanową regułę zapory sieciowej inspekcji pakietów dla pakietów, które nie próbują otwierać połączeń.

b. Czy filtrowanie SPI dla pakietów będących częścią bieżącej komunikacji jest zwykle proste i niedrogie? Wyjaśniać.

c. UDP jest bezpołączeniowy. W jaki sposób zapora SPI może obsługiwać połączenia UDP?

Pakiety, które próbują otworzyć połączenie

Do tej pory przyjrzeliśmy się, jak zapory sieciowe SPI obsługują pakiety, które nie próbują otworzyć połączenia. Rysunek pokazuje, że zapory z inspekcją stanową mają również proste domyślne zachowanie przy podejmowaniu decyzji o przepuszczaniu pakietów, które próbują otworzyć połączenia. (Ogólnie rzecz biorąc, wartością domyślną jest to, co otrzymasz, jeśli nie określisz wyraźnie czegoś innego.)

• Domyślnie zapory SPI zezwalają na wszystkie próby otwarcia połączenia między hostem wewnętrznym a hostem zewnętrznym. Ma to sens, ponieważ zazwyczaj klienci wewnętrzni mogą otwierać połączenia z serwerami zewnętrznymi. Gdy host wewnętrzny próbuje otworzyć połączenie z hostem zewnętrznym, zapora domyślnie dodaje odpowiedni wiersz do tabeli stanów.

• Domyślnie zapora SPI uniemożliwia wszystkim hostom zewnętrznym otwieranie połączeń z hostami wewnętrznymi. Ma to sens, ponieważ niewielu klientów zewnętrznych powinno mieć dostęp do

serwerów wewnętrznych. To ustawienie domyślne uniemożliwia napastnikom łączenie się z serwerami wewnętrznymi (lub klientami).

TEST CXLIII

Podaj dwie proste domyślne reguły zapory sieciowej SPI dla pakietów, które próbują otworzyć połączenia.

Listy kontroli dostępu (ACL) dla prób otwarcia połączenia

Chociaż domyślne zachowanie zapory sieciowej z inspekcją pakietów sprawdza się w większości przypadków w przypadku prób otwarcia połączenia, organizacje muszą mieć wyjątki. W przypadku wyjątków należy zastąpić zachowanie domyślne.

• Na przykład firmy mogą wymagać zezwolenia na niektóre połączenia inicjowane z zewnątrz. Na przykład klienci zewnętrzni będą potrzebować dostępu do wewnętrznego serwera e-commerce firmy.

• Aby podać inny przykład, firmy mogą być zmuszone do zapobiegania niektórym inicjowanym wewnętrznie powiązaniom ze światem zewnętrznym. Na przykład zapora może wymagać uniemożliwienia klientom wewnętrznym łączenia się ze znanymi witrynami phishingowymi. Może również wymagać zapobiegania atakom złośliwego oprogramowania na wewnętrznych zhakowanych hostach na hosty zewnętrzne lub wysyłaniu poufnych informacji poza witrynę.

Aby określić wyjątki od reguł domyślnych, zapory SPI mają listy kontroli dostępu zarówno dla wewnętrznych, jak i zewnętrznych prób otwarcia połączenia.

Listy kontroli dostępu (ACL) składają się z szeregu reguł, które są wyjątkami od zachowania domyślnego.

• W przypadku prób otwarcia połączenia inicjowanych wewnętrznie domyślną regułą jest zezwalanie na wszystkie połączenia. Dlatego listy ACL dla prób otwarcia połączenia inicjowanych wewnętrznie określają warunki, w których połączenia inicjowane wewnętrznie powinny być blokowane.

• W przypadku prób otwarcia połączenia inicjowanych zewnętrznie domyślną regułą jest zapobieganie otwieraniu wszystkich połączeń. W związku z tym listy ACL dla prób otwarcia połączenia inicjowanych zewnętrznie określają warunki, w których niektóre próby otwarcia połączenia inicjowane zewnętrznie powinny być dozwolone.

ZNANE NUMERY PORTÓW

Reguły ACL zazwyczaj obejmują numery portów TCP lub UDP. Serwery mają dobrze znane numery portów, które oznaczają konkretne aplikacje działające na serwerze. Na przykład Port 80 to dobrze znany numer portu HTTP. Aby uniemożliwić dostęp do serwerów, zapory SPI domyślnie blokują przychodzące połączenia TCP i UDP z dobrze znanymi numerami portów. Rysunek 6-9 przedstawia niektóre z dobrze znanych numerów portów, które są często przywoływane w listach ACL. Dobrze znane numery portów wahają się od 1 do 1023.

Port	Primary Protocol*	Application
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP	Domain Name System (DNS)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP)
135–139	TCP	NETBIOS service for peer-to-peer file sharing in older versions of Windows
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP over SSL/TLS
3389	TCP	Remote Desktop Protocol (RDP)

LISTY KONTROLI DOSTĘPU (ACLS) DLA FILTROWANIA WEJŚCIOWEGO

Przypomnij sobie, że w przypadku filtrowania ruchu przychodzącego domyślnym zachowaniem jest automatyczne odrzucanie prób otwarcia połączenia zewnętrznego. W konsekwencji typowa reguła ACL dla ruchu przychodzącego zezwala na określone połączenie pochodzące z zewnątrz (powiedzmy do wewnętrznego serwera WWW).

JEŻELI-TO FORMATUJ

Reguły na rysunku mają format jeśli-to. Jeśli niektóre wartości pól pakietu odpowiadają określonym wartościom kryteriów, wtedy mówimy, że pakiet pasuje do reguły. W oparciu o część reguły „wtedy”, zapora zezwoli lub nie zezwoli na próbę otwarcia połączenia.

• Jeśli pakiet jest zgodny z regułą, zapora podejmuje wskazane działanie.

• Jeśli jednak pakiet nie jest zgodny z regułą, zapora nie podejmuje działań w oparciu o tę regułę i przechodzi do następnej reguły.

• Ostateczna reguła nie ma formatu jeśli-to. Jeśli zapora osiągnie ostatnią regułę na liście ACL, zastosuje się do tej reguły.

DOSTĘP DO PORTÓW I SERWERÓW

Reguła 1 zezwala na połączenia inicjowane zewnętrznie, jeśli numer portu docelowego TCP to 80 (HTTP) lub 443 (SSL/TLS przez HTTP). Pozwala to na dostęp do wszystkich wewnętrznych serwerów WWW. Z kolei Reguła 2 zezwala na połączenia inicjowane zewnętrznie, jeśli port docelowy TCP to 25 (jest to dobrze znany port docelowy dla serwerów pocztowych). Jednak zezwala tylko na połączenia portu 25 z pojedynczym serwerem pocztowym, 60.47.3.35. Jest to oczywiście bezpieczniejsze niż zezwalanie na połączenia z dowolnym wewnętrznym serwerem pocztowym, jak to ma miejsce w Regule 1. Porównanie bezpieczeństwa Reguł 1 i 2 ilustruje kluczową kwestię. Często istnieje wiele sposobów na wdrożenie polityki. Administrator zapory powinien zawsze wybierać regułę ACL, która implementuje politykę, ale także minimalizuje otwarcia przez zaporę. Jeśli to możliwe, oznacza to zezwalanie na połączenia tylko z jednym serwerem wewnętrznym lub co najwyżej z kilkoma serwerami wewnętrznymi.

Administrator zapory powinien zawsze wybierać regułę ACL, która implementuje politykę, ale także minimalizuje otwarcia przez zaporę

ZABEZPIECZ WSZYSTKIE POŁĄCZENIA

Ostatnia zasada, zasada 3, to nie zezwalaj na WSZYSTKIE połączenia. Ta reguła implementuje domyślne zachowanie zapory sieciowej SPI dla połączeń inicjowanych zewnętrznie. Wszystkie połączenia, które nie są wyraźnie dozwolone przez wcześniejsze reguły ACL, są wyraźnie odrzucane. Zauważ, że podczas gdy reguły ACL ogólnie określają wyjątki od zachowania domyślnego, ostatnia reguła określa zachowanie domyślne. Jeśli pakiet nie podlega wyjątkowi i osiągnie ostateczną regułę, zaimplementowane zostanie zachowanie domyślne. W tej dyskusji zauważyliśmy, że (1) istnieje zachowanie domyślne i (2) listy kontroli dostępu zezwalają na wyjątki. Mogło to brzmieć tak, jakby były zaangażowane dwa procesy. W rzeczywistości jest tylko jeden. Zapora sieciowa SPI po prostu zawsze wykonuje listę ACL. Początkowo istnieje tylko jedna reguła, która określa zachowanie domyślne, więc zachowanie domyślne jest wykonywane automatycznie. Później administrator zapory doda reguły wyjątków.

TEST CXLIV

a. Na co ogólnie zezwalają listy ACL przychodzące w przypadku zapór sieciowych z inspekcją pakietów ze stanem?

b. Co ogólnie uniemożliwiają wychodzące listy ACL w zaporach SPI?

c. Co oznaczają dobrze znane numery portów?

d. Czy rysunek 6-10 jest listą ACL dla filtrowania ruchu przychodzącego lub filtrowania ruchu wychodzącego?

e. Dlaczego reguła 2 na rysunku 6-10 jest bezpieczniejsza niż reguła 1?

f. Która reguła na liście ACL na rysunku 6-10 reprezentuje domyślne zachowanie zapór SPI w przypadku prób otwarcia połączenia przychodzącego?

a. Czy podczas filtrowania przychodzącego i wychodzącego zapora sieciowa SPI zawsze uwzględnia swoje reguły ACL, gdy nadchodzi nowy pakiet, który próbuje otworzyć połączenie?

b. Czy podczas filtrowania przychodzącego i wychodzącego zapora sieciowa SPI zawsze uwzględnia swoje reguły ACL, gdy nadchodzi nowy pakiet, który nie próbuje otworzyć połączenia? (Odpowiedź nie została wyraźnie udzielona w tej sekcji.)

Perspektywa zapór sieciowych SPI

NISKA CENA

Chociaż decyzja, czy zezwolić na połączenia, jest nieco skomplikowana, na rysunku 6-5 widzieliśmy, że większość pakietów nie jest próbami otwarcia połączenia. Są to raczej kolejne pakiety w rozpoznanym połączeniu. W przypadku zdecydowanej większości pakietów firewall inspekcji pakietów przeprowadza proste wyszukiwanie w tabeli i natychmiast decyduje, czy przepuścić, czy odrzucić pakiet. (Nie ma potrzeby uwzględniania reguł ACL, jak ma to miejsce w przypadku prób otwarcia połączenia.) Jest to szybkie i dlatego niedrogie.

BEZPIECZEŃSTWO

Brak zaawansowanego badania poza sprawdzeniem, czy pakiet jest częścią połączenia, może wydawać się poważnym ograniczeniem. Jednak w praktyce ataki inne niż ataki w warstwie aplikacji rzadko przechodzą przez zaporę SPI, chyba że administrator utworzy niepoprawną listę ACL. Ponadto, jak zauważyliśmy wcześniej, zapory sieciowe SPI mogą wykraczać poza kontrolę stanową i wdrażać inne zabezpieczenia.

PRZEWAGA

Połączenie wysokiego bezpieczeństwa i niskiego kosztu sprawia, że firewalle SPI są niezwykle popularne. W rzeczywistości, zauważyliśmy wcześniej, że prawie wszystkie główne firewalle graniczne wykorzystują obecnie inspekcję pakietów ze stanem.

TEST CXLV

a. Dlaczego zapory sieciowe z inspekcją pakietów są niedrogie?

b. Czy w praktyce są dość bezpieczne?

c. Czy zapory sieciowe SPI są ograniczone do filtrowania SPI?

d. Z jakiego mechanizmu inspekcji zapory korzystają dziś prawie wszystkie główne zapory graniczne?

TŁUMACZENIE ADRESU SIECIOWEGO

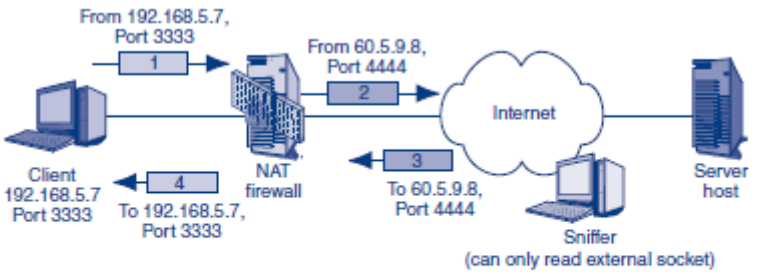
Przyjrzymy się kilku metodom filtrowania, których używają zapory ogniowe do podejmowania decyzji o przepuszczeniu/odrzuceniu pakietów przychodzących. Istnieje jednak jedna technika stosowana w kilku typach zapór ogniowych, która w rzeczywistości nie filtruje pakietów, ale skutecznie zapewnia dużą ochronę. To jest translacja adresów sieciowych (NAT). Jest stosowany w zaporach sieciowych, które wykorzystują różne rodzaje metod badania jako drugi rodzaj ochrony.

Sniffery

Rysunek pokazuje, że hakerzy czasami mogą umieszczać sniffery poza sieciami korporacyjnymi. Gdy pakiety z tych sieci korporacyjnych przechodzą przez sniffer, sniffer przechwytuje je i odnotowuje źródłowe adresy IP i numery portów. Dzięki temu atakujący może dowiedzieć się o adresach IP hostów w sieci i numerach otwartych portów na serwerach bez wysyłania pakietów sondujących. Sniffer będzie mógł wysyłać pakiety ataków na te adresy IP i numery portów.

OPERACJA NAT

Rysunek ilustruje, w jaki sposób proces zwany translacją adresów sieciowych (NAT) może udaremniać sniffery.



Translation table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	3333	60.5.9.8	4444
...	...	...	...

TWORZENIE PAKIETU

Najpierw klient wewnętrzny wysyła pakiet do serwera zewnętrznego. Ten pakiet zawiera prawdziwy adres IP klienta 192.168.5.7. Przenoszony datagram UDP lub segment TCP ma efemeryczny numer portu 3333. (W systemie Windows klienci używają efemerycznych numerów portów z zakresu od 1024 do 4999). Jest to gniazdo źródłowe 192.168.5.7:3333.

TŁUMACZENIE ADRESÓW SIECI I PORTÓW

Zapora NAT przechwytuje cały ruch wychodzący i zastępuje źródłowe adresy IP i źródłowe numery portów zewnętrznymi (stand-in) adresami IP i numerami portów. W tym przypadku zewnętrzny adres IP to 60.5.9.8, a numer portu zastępczego to 4444. Zatem gniazdo zastępcze w pakiecie wychodzącym to 60.5.9.8:4444. Zapora NAT wysyła następnie pakiet do serwera zewnętrznego.

TABELA TŁUMACZEŃ

Zapora NAT umieszcza również gniazdo wewnętrzne i gniazdo zewnętrzne w tabeli translacji.

PAKIET ODPOWIEDZI

Gdy serwer odpowie, wyśle pakiet do docelowego adresu IP 60.5.9.8 i docelowego portu 4444.

PRZYWRÓCENIE

Zapora NAT zauważa, że w jej tablicy translacji istnieje gniazdo 60.5.9.8:4444. Zastępuje zewnętrzny docelowy adres IP i numer portu adresami 192.168.5.7 i 3333. Zapora wysyła ten pakiet do komputera klienckiego.

OCHRONA

Sniffer nie może nauczyć się wewnętrznych adresów IP ani numerów portów, więc nie może wykorzystać tych informacji do przeprowadzania ataków (chyba że może działać natychmiast, co jest rzadkością). Ponadto sondy skanujące sieć są automatycznie odrzucane, ponieważ adresy IP i numery portów nie będą znajdować się w tabeli translacji.

Perspektywa NAT

NAT/PAT

Chociaż omawiane przez nas zapory sieciowe nazywane są zaporami NAT, tłumaczą one zarówno adresy sieciowe (adresy IP), jak i adresy portów. Dlatego wydaje się właściwe nazywać je firewallami NAT/PAT. Robi się to rzadko, ale ważne jest, aby zrozumieć, że NAT nie tylko tłumaczy sieciowe adresy IP, ale także numery portów.

PRZEZROCZYSTOŚĆ

NAT jest przezroczysty zarówno dla hosta wewnętrznego, jak i zewnętrznego. Ani klient, ani serwer nie wiedzą, że NAT jest wykonywany. W ogóle nie muszą zmieniać swojego sposobu działania.

PRZEJAZD NAT

Niestety, niektóre protokoły mają problemy z NAT. Należą do nich tak szeroko stosowane aplikacje, jak VoIP i tak ważne protokoły bezpieczeństwa, jak IPsec. VoIP tworzy nowy numer portu dla konwersacji po nawiązaniu połączenia administracyjnego, a IPsec wymaga prawdziwych wewnętrznych adresów IP. Chociaż aplikacje zezwalające na przechodzenie przez NAT, które nie zostały zaprojektowane do pracy z NAT-em, są możliwe, istnieje kilka metod przechodzenia przez NAT i wszystkie mają ograniczenia.

Wybór i używanie ich może być skomplikowane.

TEST CXLVI

a. Kiedy używany jest NAT, dlaczego sniffery nie mogą dowiedzieć się niczego o wewnętrznych adresach IP hostów wewnętrznych?

b. Dlaczego NAT zatrzymuje skanowanie sond?

c. Dlaczego przechodzenie przez NAT jest konieczne?

dD. Czy łatwo wybrać metodę przechodzenia przez NAT?

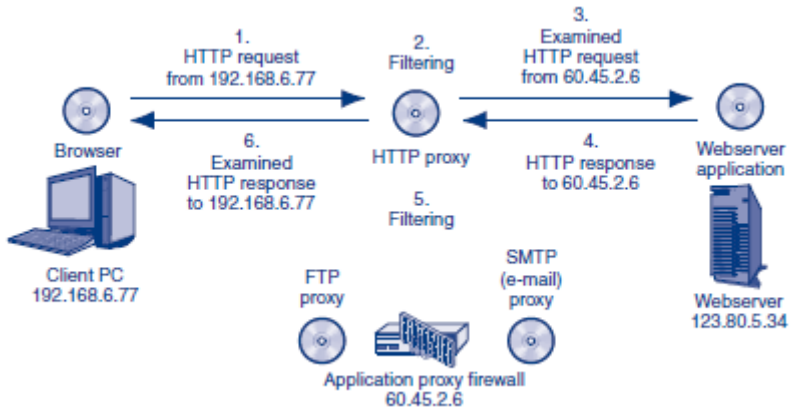
ZAPORY PRZECIWPOŻAROWEJ APLIKACJI I FILTROWANIE TREŚCI

Ani statyczne zapory filtrujące pakiety, ani zapory stanowe inspekcji pakietów nie sprawdzają komunikatów aplikacji. Jest to niefortunne, ponieważ komunikaty aplikacji zawierają informacje przydatne do wykrywania wielu rodzajów ataków. Zapory proxy aplikacji eliminują to niedopatrzenie, jawnie filtrując komunikaty warstwy aplikacji.

Działanie zapory serwera proxy aplikacji

SZCZEGÓŁY OPERACYJNE

Rysunek przedstawia działanie zapory proxy aplikacji.



Należy zauważyć, że zapora serwera proxy aplikacji sprawdza zawartość aplikacji w całym ruchu między klientami i serwerami. W tym przypadku klient jest wewnętrzny, a serwer zewnętrzny. Jest to interakcja HTTP, więc program proxy HTTP na zaporze proxy aplikacji wykonuje filtrowanie.

W tym celu program proxy HTTP nawiązuje połączenia HTTP zarówno z klientem, jak i serwerem WWW. Dla klienta program proxy działa jak serwer WWW. Dla serwera WWW program proxy HTTP działa jak klient przeglądarki. Za każdym razem, gdy nadchodzi pakiet, zapora proxy aplikacji sprawdza zawartość warstwy aplikacji. Dokładniej, zbiera wszystkie segmenty komunikatu aplikacji, jeśli komunikat aplikacji jest pofragmentowany, a następnie sprawdza zawartość. Jeśli nie ma problemu, zapora serwera proxy aplikacji przekazuje komunikat aplikacji dalej.

PROGRAMY PROXY APLIKACJI KONTRA ZAPORY APLIKACYJNE PROXY

Serwery proxy aplikacji używają przekazywania specyficznego dla aplikacji, w którym działają zarówno jako klient, jak i host, gdy nadchodzą pakiety. W konsekwencji zapora wymaga oddzielnego programu proxy aplikacji dla każdego protokołu aplikacji, jak pokazano na rysunku 6-13.

INTENSYWNA OBRÓBKA EKSPLOATACYJNA

Utrzymywanie dwóch połączeń dla każdej pary klient/serwer wymaga dużego nakładu przetwarzania. Z tego powodu zapory proxy aplikacji mogą obsługiwać tylko ograniczoną liczbę par klient/serwer. W związku z tym zapory proxy aplikacji nie mogą być używane jako zapory na granicach głównych. Po prostu nie mogli poradzić sobie z obciążeniem ruchem.

TYLKO NIEKTÓRE APLIKACJE MOGĄ BYĆ PRZEKAZYWANE

Oprócz powolnego działania na obsługiwany pakiet, zapory aplikacji proxy mają jeszcze jedno poważne ograniczenie. Tylko kilka aplikacji może być skutecznie proxy. W przypadku większości aplikacji nie ma określonych wzorców, które można filtrować, ani protokołów, które można wymusić. W rzeczywistości większość zapór proxy aplikacji obsługuje protokół HTTP lub SMTP.

DWA WSPÓLNE ZASTOSOWANIA

Kiedyś zapory proxy aplikacji były używane jako główne zapory graniczne. Z powodów, które właśnie widzieliśmy, wymagają zbyt dużej mocy obliczeniowej, aby dziś pełnić tę rolę. Jednak zapory proxy aplikacji nigdy nie zniknęły. Rysunek 6-14 pokazuje, że obecnie istnieją dwa popularne zastosowania zapór proxy aplikacji. Pierwszą rolą jest ochrona klientów wewnętrznych przed złośliwymi serwerami zewnętrznymi. Wszystkie połączenia klientów z serwerami zewnętrznymi są udostępniane za pośrednictwem pojedynczej zapory proxy aplikacji. Zapora ta sprawdza zawartość aplikacji wszystkich pakietów przychodzących z serwerów zewnętrznych. Jeśli zapora wykryje niebezpieczną zawartość, odrzuca pakiet. Druga rola dzisiejszych zapór proxy aplikacji polega na umieszczeniu między serwerem wewnętrznym a klientami zewnętrznymi. W takich przypadkach zapora proxy aplikacji chroni pojedynczy serwer. Sprawdza zawartość warstwy aplikacji wszystkich przychodzących żądań klientów pod kątem niebezpiecznego zachowania.

TEST CXLVII

a. Co odróżnia zaporę serwera proxy aplikacji od zapór statycznego filtrowania pakietów i zapór SPI?

b. Rozróżnij programy proxy i zapory proxy aplikacji.

c. Jeśli będziesz używać proxy do czterech różnych aplikacji, ile programów proxy będziesz potrzebować?

d. Ile co najmniej zapór proxy aplikacji będzie potrzebnych?

e. Czy prawie wszystkie aplikacje mogą być proxy?

f. Dlaczego działanie zapory proxy aplikacji wymaga intensywnego przetwarzania?

g. Dlaczego firmy nie używają zapór proxy aplikacji jako głównych zapór granicznych?

h. Jakie są obecnie dwie główne role zapór serwerów proxy aplikacji?

Filtrowanie zawartości aplikacji w zaporach typu Stateful Packet Inspection

Zapory proxy aplikacji nie są jedynymi zaporami, które umożliwiają filtrowanie zawartości aplikacji. Jak zauważa Rysunek 6-15, większość stanowych zapór pakietowych zaczęła uwzględniać filtrowanie zawartości aplikacji — często te same typy filtrowania zawartości aplikacji, co zapory proxy aplikacji. Zapory sieciowej inspekcji pakietów nie muszą implementować operacji przekazywania, tak jak robią to zapory aplikacyjne. Pozwala to zaporom sieciowym SPI na bardziej ekonomiczne dodawanie filtrowania zawartości aplikacji. Jednak inspekcja aplikacji zapory SPI nie obejmuje niektórych zabezpieczeń oferowanych przez zapory proxy aplikacji, które zostały omówione w następnej sekcji. Co najważniejsze, inspekcja aplikacji SPI nie zapewnia ważnych automatycznych zabezpieczeń

oferowanych przez zapory proxy aplikacji - ukrywanie wewnętrznych adresów IP, niszczenie nagłówków i wierność protokołu. Ogólnie rzecz biorąc, możliwość filtrowania zawartości aplikacji znacznie zwiększa użyteczność zapór sieciowych SPI, dodatkowo umacniając ich pozycję jako głównego typu zapór korporacyjnych w dzisiejszych czasach.

TEST CXLVIII

a. Czy zapory z inspekcją pakietów ze stanową inspekcją pakietów automatycznie filtrują zawartość aplikacji? Wyjaśniać.

b. Czy mają niską prędkość działania przekaźnika?

c. Jakie trzy zalety mają zapory proxy aplikacji w zakresie ochrony, których nie mają zapory SPI z inspekcją treści?

d. Dlaczego zapory filtrujące zawartość SPI są szybsze niż zapory proxy aplikacji?

Filtrowanie zawartości aplikacji dla HTTP

Zauważyliśmy, że zapory proxy aplikacji filtrują zawartość komunikatów aplikacji. Specyfika tego filtrowania różni się w zależności od aplikacji. Wspomnimy tylko o kilku akcjach filtrowania, które mogą wykonać serwery proxy aplikacji HTTP. Istnieją inne akcje filtrowania dla HTTP, SMTP i innych typów aplikacji.

Ochrona klienta

Jak wspomniano wcześniej, wiele firm używa zapór proxy aplikacji do ochrony klientów wewnętrznych przed złośliwymi serwerami zewnętrznymi. W przypadku protokołu HTTP programy proxy mogą wykonywać kilka rodzajów filtrowania. Wymienimy tylko trzy:

• Serwer proxy może sprawdzić adres URL i porównać go z tabelą adresów URL z czarnej listy, które są znanymi witrynami phishingowymi, pornograficznymi lub rekreacyjnymi.

• Serwer proxy może sprawdzać skrypty na pobranych stronach internetowych, porzucając te strony, jeśli skrypty wydają się złośliwe lub jeśli zasady zabraniają niektórych typów skryptów lub wszystkich skryptów.

• Serwer proxy może sprawdzić typ MIME w komunikacie odpowiedzi HTTP. Typ MIME opisuje typ pliku pobranego w wiadomości. Niektóre typy plików MIME mogą być dozwolone lub odrzucane przez zasady.

Serwer proxy HTTP może również badać pakiety wychodzące od klienta wewnętrznego do zewnętrznego serwera WWW w celu wykrycia niewłaściwego zachowania klienta. Na przykład serwer proxy może sprawdzić metodę w nagłówku adresu URL. Metoda HTTP GET jest ogólnie bezpieczna, ponieważ służy do pobierania plików. Jednak metoda POST może wysyłać pliki z firmy. Wiele firm odrzuca każdy komunikat żądania HTTP, który używa metody POST, aby zapewnić zapobieganie ekstruzji.

Zabezpieczenia serwerów

W przypadku serwerów program proxy HTTP próbuje chronić serwer przed złośliwymi klientami.

• Jak już wspomniano, proxy może sprawdzić metodę w nagłówku adresu URL. Metoda POST umożliwi klientom przesyłanie plików na serwer WWW. Może to być zabronione przez zasady uniemożliwiające

klientom przesyłanie złośliwego oprogramowania, pornografii lub innego rodzaju nieulepszonej zawartości.

• Serwer proxy HTTP może również odfiltrować komunikaty żądań HTTP, które wydają się zawierać ataki typu SQL injection. (O tym typie ataku dowiemy się w następnym rozdziale.)

Strategia i technologia bezpieczeństwa

Tor - trasowanie cebuli

W czerwcu 2010 r. Wired.com poinformował, że aktywista WikiLeaks i jej znany założyciel Julian Assange wykorzystali węzeł wyjściowy w sieci Tor, aby zebrać tajemnice rządów i korporacji. Dokumenty rzekomo pochodziły od chińskich hakerów, którzy ukradli dane. Dokumenty zostały następnie wykorzystane do promocji WikiLeaks. Assange zaprzeczył temu twierdzeniu, mówiąc The Register: „Przypisanie jest błędne. Fakty dotyczą śledztwa w sprawie chińskiego szpiegostwa z 2006 roku, w które zaangażowany był jeden z naszych kontaktów na WikiLeaks". Amerykańska firma ochroniarska Tiversa twierdziła, że WikiLeaks szukał również tajnych informacji za pomocą źle skonfigurowanych komputerów, które korzystały z usług P2P, takich jak LimeWire i Kazaa. Te zebrane dane miały następnie pochodzić od sygnalistów lub innych aktywistów. Temu również zaprzeczyła WikiLeaks.

TOR DLA ANONIMOWOŚCI

Skutecznym sposobem na wysyłanie i odbieranie danych przez Internet przez sygnalistów i dziennikarzy jest korzystanie z routingu cebulowego. Popularną implementacją routingu cebulowego jest sieć Tor (TorProject.org). Sieć Tor zapewnia prawie całkowicie anonimowy dostęp do Internetu. Wykorzystuje szereg zaszyfrowanych węzłów przekaźnikowych do przesyłania pakietów od nadawców do odbiorców. Tor jest również przydatny, jeśli mieszkasz lub odwiedzasz kraj, który zabrania dostępu do określonych stron internetowych lub usług, takich jak czat lub wiadomości błyskawiczne. Może być używany przez dysydentów politycznych do przekazywania poufnych materiałów. Korporacje mogą czerpać korzyści z używania sieci Tor, ukrywając wszystkie informacje, które można uzyskać z analizy wzorców ruchu do i z firmy. Konkurenci mogą monitorować ruch pod kątem wyszukiwanych haseł, wizyty w Urzędzie Patentów i Znaków Towarowych USA, komunikację między niektórymi producentami i tak dalej. Wszystko to może dostarczyć wskazówek dotyczących poufnej strategii firmy lub rozwoju nowych produktów. Korzystanie z sieci Tor może zapobiec tego rodzaju szpiegostwu korporacyjnemu.

JAK DZIAŁA TOR

Krok 1

Po zainstalowaniu klienta Tor, użytkownik zażądałby listy wszystkich węzłów Tora z serwera katalogowego. Węzły Tora będą używane do przekazywania danych między nadawcami i odbiorcami. Komputer użytkownika może również pełnić rolę węzła przekazującego dla cudzego transferu danych.

Krok 2

Klient Tora następnie losowo wybierałby ścieżkę od lokalnego hosta do komputera docelowego. W tym przypadku komputerem docelowym jest serwer WWW. Klient Tor buduje serię zaszyfrowanych łączy między każdym węzłem Tora. Każdy węzeł Tora widzi tylko następny przeskok na ścieżce. Nie widzi inicjującego użytkownika, docelowego serwera internetowego ani żadnych węzłów Tora poza pojedynczym przeskokiem. Cały ruch jest w pełni szyfrowany, gdy jest przekazywany z węzła do węzła.

Krok 3

Węzeł Tora, który kończy się jako ostatni przeskok przed dotarciem do docelowego serwera internetowego, jest znany jako węzeł wyjściowy. Połączenie między węzłem wyjściowym a docelowym serwerem internetowym nie jest szyfrowane. To jest punkt, w którym ruch sieciowy Tora może być monitorowany. W rzeczywistości z punktu widzenia serwera WWW cały ruch wygląda tak, jakby pochodził z węzła wyjściowego. Aby zapobiec przechwyceniu lub monitorowaniu ruchu w węźle wyjściowym, użytkownicy powinni korzystać z połączeń SSL lub VPN. Zapewni to szyfrowanie typu end-to-end. Sieć Tor nie zapewnia automatycznie szyfrowania typu end-to-end. Następnym razem, gdy użytkownik nawiąże nowe połączenie z tym samym serwerem WWW, zostanie utworzona alternatywna ścieżka. Klient Tora wybrałby zupełnie nową ścieżkę i prawdopodobnie nowy węzeł wyjściowy. Ruch z tego samego oryginalnego klienta wydaje się pochodzić z innego węzła wyjściowego. Serwer sieciowy i każdy, kto przechwytuje pakiety na trasie, nie byłby w stanie zidentyfikować klienta, z którego pochodzi.

USŁUGI UKRYTE I DNS

W tym przykładzie Tor może ukryć tożsamość użytkownika zgłaszającego żądanie sieciowe. Może jednak również ukryć serwer WWW. Korzystając z usług ukrytych, sieć Tor może łączyć użytkowników i usługi sieciowe bez znajomości tożsamości użytkownika lub lokalizacji serwera WWW. Użytkownicy mogą publikować treści bez obaw o represje lub cenzurę. Tor zapewnia również własny wewnętrzny DNS. Nazwy hostów można rozwiązać, wysyłając żądanie DNS przez węzeł wyjściowy. To ma tę zaletę anonimowości wszystkich żądań DNS.

Inne zabezpieczenia

Oprócz filtrowania zawartości wiadomości warstwy aplikacji istnieją trzy inne zabezpieczenia oferowane przez zapory proxy aplikacji.

• Ukrywanie wewnętrznego adresu IP - Podobnie jak NAT, zapory proxy aplikacji ukrywają adresy IP hostów wewnętrznych. Pakiety opuszczające firmę mają jako źródłowe adresy IP adres IP zapory proxy aplikacji, a nie adresy IP hostów wewnętrznych. Może to uniemożliwić sniffery pakietów i mapowanie sieci.

• Zniszczenie nagłówka - pamiętaj, że gdy pakiet dociera do zapory proxy aplikacji, program proxy sprawdza komunikat warstwy aplikacji. W tym celu program proxy dekapsuluje komunikat aplikacji. Czyniąc to, odrzucanagłówki warstwy internetowej i transportowej w przychodzącym pakiecie. Jeśli atakujący manipulował polami w nagłówkach Internetu lub warstwy transportowej, aby spowodować problemy, zniszczenie nagłówka automatycznie pokonuje te metody ataku. Jeśli zapora proxy aplikacji przekaże komunikat warstwy aplikacji, umieszcza ją w nowym komunikacie transportowym i nowym pakiecie internetowym. Atakujący nie ma możliwości wpływania na zawartość pól w tych nowych nagłówkach.

• Wierność protokołu - podczas działania program proxy aplikacji działa jak serwer dla klienta i jak klient dla serwera. Załóżmy, że klient i serwer próbują obejść zapory sieciowe, używając portu 80 - dobrze znanego portu HTTP - do obsługi innego programu, takiego jak komunikator internetowy, którego firma zabroniła. W takich przypadkach połączenia z zaporą serwera proxy aplikacji zakończą się niepowodzeniem, ponieważ program proxy HTTP będzie oczekiwał interakcji HTTP i ich nie odbierze. Połączenia zostaną automatycznie zerwane.

TEST CXLIX

a. Jakie akcje filtrowania zostały wymienione w celu ochrony klientów przed złośliwymi serwerami sieciowymi?

b. O jakiej akcji filtrowania wspomniano, aby zapobiec niewłaściwemu zachowaniu klienta wewnętrznego w HTTP?

c. Jakie dwie akcje filtrowania zostały wymienione w celu ochrony serwerów WWW przed złośliwymi klientami?

d. Jakie trzy automatyczne zabezpieczenia zapewniają zapory proxy aplikacji ze względu na sposób ich działania?

SYSTEMY WYKRYWANIA WŁAMANIA I ZAPOBIEGANIA WŁAMANIU

Jak wspomniano na początku, zaawansowanie filtrowania zapory jest ograniczone przez moc obliczeniową zapór. Najwcześniejsze zapory mogły wykonywać tylko proste statyczne filtrowanie pakietów. Wraz ze wzrostem mocy obliczeniowej nastąpiła inspekcja pakietów stanowych , a następnie stały się dominujące. Dzisiaj SPI zaczyna być kwestionowany przez nowy rodzaj filtrowania, który nazywa się filtrowaniem systemu zapobiegania włamaniom (IPS). Ta nowa metoda filtrowania jest w stanie wykrywać i powstrzymywać ataki, które są bardziej wyrafinowane niż wcześniejsze formy filtrowania, w tym SPI. Tylko czas pokaże, czy filtrowanie IPS może stać się dominującą metodą filtrowania dla zapór granicznych.

Systemy wykrywania włamań

Filtrowanie systemów zapobiegania włamaniom wyrosło z wcześniejszych technologii - systemów wykrywania włamań. Wiele domów i samochodów ma alarmy antywłamaniowe, które włączają się w przypadku podejrzanego ruchu. Podobnie wiele korporacji instaluje systemy wykrywania włamań (IDS), które badają strumienie pakietów w poszukiwaniu podejrzanych działań wskazujących na możliwe ataki. Jeśli system IDS wykryje pozornie poważny atak, może wysłać komunikat alarmowy do administratora bezpieczeństwa. (Jeśli atak nie wydaje się zbyt poważny, system IDS po prostu go zarejestruje).

ZAPORY KONTRA IDSS

Tradycyjnie istniało silne rozróżnienie między zaporami ogniowymi a systemami IDS. Zapory sieciowe zatrzymują możliwe do udowodnienia pakiety ataków. Jeśli pakiet nie jest możliwym do udowodnienia pakietem ataku, zapora nie może go odrzucić. Z kolei IDS identyfikują podejrzane pakiety, które mogą, ale nie muszą być częścią ataków. Dla porównania, policjant może kogoś aresztować tylko wtedy, gdy ma prawdopodobną przyczynę (stosunkowo wysoki standard dowodu). Jeśli ktoś zachowuje się podejrzanie, funkcjonariusz policji może tylko przeprowadzić dochodzenie.

Zapory sieciowe zatrzymują możliwe do udowodnienia pakiety ataków. Jeśli pakiet nie jest możliwym do udowodnienia pakietem ataku, zapora nie może go odrzucić. Z kolei IDS identyfikują podejrzane pakiety, które mogą, ale nie muszą być częścią ataków.

FAŁSZYWE POZYTYWY (FAŁSZYWE ALARMY)

Przyjrzymy się IDS bardziej szczegółowo w rozdziale 10. W tym rozdziale skupimy się na dwóch poważnych ograniczeniach IDS. Po pierwsze, podobnie jak wiele alarmów domowych i samochodowych, IDS mają tendencję do generowania zbyt wielu fałszywych alarmów, które w języku IDS są fałszywymi alarmami. Podobnie jak mały chłopiec, który zbyt wiele razy płakał wilkiem, IDS są

zwykle ignorowane po tym, jak wyczerpani pracownicy ochrony otrzymują zbyt wiele fałszywych alarmów.

Możliwe jest dostrojenie IDS w celu zmniejszenia liczby fałszywych alarmów do znośnego stopnia. Wiele zasad nie ma sensu w konkretnej organizacji. Na przykład, jeśli reguła identyfikuje pakiet, który byłby niebezpieczny, gdyby został wysłany do określonego typu serwera uniksowego, a organizacja nie ma serwerów uniksowych tego typu, reguła może zostać usunięta, aby wyeliminować generowane przez nią alarmy. Jednak strojenie wymaga dużego nakładu pracy. Systemy IDS rejestrują wszystkie podejrzane działania, ale tworzą alarmy tylko dla niektórych podejrzanych działań. Oprócz usunięcia bezsensownych reguł, strojenie może zmniejszyć liczbę sygnatur ataków, które generują alarmy. Jednak, chociaż zmniejsza to liczbę alarmów, powoduje również, że administratorzy bezpieczeństwa muszą regularnie czytać pliki dziennika w celu wyłapania ataków, które nie są już alarmowane. Istnieje wiele zasad i każdy musi być bardzo dokładnie rozważony. W związku z tym strojenie jest tak drogie i wyczerpujące zasoby, że niewiele organizacji wdraża je w pełni.

WYMAGANIA DOTYCZĄCE CIĘŻKIEGO PRZETWARZANIA

Innym problemem jest to, że metodologie IDS są bardzo intensywne pod względem przetwarzania. Ogranicza to natężenie ruchu, które mogą filtrować IDS.

Głęboka inspekcja pakietów.

Jednym z powodów intensywności przetwarzania IDS jest to, że IDS nie tylko sprawdzają kilka pól w pakiecie. Używają głębokiej inspekcji pakietów, która sprawdza wszystkie pola w pakiecie, w tym nagłówek IP, nagłówek TCP lub UDP oraz komunikat aplikacji. Wielu ataków nie można powstrzymać, jeśli zapora przegląda tylko zawartość aplikacji lub tylko nagłówki warstwy internetowej i transportowej.

Analiza strumienia pakietów.

IDS muszą również filtrować strumienie pakietów, a nie pojedyncze pakiety. Wiele ataków nie wynika z pojedynczych pakietów. Na przykład pojedyncza wiadomość echa ICMP nie jest zbyt diagnostyczna, ale strumień wiadomości echa ICMP próbujących różnych adresów IP jest bardzo silnym sygnałem, że firma przeprowadza systematyczne skanowanie.

Bardziej subtelnie, zawartość aplikacji zostanie rozłożona na kilka pakietów. Aby przeanalizować zawartość aplikacji, IDS będzie musiał ponownie złożyć oryginalne komunikaty aplikacji — czasami są to kolejne komunikaty aplikacji. Badanie strumieni pakietów zamiast pojedynczych pakietów pod kątem niebezpiecznych wzorców jest bardzo intensywne w przetwarzaniu.

TEST CL

a. Rozróżnij firewalle i IDS.

b. Dlaczego alarmy IDS są często problemem?

c. Co to jest fałszywy alarm?

d. Z jakich dwóch typów filtrowania korzystają systemy IDS?

e. Dlaczego głęboka inspekcja pakietów jest ważna?

f. Dlaczego przetwarzanie głębokiej inspekcji pakietów jest intensywne?

g. Dlaczego analiza strumienia pakietów jest ważna?

h. Dlaczego analiza strumienia pakietów powoduje duże obciążenie IDS?

Systemy zapobiegania włamaniom

Jak już wspomniano, systemy zapobiegania włamaniom wyrosły z przetwarzania IDS. Jednak chociaż używają metod filtrowania IDS, systemy zapobiegania włamaniom (IPS) faktycznie zatrzymują niektóre rodzaje ataków, zamiast jedynie je identyfikować i generować alarmy, tak jak robią to systemy IDS. Dlatego nazywa się je systemami zapobiegania włamaniom.

Chociaż wykorzystują metody filtrowania IDS, systemy zapobiegania włamaniom (IPS) faktycznie zatrzymują niektóre rodzaje ataków, zamiast jedynie je identyfikować i generować alarmy, jak to robią IDS.

ASICS DLA SZYBSZEGO PRZETWARZANIA

Jak wspomniano wcześniej, filtrowanie IDS/IPS wymaga bardzo intensywnego przetwarzania. Najważniejszym osiągnięciem prowadzącym do IPS było pojawienie się układów scalonych specyficznych dla aplikacji (ASIC), które mogą filtrować sprzętowo. Filtrowanie sprzętowe jest znacznie szybsze niż filtrowanie programowe, umożliwiając korzystanie z IPS nawet przy dużym natężeniu ruchu.

SPEKTRUM ZAUFANIA IDENTYFIKACJI ATAKU

Kiedy doświadczeni specjaliści ds. bezpieczeństwa, którzy pracowali z IDS, słyszą o IPS, zwykle na początku wzdrygają się. Biorąc pod uwagę liczbę fałszywych alarmów generowanych przez systemy IDS, myśl o umożliwieniu tym niewiarygodnym mechanizmom filtrowania faktycznego zatrzymania ruchu jest głęboko niepokojąca. W praktyce jednak zawsze istnieje spektrum pewności identyfikacji ataku w wykrywaniu włamań. Niektóre ataki, zwłaszcza ataki DoS, można zidentyfikować z bardzo wysokim stopniem pewności. W rzeczywistości wiele zapór granicznych już dziś identyfikuje i powstrzymuje ataki DoS, niezależnie od ich głównej technologii filtrowania. Inne ataki nie mogą być identyfikowane z tak dużą pewnością.

TEST CLI

a. Rozróżnij systemy IDS i IPS.

b. Dlaczego spektrum ufności identyfikacji ataku jest ważne przy podejmowaniu decyzji, czy pozwolić dostawcom usług internetowych na powstrzymanie określonych ataków?

Działania IPS

Co robią dostawcy usług internetowych, gdy wykryją podejrzany ruch na wyższym końcu spektrum ufności identyfikacji ataku?

UPUSZCZANIE PAKIETÓW

W wielu przypadkach IPS odrzuca pakiety ataków, działając jak tradycyjna zapora ogniowa. Jest to niebezpieczne, ale bardzo skuteczne.

OGRANICZENIE RUCHU

W innych przypadkach IPS ogranicza podejrzany ruch do pewnego procentu całkowitej przepustowości. Ograniczenie przepustowości może zapewnić, że nawet jeśli ruch wymiany plików peer-to-peer i inny nielegalny ruch nie może zostać zidentyfikowany z precyzją i odrzucony, ten niepożądany ruch przynajmniej nie spowoduje przeciążenia sieci.

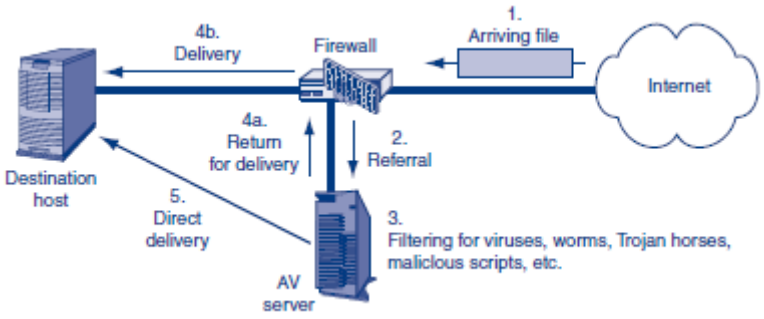
TEST CLII

a. Jakie dwie czynności mogą podjąć dostawcy usług internetowych, gdy zidentyfikują atak?

b. Który może być najskuteczniejszy?

FILTROWANIE ANTYWIRUSOWE I JEDNOLITE ZARZĄDZANIE ZAGROŻENIAMI

Zapory zwykle nie wykonują filtrowania antywirusowego. Jednak zapory sieciowe i serwery filtrujące antywirusy ściśle ze sobą współpracują. Wszyscy główni dostawcy zapór sieciowych mają protokoły do pracy z serwerami antywirusowymi. Rysunek ilustruje tę dynamikę.



Kiedy pakiet dociera do zapory, zapora decyduje, co z nim zrobić. (Właściwie, przed podjęciem decyzji, co z nimi zrobić, zapora może łączyć wiele pakietów w wiadomość e-mail, stronę internetową lub obraz.) Aby podjąć decyzję, zapora sprawdzi swoją bazę reguł zasad. Jeśli regułą dla tego typu obiektu jest przekazanie obiektu do serwera antywirusowego, zrobi to zapora. Serwer antywirusowy zbada obiekt. To filtrowanie wykracza poza wirusy. Wyszukuje również robaki, konie trojańskie, spam, phishing, rootkity, złośliwe skrypty i inne złośliwe oprogramowanie. Po przefiltrowaniu, jeśli serwer antywirusowy nie usunie obiektu, zwraca obiekt do zapory sieciowej w celu przekazania, lub serwer antywirusowy sam przekazuje obiekt do odbiorcy.

Niektóre zapory wykorzystują zarówno tradycyjne metody filtrowania zapory, jak i filtrowanie antywirusowe. Jak wspomniano pokrótce na początku rozdziału, są one nazywane zaporami ogniowymi UTM. Chociaż produkty UTM istnieją, te sprzedawane dzisiaj wydają się być dobre w jednej dziedzinie, a brakuje im w innych. Ponadto, biorąc pod uwagę potrzebę stosowania zarówno zapory ogniowej, jak i filtrowania antywirusowego, większość produktów UTM ma moc obliczeniową tylko do wykorzystania w mniejszych firmach lub oddziałach większych firm.

TEST CLIII

a. Jak współpracują ze sobą zapory i serwery antywirusowe?

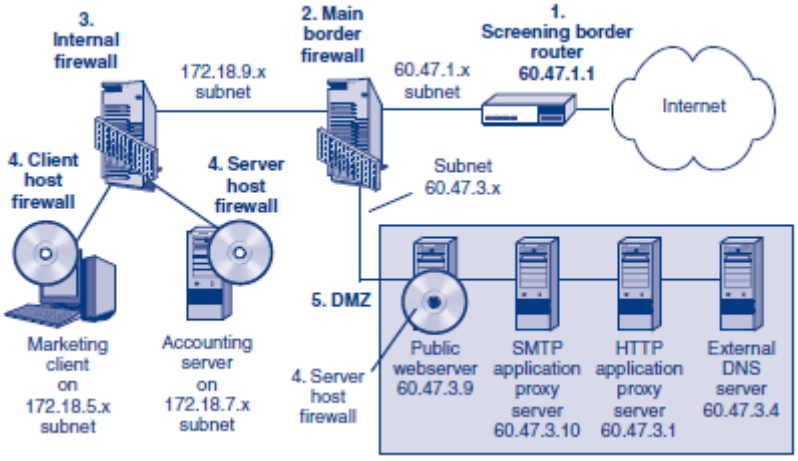
b. Czy serwery antywirusowe ograniczają się do wyszukiwania wirusów? Wyjaśniać.

c. Co może zrobić serwer antywirusowy po wykonaniu filtrowania?

d. Jaki typ zapory zapewnia zarówno tradycyjne filtrowanie zapory, jak i filtrowanie antywirusowe?

ARCHITEKTURY FIREWALLA

Większość firm ma wiele zapór ogniowych, z których każda służy innym celom. Rysunek 6-20 przedstawia reprezentatywną architekturę zapory sieciowej dla jednej dużej firmy.



Rodzaje zapór sieciowych

ZAPORY NA GŁÓWNEJ GRANICY

Zgodnie z oczekiwaniami rysunek przedstawia główną zaporę graniczną (2) w punkcie, w którym sieć firmowa łączy się z Internetem. Jednak pokazuje również kilka innych zapór.

SCREENINGOWE ROUTERY GRANICZNE

Pomiędzy zaporą graniczną a Internetem znajduje się router graniczny witryny (1). Jak wspomniano wcześniej, niektóre firmy umieszczają na routerze oprogramowanie do statycznego filtrowania pakietów i czynią z niego router graniczny screeningu. Ten skriningowy router graniczny zatrzymuje proste, duże ilości ataków i zapewnia, że odpowiedzi na zewnętrzne sondy skanujące nie mogą dotrzeć do zewnętrznego atakującego. Ekonomicznie zmniejsza obciążenie głównej zapory granicznej.

ZAPORY WEWNĘTRZNE

Ponadto rysunek przedstawia wewnętrzną zaporę ogniową (3), która kontroluje ruch przepływający między różnymi częściami sieci wewnętrznej firmy. Na przykład komputery w dziale księgowości mogą mieć możliwość wysyłania pakietów do serwera księgowego, ale pakiety od osób z innych działów do serwera księgowego powinny być zatrzymane. Chociaż Rysunek pokazuje tylko jedną wewnętrzną zaporę ogniową, wiele witryn ma kilka wewnętrznych zapór ogniowych, które oddzielają części sieci według różnych relacji zaufania.

ZAPORY NA HOSTA

Poszczególne hosty - zarówno klienci, jak i serwery - mogą mieć zapory. Zapory graniczne i zapory wewnętrzne są skomplikowane w konfiguracji, ponieważ muszą chronić dużą liczbę połączeń klient-serwer o różnych potrzebach filtrowania. W takich okolicznościach łatwo jest popełnić błąd podczas tworzenia reguły ACL. W przeciwieństwie do tego, typowy serwer ma tylko jedną aplikację lub co najwyżej kilka aplikacji. W takich okolicznościach znacznie łatwiej jest stworzyć odpowiednie reguły ACL. Na przykład zapora sieciowa hosta zwykle zezwala na dostęp zewnętrzny tylko na portach TCP 80 (HTTP) i 443 (HTTP przez SSL/TLS).

OBRONA W GŁĘBI

Korzystanie z zapór granicznych, wewnętrznych i hosta ma jeszcze jedną zaletę. Tworzy obronę dogłębną. Jeśli główna lub wewnętrzna zapora ma błąd konfiguracji ACL, poszczególne hosty będą nadal chronione.

TEST CLIV

a. Dlaczego w architekturze zapory używane są routery screeningowe?

b. Dlaczego pożądane są wewnętrzne zapory sieciowe?

c Dlaczego łatwiej jest tworzyć odpowiednie reguły ACL dla zapór hosta serwera niż dla zapór granicznych?

d. W jaki sposób korzystanie z zapór granicznych, wewnętrznych i hosta zapewnia dogłębną obronę?

Strefa Zdemilitaryzowana

DMZ Na rysunku firewall graniczny jest wieloadresowy, co oznacza, że łączy się z wieloma podsieciami. W tym przypadku jest podłączony do trzech podsieci (tri-homed). Jedna podsieć prowadzi tylko do routera zapory ekranowej (podsieci 60.47.1.x). Inna podsieć (172.18.9.x) prowadzi do sieci wewnętrznej firmy. Trzecia podsieć (60.47.3.x) to strefa zdemilitaryzowana (DMZ). Strefa DMZ to podsieć zawierająca wszystkie serwery i zapory proxy aplikacji, które muszą być dostępne dla świata zewnętrznego. Ponieważ te hosty są dostępne dla atakujących w Internecie, będą narażone na ciągłe ataki. W związku z tym muszą być szczególnie uodpornione na atak.

Strefa zdemilitaryzowana (DMZ) to podsieć zawierająca wszystkie serwery i zapory proxy aplikacji, które muszą być dostępne dla świata zewnętrznego.

IMPLIKACJE DLA BEZPIECZEŃSTWA

Multihoming umożliwia firewallowi granicznemu tworzenie oddzielnych reguł dostępu dla strefy DMZ i podsieci wewnętrznej. Zapora powinna ułatwiać dostęp do strefy DMZ zewnętrznym użytkownikom Internetu. Nie powinno jednak zezwalać na żadne zewnętrznie inicjowane połączenia z Internetu bezpośrednio do wewnętrznych klientów lub serwerów w sieci. Tylko zewnętrznie inicjowane połączenia z hostami w strefie DMZ mają sens, więc tylko one są dozwolone. A co z połączeniami między strefą DMZ a podsiecią wewnętrzną? Niektóre serwery DMZ muszą łączyć się z serwerami wewnętrznymi. Na przykład serwery aplikacji handlu elektronicznego w strefie DMZ mogą być zmuszone do łączenia się z wewnętrznymi bazami danych. Aby podać inny przykład, serwer aplikacji proxy HTTP w strefie DMZ będzie musiał połączyć się z wewnętrzną przeglądarką. Wszystkie połączenia między strefą DMZ a wewnętrzną podsiecią są niebezpieczne. Firmy ograniczają ich liczbę i ściśle kontrolują nieliczne, które są dozwolone. Ogólnie rzecz biorąc, multihoming ułatwia tworzenie reguł kontroli dostępu do hostów publicznych i hostów wewnętrznych.

HOSTY W DMZ

Ogólnie strefy DMZ mają trzy rodzaje hostów.

Serwery publiczne.

Na rysunku strefa DMZ ma publiczny serwer sieciowy (60.47.3.9). Gdyby miał publiczny serwer FTP lub inny publiczny serwer, umieściłby je również w strefie DMZ. Serwery publiczne muszą być dostępne dla klientów w Internecie, a umieszczenie ich w strefie DMZ zmniejsza ryzyko.

Zapory proxy aplikacji.

Oprócz tego, że jest dobrym miejscem dla serwerów publicznych, strefa DMZ jest dobrym miejscem dla zapór proxy aplikacji, które również muszą być połączone ze światem zewnętrznym. Zapory proxy aplikacji umieszczone w strefie DMZ mogą służyć do egzekwowania zasady, zgodnie z którą cała komunikacja ze światem zewnętrznym musi przechodzić przez strefę DMZ. Na rysunku znajdują się dwie zapory proxy aplikacji w strefie DMZ - zapora proxy HTTP i zapora proxy przekaźnika SMTP. Oczywiście możliwe jest uruchamianie programów proxy HTTP i SMTP na tym samym serwerze. Jednak umieszczenie programów proxy na różnych serwerach zwiększa bezpieczeństwo. Jeśli atakujący przejmą jeden serwer, tylko ten program proxy aplikacji zostanie naruszony.

Zewnętrzny serwer DNS.

Strefa DMZ na Rysunku 6-20 zawiera zewnętrzny serwer DNS, 60.47.3.4, który został utworzony w celu uzyskania dostępu dla świata zewnętrznego. Dzięki temu firma może nadać serwerom nazwy hostów w strefie DMZ. Jednak ten zewnętrzny serwer DNS w strefie DMZ zna tylko nazwy hostów i adresy IP hostów w strefie DMZ. W ten sposób osoby atakujące z zewnątrz nie mogą korzystać z serwera DNS w strefie DMZ, aby dowiedzieć się o adresach IP hostów w chronionej wewnętrznej sieci firmy.

TEST CLV

a. Co to jest router wieloadresowy?

b. Co to jest strefa DMZ?

c. Dlaczego firmy korzystają ze stref DMZ?

d. Jakie trzy typy hostów znajdują się w strefie DMZ?

e. Dlaczego firmy umieszczają serwery publiczne w strefie zdemilitaryzowanej?

f. Dlaczego firmy umieszczają zapory proxy aplikacji w strefie DMZ?

g. Jakie nazwy hostów zna zewnętrzny serwer DNS?

h. Dlaczego wszystkie hosty w strefie DMZ muszą być ściśle zahartowane?

ZARZĄDZANIE ZAPORĄ

Zapory nie działają automatycznie. Wymagają starannego planowania, wdrażania i codziennego zarządzania. Bez dużej ilości początkowej i ciągłej pracy związanej z zarządzaniem zapory ogniowe wyglądają imponująco fizycznie, ale zapewniają niewielką ochronę.

Definiowanie zasad zapory

W Części 2 omówiono strategiczne planowanie bezpieczeństwa i planowanie bezpieczeństwa aktywów. Powinny one prowadzić do stworzenia zasad zapory, które są wysokopoziomowymi oświadczeniami, które mają kierować realizatorami zapory. Na przykład zasady zapory mogą wymagać, aby każde połączenie HTTP przychodzące z Internetu było nawiązywane tylko z serwerem w strefie DMZ.

DLACZEGO KORZYSTAĆ Z ZASAD?

Każda zasada zapory musi zostać przetłumaczona na regułę ACL (lub wiele reguł), którą zapora może zrozumieć. Lista kontroli dostępu z wieloma regułami może być trudna do zrozumienia. Jednak lista zasad zapory jest stosunkowo łatwa do zrozumienia. Ponadto może istnieć wiele sposobów spełnienia tej zasady. Gdyby określono metody wdrażania zamiast ogólnej polityki, realizatorzy nie mieliby swobody wyboru najlepszego podejścia do osiągnięcia podstawowego celu, który określiłaby polityka.

PRZYKŁADY ZASAD

Poniżej znajduje się lista niektórych możliwych zasad zapory, z których może korzystać firma.

• Firma zezwoli na wszelki dostęp klientów wewnętrznych do zewnętrznych serwerów internetowych, z wyjątkiem serwerów internetowych znajdujących się na czarnej liście witryn zajmujących się pornografią i innymi problematycznymi tematami.

• Tylko osoby zajmujące się marketingiem powinny mieć dostęp do serwera zawierającego firmowe dane sprzedażowe.

• Wszystkie osoby muszą się uwierzytelnić, zanim będą mogły korzystać z serwera w dziale zasobów ludzkich.

• Cały ruch do serwera inżynierskiego musi być rejestrowany.

• W przypadku niepowodzenia pięciu prób uwierzytelnienia do administratora bezpieczeństwa należy wysłać alert.

TEST CLVI

a. Rozróżnij zasady zapory i reguły ACL.

b. Dlaczego tworzenie zasad zapory jest pożądane w porównaniu do tworzenia listy reguł ACL?

c. Utwórz trzy zasady zapory niewymienione w tekście.

Realizacja

Po zakończeniu planowania nadszedł czas na wdrożenie zasad firmy dotyczących poszczególnych zapór.

UTWARDZANIE ZAPOROWE

Ważne jest, aby chronić same zapory ogniowe przed atakami, ponieważ jeśli atakujący przejmie zaporę, może wyrządzić ogromne szkody.

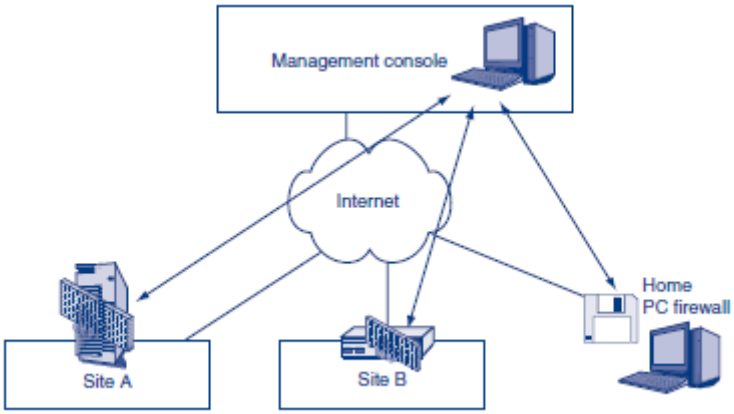
• Urządzenia zapory to gotowe zapory. Firma po prostu instaluje urządzenie między routerem dostępu do Internetu a siecią wewnętrzną. Działanie jest w dużej mierze automatyczne. Urządzenia Firewall są fabrycznie utwardzane.

• Ponadto dostawcy zapór często sprzedają komputery z zaporami, które mają wstępnie utwardzone wersje systemu UNIX lub Windows. Ograniczają one zdolność organizacji do popełniania błędów podczas wzmacniania systemu operacyjnego.

• Jeśli jednak firma kupuje komputer ogólnego przeznaczenia i instaluje samo oprogramowanie zapory, należy podjąć zdecydowane działania w celu wzmocnienia zapory. Ogólne hartowanie komputerowe zostało omówione w następnych dwóch rozdziałach.

CENTRALNE SYSTEMY ZARZĄDZANIA FIREWALLEM

Jeśli firma ma wiele zapór ogniowych, prawdopodobnie użyje centralnego systemu zarządzania zaporą ogniową. Rysunek pokazuje, że sercem tego systemu jest serwer zarządzania zasadami zapory, który posiada bazę danych zasad zapory zawierającą zasady zapory firmy.



• Pracując z komputerów klienckich, administratorzy zapory tworzą zasady i wysyłają je do serwera zarządzania zasadami zapory.

• Po drugie, administrator wybiera zapory, które powinny podlegać zasadom. Często reguła rządzi wieloma zaporami.

• Na podstawie polityk centralny system konfiguracji wysyła odpowiednie reguły ACL na podstawie tych polityk do poszczególnych zapór. Administrator nie musi ręcznie instalować reguł na każdej zaporze.

BAZA DANYCH ZASAD FIREWALL

Rysunek przedstawia dość typową bazę danych strategii zapory. Pokazuje, że każda polityka ma kilka pól.

Policy Number	Source	Destination	Service	Action	Track	Firewalls
1	Internal	DNS servers	UDP dns	Pass	None	All
2	External	Internal	TCP http	Drop	Log	All
3	External	DMZ webserver	TCP http	Pass	None	Border
4	Internal	External	TCP http	Pass	Log	Border
5	Internal	External	ICMP	Drop	None	Border
6	Internal	Mail server	TCP smtp	Authenticate	Log if fail	Central
7	Marketing	Plans server	TCP http	Authenticate	Alert if fail	Marketing
8	Any	Plans server	TCP http	Drop	Log	Marketing
9	Any	Any	Any*	Drop	Log	All

• Pole numeru polityki ma unikalny numer dla każdej polityki. Polityki można zatem odwoływać się do numerów.

• Pola źródłowe i docelowe są dość objaśniające. Mogą to być nazwy hostów lub grupy adresów IP. Niektóre grupy, takie jak Any, są definiowane automatycznie przez system. Administrator zapory musi ręcznie zdefiniować inne grupy.

• Pole usługi opisuje usługę, która ma zostać przefiltrowana. Często będzie to TCP lub UDP plus numer portu lub nazwa aplikacji. Może to być również ICMP lub inny rodzaj usługi określony przez liczbę w polu protokołu nagłówka IP

• Pole działania określa, co zapory powinny zrobić z tą usługą. Najbardziej oczywiste akcje to Pass and Drop. Inną możliwą akcją jest Uwierzytelnij, która nakazuje zaporze uwierzytelnienie użytkownika. Inne działania związane z obsługą specjalną można zdefiniować w zależności od konkretnej polityki firmy.

• Pole śledzenia opisuje, co zapora powinna zrobić po wykonaniu swojej akcji. Może to być nic („brak"), rejestrowanie informacji w pliku dziennika lub powiadamianie kogoś.

• Pole zapory informuje serwer zarządzania zaporą, jakie zapory lub routery powinny zostać wysłane do list ACL zgodnie z tą zasadą.

Baza danych reguł zapory na rysunku zawiera tylko dziewięć reguł. Większość baz danych zasad jest znacznie dłuższa. Zasada 1 zezwala wszystkim hostom wewnętrznym na dostęp do serwerów DNS firmy. Usługa to DNS przez UDP, wszystkie pakiety są przesyłane i nic nie jest śledzone. Ta zasada jest instalowana na wszystkich zaporach. Zasady od 2 do 4 obsługują ruch HTTP przepływający między hostami zewnętrznymi, hostami w strefie DMZ i hostami w sieci wewnętrznej.

BADANIE PODATNOŚCI PO KONFIGURACJI

Biorąc pod uwagę złożoność zasad zapory, złożoność tłumaczenia zasad zapory na określone zestawy reguł ACL oraz złożoność pisania poszczególnych reguł ACL, błędy reguł ACL zapory są nieuniknione podczas instalacji. Ważne jest, aby po instalacji przeprowadzić testy podatności w celu wykrycia tych błędów.

Tak jak zasady regulują wdrażanie, rządzą również testowaniem podatności na ataki. Na przykład, w przypadku czarnej listy klientów, plan testowania podatności polegałby na tym, że tester próbowałby dotrzeć do kilku stron internetowych znajdujących się na czarnej liście z każdego z kilku klientów w różnych częściach witryny lub firmy.

ZEZWOLENIE NA ZMIANY I ZARZĄDZANIE

Aktywa i zagrożenia nieustannie się zmieniają. Ważne jest, aby baza danych zasad była aktualna. Chociaż aktualizacje są nieuniknione, firmy muszą je wprowadzać w zdyscyplinowany sposób. Istnieje tendencja do tego, że zapory ogniowe są początkowo bardzo mocne, ale potem mają dziury w nich, aż przypominają plasterki szwajcarskiego sera.

• Po pierwsze, tylko niektóre osoby powinny mieć możliwość wnioskowania o zmiany, a mniej osób powinno mieć możliwość autoryzacji zmian. Co najważniejsze, osoba zgłaszająca żądanie zmiany zawsze powinna być inna niż osoba autoryzująca zmiany.

• Po drugie, administrator zapory powinien zaimplementować zmianę w najbardziej restrykcyjny sposób — w taki sposób, aby przepuścić najmniejszą liczbę pakietów. Na przykład, zamiast całkowicie otwierać port, personel powinien otwierać go tylko dla konkretnego hosta, jeśli to możliwe.

• Po trzecie, administrator zapory powinien dokładnie udokumentować zmianę. Jeśli każda zmiana nie jest dobrze udokumentowana, zapora będzie niemożliwa do zrozumienia, a przyszłe zmiany mogą mieć niezamierzone konsekwencje. Ponadto wiele przepisów dotyczących zgodności wymaga obszernej dokumentacji.

• Po czwarte, zapora powinna być testowana pod kątem luk po każdej zmianie, aby upewnić się, że zmiana działa i że wszystkie poprzednie zachowania nadal działają. Testowanie, czy wszystkie poprzednie zachowania działają, nazywa się testowaniem regresji.

• Po piąte, firma powinna często kontrolować cały proces, aby zapewnić zgodność z tymi procedurami. Jest to szczególnie ważne, aby administrator zapory otwierał zaporę tak rzadko, jak to możliwe, aby zaimplementować zmienioną politykę.

ODCZYTYWANIE DZIENNIKÓW ZAPORU ZAPOMOWEGO

Jednym z kluczowych sposobów zrozumienia zmieniającego się środowiska zagrożeń jest codzienne lub nawet kilkakrotne czytanie dzienników zapory. Ogólnie rzecz biorąc, czytanie dzienników zapory jest najbardziej czasochłonną częścią administrowania zaporą.

Odczytywanie dzienników zapory jest najbardziej czasochłonną częścią administrowania zaporą.

Podstawową strategią odczytu pliku dziennika jest określenie, jaki ruch jest nietypowy. Na przykład jeden administrator zapory co godzinę przegląda swój plik dziennika, aby zobaczyć dziesięć adresów IP, które były odpowiedzialne za większość porzuconych pakietów. W ataku skanującym adres IP atakującego pojawi się na liście „pierwszej dziesiątki".

Podstawową strategią odczytu pliku dziennika jest określenie, jaki ruch jest nietypowy.

Jeśli atak nie wygląda na zbyt poważny, administrator dziurawi adres IP, co oznacza, że do zapory dodawana jest reguła (przynajmniej tymczasowo) blokująca cały ruch z tego adresu IP. Jeśli atak wydaje się być poważniejszy, administrator może rejestrować wszystkie pakiety z adresu IP, niezależnie od tego, czy są to pakiety ataków, czy nie. Innym przydatnym podejściem jest opracowanie danych historycznych, a następnie podzielenie liczby zdarzeń występujących w danym dniu w kategorii przez średnią liczbę zdarzeń. Na przykład, jeśli liczba nieudanych zapytań DNS jest sto razy większa od zwykłej wartości, jest to silny wskaźnik, na który powinien zwrócić uwagę administrator zapory

Bardziej szczegółowe zapytania DNS. Ogólnie rzecz biorąc, nie ma jednego zestawu reguł ani strategii odczytywania dzienników zapory.

TEST CLVII

a. Porównaj potrzeby wzmacniania zapory dla urządzeń zapory, systemów dostarczonych przez dostawców i zapór zbudowanych na komputerach ogólnego przeznaczenia.

b. Wymień, co robią scentralizowane systemy zarządzania zaporą ogniową.

cC. Jakie kolumny zawiera opisana w tekście baza danych strategii zapory? Umieć opisać każdą i jakie opcje oferuje.

d. Dlaczego konieczne jest testowanie podatności?

e. Dlaczego zasady zapory powinny regulować zarówno konfigurację, jak i testowanie?

f. Jakie są kroki w zarządzaniu zmianami zapory?

g. Dlaczego czytanie dzienników zapory jest ważne?

h. Jaka jest najbardziej czasochłonna część zarządzania zaporą sieciową?

Odczytywanie dzienników zapory

Jak wspomniano na początku tego rozdziału, ważne jest, aby administratorzy zapory codziennie lub nawet częściej czytali swoje pliki dziennika. W tej sekcji przyjrzymy się niektórym strategiom używanym przez administratorów do skanowania plików dziennika.

Pliki dziennika

Aby pomóc w zrozumieniu odczytywania plików dziennika zapory, Rysunek 6-25 przedstawia fragment pliku dziennika przychodzącego dla zapory granicznej.

ID	Time (hh:mm:sss)	Rule	Source IP	Destination IP	Service
1	15:34:005	Echo probe	14.17.3.139	60.3.87.6	ICMP
2	15:34:007	Echo probe	14.17.3.139	60.3.87.7	ICMP
3	15:34:008	Forbidden webserver access	128.171.17.3	60.17.14.8	HTTP
4	15:34:012	External access to internal FTP server	14.8.23.96	60.8.123.56	FTP
5	15:34:015	Echo probe	14.17.3.139	60.3.87.8	ICMP
6	15:34:020	External access to internal FTP server	128.171.17.34	60.19.8.20	FTP
7	15:34:021	Echo probe	1.124.82.6	60.14.42.68	ICMP
8	15:34:023	External access to internal FTP server	14.17.3.139	24.65.56.97	FTP
9	15:34:040	External access to internal FTP server	14.17.3.139	60.8.123.56	FTP
10	15:34:047	Forbidden webserver access	128.171.17.3	60.17.14.8	HTTP
11	15:34:048	Echo probe	14.17.3.139	60.3.87.9	ICMP
12	15:34:057	Echo probe	1.30.7.45	60.32.29.102	ICMP
13	15:34:061	External packet with private IP source address	10.17.3.139	60.32.29.102	ICMP
14	15:34:061	External access to internal FTP server	1.32.6.18	60.8.123.56	FTP
15	15:34:062	Echo probe	14.17.3.139	60.3.87.10	ICMP
16	15:34:063	Insufficient capacity	1.32.23.8	60.3.12.47	DNS
17	15:34:064	Echo probe	14.17.3.139	60.3.87.11	ICMP
18	15:34:065	Forbidden webserver access	128.171.17.3	60.17.14.8	HTTP

Plik dziennika zawiera wybrane dane dla każdego odrzuconego pakietu. Ten uproszczony plik dziennika zawiera sześć informacji dla każdego pakietu:

• Pierwsze pole to numer identyfikacyjny. W prawdziwym pliku dziennika nie ma numeru ID. Jednak numer identyfikacyjny ułatwia nam rozmowę o wpisach w pliku dziennika.

• Drugie pole podaje czas dotarcia pakietu do zapory (w tysięcznych częściach sekundy).

• Trzecie pole to reguła, która spowodowała odrzucenie pakietu. Na rysunku 6-24 regułom nie nadano nazw. Rysunek 6-25 używa nazw reguł, ponownie, aby ułatwić czytanie rysunku.

• Czwarte i piąte pole podają źródłowy i docelowy adres IP pakietu.

• Ostatnie pole w tabeli to żądana usługa. W tym

w stanie, usługi obejmują ICMP, FTP i HTTP.

Sortowanie pliku dziennika według reguły

Nie ma sztywnego zestawu reguł dotyczących odczytywania plików dziennika. Jedyną ogólną radą, którą podaje większość administratorów zapór ogniowych, jest „Poszukaj czegoś innego niż normalne wzorce”. Jednym ze sposobów wyszukiwania nietypowych wzorców jest sortowanie pliku według różnych pól formularza. Na przykład, na Rysunku, administrator zapory może sortować według

kolumny Rule, sortując od najczęściej używanej reguły do najrzadziej używanej reguły. Następnie administrator zlicza liczbę zdarzeń dla każdej reguły.

Sondy echa

Na rysunku najczęściej używana reguła zatrzymuje przychodzące sondy echa ICMP, które są używane do skanowania adresów IP. Zasada ta została zastosowana osiem razy. Jeśli host pod docelowym adresem IP odpowie, wysyłając wiadomość odpowiedzi ICMP echo, atakujący wie, że istnieje host pod pierwotnym docelowym adresem IP ICMP echo. Odrzucanie przychodzących pakietów z komunikatami ICMP echo zapewnia, że żadne odpowiedzi ICMP echo nie są wysyłane. Wszystkie komunikaty ICMP echo zostały wysłane z tego samego źródłowego adresu IP, 14.17.3.139. Pierwsza wiadomość echa trafiła do 60.3.87.6. Kolejne komunikaty ICMP echo zwiększały za każdym razem numer części hosta o 1. Ogólnie rzecz biorąc, jest to po prostu klasyczny atak sondą skanującą. W rzeczywistości jest to najmniej wyrafinowany atak sondą skanującą. Biorąc pod uwagę brak wyrafinowania i normalną częstotliwość, pakiety te nie budzą niepokoju. Administrator zapory może mieć adres czarnej dziury 14.17.3.139 (odrzucać z niej wszystkie przychodzące pakiety), aby zapobiec hałasowi ataków tego niewyrafinowanego napastnika (i powstrzymać atakującego przed wysyłaniem różnych rodzajów ataków, które mogą być bardziej niebezpieczne).

Zewnętrzny dostęp do wszystkich wewnętrznych serwerów FTP

W bardzo krótkim okresie objętym logiem pięciokrotnie zastosowano zasadę zakazującą dostępu z zewnątrz do wewnętrznych serwerów FTP. Pakiety te pochodziły z wielu źródłowych adresów IP i trafiały do wielu serwerów FTP. Jeśli ten wzorzec jest rzadko spotykany i jeśli istnieje wiele ataków z wielu źródeł na wiele docelowych serwerów FTP, może to oznaczać, że celem ataków jest wykorzystanie nowo wykrytej luki w zabezpieczeniach jednego lub wszystkich programów serwera FTP. Fakt, że ataki pochodzą z różnych adresów IP, może wskazywać na wyrafinowany atak. To wymaga dalszych badań. Jeśli firma ma jakieś serwery FTP, które są dostępne z zewnątrz, powiedzmy w strefie DMZ, należy je natychmiast sprawdzić. Ponadto wewnętrzne serwery FTP firmy mogą być podatne na ataki wewnętrzne.

Próba dostępu do wewnętrznych serwerów WWW

Podjęto trzy próby uzyskania dostępu do serwera WWW, do którego dostęp był zabroniony. Wszystkie pochodziły z tego samego źródłowego adresu IP. Przybyli bardzo szybko na czas, więc był to zautomatyzowany atak. To prawdopodobnie częsty atak, a gdyby były tylko trzy próby, to prawdopodobnie nie stanowi to problemu. Jednak plik dziennika obejmuje tylko bardzo krótki okres czasu, więc nie możemy stwierdzić, czy jest to część trwającego ataku opartego na próbie uzyskania dostępu do serwera WWW.

Przychodzący pakiet z prywatnym adresem źródłowym IP

Jeden pakiet przychodzący został odrzucony, ponieważ jego źródłowy adres IP znajdował się w zakresie adresów IP dla prywatnych adresów IP - takich, które powinny być używane tylko w firmach i nigdy nie powinny być wysyłane przez Internet. Jest to niezdarny atak i nie jest powtarzany w okresie rejestrowania. W konsekwencji prawdopodobnie nie stanowi zagrożenia.

Brak pojemności

W końcu jeden pakiet został odrzucony, ponieważ zapora ogniowa nie miała wystarczającej przepustowości, aby go przetworzyć. Jak widzieliśmy na początku, jeśli firewall nie jest w stanie przetworzyć pakietu, odrzuca pakiet na wypadek, gdyby mógł być pakietem ataku. W tej małej próbce

18 pakietów jeden pakiet został odrzucony z powodu braku pojemności. Jeśli coś podobnego do tego wskaźnika utrzymuje się przez dłuższy czas, konieczne jest natychmiastowe zwiększenie pojemności zapory.

Perspektywy

Ogólnie tylko ataki na serwery FTP wydają się stanowić zagrożenie warte dalszego zbadania. Chociaż fajnie byłoby móc zbadać wszystkie ataki, w praktyce jest to niemożliwe.

Rozmiary plików dziennika

Plik dziennika na rysunku jest bardzo krótki i przedstawia ataki odrzucone w ciągu zaledwie 60 milisekund. Oczywiście rzeczywiste pliki dziennika obejmują znacznie dłuższe okresy czasu. W idealnym przypadku czas objęty plikami dziennika powinien być bardzo długi, aby można było wykryć ataki rozłożone w czasie. Można by sprawdzić, czy trzy nielegalne próby uzyskania dostępu do zabronionych serwerów były wyizolowane, czy też stanowiły część większego ataku. Po prostu trudno jest wykryć ataki wykraczające poza granice plików dziennika. Długie pliki dziennika wymagają dużej pojemności dysku. Ponadto w miarę upływu czasu ruch zwykle wzrasta, więc pojemność dysku wystarczająca do przechowywania rozsądnych plików dziennika wymaga skrócenia czasu przechowywania plików dziennika. Rozmiar dysków zapory jest niezwykle ważny, podobnie jak zapewnienie wystarczającej pojemności archiwalnej do przechowywania starszych plików dziennika, aby można było je wykorzystać do zrozumienia ataków, które miały miejsce w poprzednim okresie.

Rejestrowanie wszystkich pakietów

Zwykle zapory są skonfigurowane tak, aby rejestrować tylko te pakiety, które upuszczają. Jednak wiele zapór można skonfigurować tak, aby rejestrowały wszystkie pakiety, niezależnie od tego, czy pakiety są odrzucane, czy przekazywane. Wadą tego podejścia jest to, że znacznie zwiększa liczbę wpisów, które muszą być rejestrowane w danym okresie. To nieuchronnie skraca czas, jaki może pokryć każdy plik dziennika, nawet w przypadku bardzo dużych dysków twardych do przechowywania plików dziennika. Dlaczego więc niektóre firmy rejestrują wszystkie pakiety? Odpowiedź brzmi, że mogą zadawać głębsze pytania dotyczące ruchu przechodzącego przez zaporę. W podanym wcześniej przykładzie host 14.17.3.139 wysłał do firmy pewną liczbę niewyszukanych sond echa. Zapora z łatwością zatrzymała te sondy echa. Co by się jednak stało, gdyby Host 14.17.3.139 przeszedł na bardziej wyrafinowane sondy i ataki hakerskie, których zapora nie byłaby w stanie zatrzymać? Jeśli firma zarejestrowałaby wszystkie pakiety, mogłaby przejrzeć wszystkie pakiety wysłane z hosta 14.17.3.139, aby sprawdzić, czy atakującemu udało się wysłać do sieci pakiety, których zapora nie odrzuciła. Zasadniczo rejestrowanie tylko odrzuconych pakietów pokazuje tylko te pakiety, które udało się zatrzymać zaporze. Znacznie bardziej niebezpieczne są pakiety, których zapora nie zatrzymała, a te pakiety nie są rejestrowane, jeśli rejestrowane są tylko pakiety porzucone.

TEST CLVIII

a. Jakie pakiety są zwykle rejestrowane w plikach dziennika?

b. Jakie są pola w pliku dziennika pokazane na rysunku 6-25?

c. W podanych przykładach według jakiego pola posortowano plik dziennika?

d. Co możemy wywnioskować z pliku dziennika o ataku sondy echa?

e. Czy ten atak wydawał się poważny? Wyjaśniać.

f. Co możemy wywnioskować z pliku dziennika o ataku FTP?

g. Czy ten atak wydawał się poważny? Wyjaśniać.

h. Dlaczego odrzucenie pojedynczego pakietu z powodu braku przepustowości zapory było powodem do niepokoju?

i. Czego nie można ustalić, jeśli pliki dziennika obejmują zbyt krótki okres czasu?

J. Dlaczego plik dziennika jest trudny do pokrycia długiego okresu czasu?

k. Jaka jest zaleta rejestrowania wszystkich pakietów przechodzących przez zaporę?

l. Dlaczego logowanie wszystkich pakietów jest problematyczne?

PROBLEMY Z FILTROWANIEM FIRMY

Naszą dyskusję na temat zapór zakończymy trzema trudnymi problemami, które mogą stwarzać długoterminowe wyzwania dla zapór.

Śmierć obwodu

Aby zapory graniczne były skuteczne, musi istnieć jeden punkt połączenia między siecią lokacji a światem zewnętrznym. Jednak w prawdziwych firmach nie da się utrzymać jednego punktu wejścia.

UNIKANIE ZAPORY GRANICZNEJ

Wielu atakujących może uniknąć filtrowania przez zaporę ogniową, całkowicie omijając zaporę graniczną.

Atakujący wewnętrzni.

Co najważniejsze, wielu napastników jest wewnątrz firmy. Według różnych kont, od 30 do 70 procent wszystkich niewłaściwych zachowań jest popełnianych przez pracowników pracujących w witrynie. Zapory graniczne nie mają w ogóle możliwości powstrzymania takich wewnętrznych ataków. Zaatakowane hosty wewnętrzne. Nawet jeśli osoba korzystająca z wewnętrznego komputera jest uczciwa, jej komputer może zostać naruszony i może atakować wewnętrzne hosty, które nie są chronione przez zaporę graniczną. Hakerzy bezprzewodowej sieci LAN. Ponadto bezprzewodowe sieci LAN mogą umożliwiać hakerom drive-by na wejście do sieci witryny przez punkt dostępowy. Umożliwi to atakującemu całkowite ominięcie zapory granicznej. Strona główna Notebooki, telefony komórkowe i multimedia wprowadzone do witryny. Użytkownicy często przynoszą domowe notebooki, telefony komórkowe i inne urządzenia przenośne do firmy i podłączają je do gniazdek ściennych lub do bezprzewodowej sieci LAN za pośrednictwem punktu dostępowego. Jeśli urządzenie zawiera wirusa lub robaka, może rozprzestrzeniać infekcję w witrynie. Zapora graniczna nie miałaby szans na jej zatrzymanie. Dyski optyczne i napędy USB RAM mogą również sprowadzać do firmy szkodliwe oprogramowanie lub usuwać z firmy informacje stanowiące tajemnicę handlową.

Zapory wewnętrzne. Jak wspomniano wcześniej, wewnętrzne zapory ogniowe zapobiegają atakom między podsieciami w witrynie. Łatwość, z jaką wiele zagrożeń może ominąć zapory graniczne, sprawi, że wewnętrzne zapory będą coraz bardziej potrzebne.

PRZEDŁUŻENIE OBWODU

Innym problemem związanym z zaporami granicznymi jest to, że użytkownicy zewnętrzni i lokalizacje mogą wymagać przepuszczenia przez zaporę, aby mogli wykonywać swoją pracę. Jeśli ci zewnętrzni użytkownicy nie zachowają ostrożności, mogą nieumyślnie wysłać do sieci robaki, wirusy i inne szkodliwe pliki.

Zdalni pracownicy.

Zdalny dostęp pracowników w drodze lub w domu to jeden z największych problemów związanych z myśleniem obwodowym. Komunikacja z komputerem zdalnym przechodzi przez zaporę ogniową, skutecznie umieszczając dom pracownika lub pokój hotelowy „wewnątrz" obwodu witryny. Jeśli zdalny komputer zostanie zhakowany, jest to tak złe, jak w przypadku zhakowania wewnętrznego komputera.

Konsultanci, Outsourcerzy, Klienci, Dostawcy i Spółki zależne.

Ponadto firmy stale współpracują z konsultantami, firmami outsourcingowymi IT, klientami, dostawcami, a nawet innymi spółkami zależnymi firmy. Często witryny tych podmiotów zewnętrznych wykorzystują VPN, aby stać się rozszerzeniem sieci wewnętrznej. Ich witryny skutecznie są sprowadzane w granicach witryny.

PERSPEKTYWY

Chociaż zapory graniczne nie znikną w najbliższej przyszłości, nie są już akceptowane jako jedyna linia obrony firmy i tak naprawdę nigdy nie były. Oprócz wdrażania wewnętrznych firewalli firmy muszą zakładać, że coraz większa liczba ataków dotrze do ich wewnętrznych klientów i serwerów. W związku z tym coraz ważniejsze będzie zabezpieczenie hostów wewnętrznych przed atakami. W następnych dwóch rozdziałach omówiono sposób wzmacniania klientów i serwerów.

TEST CLIX

a. Jak atakujący mogą uniknąć zapory granicznej?

b. W jaki sposób obwód rozszerzył się poza teren witryny?

c. Jak firmy mogą zareagować na ten spadek skuteczności filtrowania firewalla na granicy?

Sygnatury ataków a wykrywanie anomalii

Na listach kontroli dostępu przedstawionych wcześniej w tym rozdziale każda reguła wykrywała atak na podstawie sygnatury ataku, która jest wzorcem w danych o ruchu. (Filtrowanie antywirusowe wykorzystuje również sygnatury do wykrywania wirusów, robaków i koni trojańskich). Gdy pojawiają się nowe zagrożenia, ich sygnatury są identyfikowane i dodawane do bazy reguł zapory.

ATAKI ZERO-DAY

Oczywiście nowe ataki, których wcześniej nie widziano, nie mają sygnatur dla zapór ogniowych i programów antywirusowych. Nowe ataki przeprowadzane przed zdefiniowaniem sygnatur są nazywane atakami dnia zerowego. Dopóki sygnatura ataku nie zostanie zdefiniowana i dodana do bazy reguł zapory, zapora oparta na sygnaturach nie może powstrzymać ataku.

WYKRYWANIE ANOMALII

Jednym ze sposobów radzenia sobie z zagrożeniami, dla których nie ma sygnatury, jest użycie funkcji wykrywania anomalii, która analizuje wzorce ruchu wskazujące, że trwa pewien rodzaj ataku. Na przykład, jeśli host, który zawsze zachowuje się jak klient, zaczyna działać jak serwer FTP, oznacza to, że jest to klient, który został naruszony i jest używany jako serwer FTP, być może jako sposób przechowywania informacji o tożsamości, które napastnik chce sprzedać. Wykrywanie anomalii może powstrzymać nowe ataki, które nie mają dobrze zdefiniowanych sygnatur.

PRECYZJA

Niestety, wykrywanie anomalii jest obecnie mniej dokładne niż wykrywanie oparte na sygnaturach. Wzorce ruchu różnią się z wielu uzasadnionych powodów. Podobnie jak w przypadku IDS, wykrywanie anomalii ma tendencję do generowania tak wielu fałszywych alarmów, że wiele firm z niego nie korzysta. Jednak biorąc pod uwagę szybkość, z jaką zaczynają się rozprzestrzeniać exploity, robaki i wirusy, wykrywanie anomalii ma dziś kluczowe znaczenie w zaporach sieciowych.

TEST CLX

a. Rozróżnij wykrywanie sygnatur i wykrywanie anomalii.

b. Co to jest atak dnia zerowego?

c. Dlaczego nie można zatrzymać ataków typu zero-day za pomocą sygnatur ataków?

d. Jaka jest obietnica wykrycia anomalii?

e. Dlaczego wykrywanie anomalii staje się krytyczne dla zapór sieciowych?

WNIOSEK

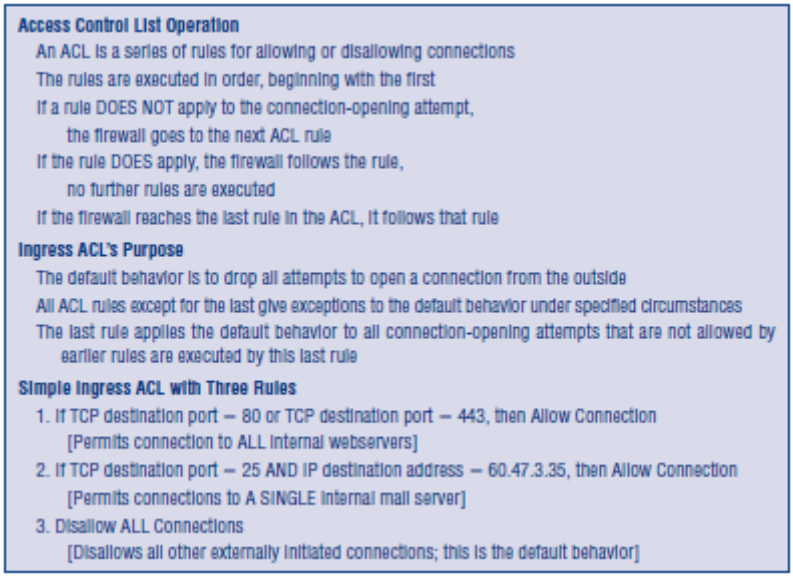
Zapory sieciowe stoją jak strażnicy przy elektronicznych bramach do sieci witryn. Chociaż nie zapewniają całkowitej ochrony, pozostają jednym z podstawowych elementów bezpieczeństwa każdej firmy. Tradycyjnie zapory ogniowe zapewniały filtrowanie przychodzące, aby powstrzymać pakiety ataków przed dostaniem się do firmy. Obecnie wykonują również filtrowanie wychodzące, aby zapobiec atakom wychodzącym ze strony zainfekowanych komputerów, odpowiedziom na ataki sondażowe i kradzieży własności intelektualnej. Zapory wewnętrzne zapewniają ochronę wrażliwym serwerom przed atakami wewnętrznymi, a zapory hostów chronią bezpośrednio zarówno klientów, jak i serwery. Firmy muszą starannie zaplanować architekturę zapory (w jaki sposób rozmieszczają zapory, aby zapewnić maksymalną ochronę). Zapory zwykle rejestrują pakiety ataków porzuconych, a pracownicy ochrony powinni często przeglądać te dzienniki. Istnieje wiele mechanizmów filtrowania firewalla. Pierwsze zapory wykorzystywały statyczną inspekcję pakietów, która analizuje tylko pojedyncze pakiety w izolacji. Statyczna inspekcja pakietów nie jest w stanie powstrzymać wielu ataków, więc jest teraz używana tylko jako mechanizm wtórnego filtrowania lub na routerze przesiewającym - jeśli w ogóle jest używana. Większość dzisiejszych zapór granicznych wykorzystuje stanową inspekcję pakietów (SPI) jako główny mechanizm filtrowania. SPI ma inne reguły dla pakietów, które próbują otworzyć połączenia i dla innych typów pakietów. W przypadku pakietów, które próbują otworzyć połączenia (takich jak pakiety przenoszące segmenty TCP SYN), połączenia inicjowane wewnętrznie są domyślnie otwierane, podczas gdy połączenia inicjowane zewnętrznie są domyślnie blokowane. Listy kontroli dostępu (ACL) modyfikują te domyślne zachowania odpowiednio do zasad zapory firmy. Wszystkie inne pakiety (tj. pakiety, które nie próbują otwierać połączeń) są przepuszczane, jeśli są częścią zatwierdzonego połączenia i odrzucane, jeśli nie są. Zapory sieciowe SPI są szybkie i dlatego niedrogie, ponieważ większość pakietów jest przetwarzana w prosty sposób i zapewniają dużą ochronę. Wiele routerów zapewnia translację adresów sieciowych (NAT). NAT ukrywa wewnętrzne adresy IP i numery portów używane przez hosty wewnętrzne. W związku z tym sniffery nie mogą poznać używanych adresów IP i numerów portów. NAT w rzeczywistości nie filtruje, ale sieci z ochroną NAT są zazwyczaj bardzo trudne do zaatakowania.

Zapory proxy aplikacji zapewniają ochronę w warstwie aplikacji. Przekazują pakiety między hostem wewnętrznym a hostem zewnętrznym, badając zawartość aplikacji. Zapory proxy aplikacji zapewniają wyjątkowo silne zabezpieczenia, ale dla każdej aplikacji, która ma być chroniona, potrzebny jest oddzielny program proxy, a tylko kilka typów aplikacji nadaje się do ochrony serwera proxy aplikacji. Co najgorsze, zapory proxy aplikacji działają bardzo wolno. Najczęściej zdarza się, że zapora proxy

aplikacji jest umieszczona między pojedynczym serwerem a klientami próbującymi się z nim połączyć lub między klientami wewnętrznymi a zewnętrznymi serwerami WWW. Firmy od dawna stosują systemy wykrywania włamań (IDS), które zapewniają głęboką inspekcję pakietów i badają strumienie pakietów zamiast pojedynczych pakietów. Celem IDS jest wyszukiwanie podejrzanych pakietów i zgłaszanie ich, ale nie zatrzymywanie ich. Nowe zapory, które wykorzystują metody IDS do faktycznego odrzucania pakietów, nazywane są systemami zapobiegania włamaniom (IPS). IPS używają sprzętu ASIC, aby zapewnić prędkość niezbędną do analizy ruchu w czasie rzeczywistym (co jest niezbędne do odrzucania pakietów). Ponadto IPS odrzucają pakiety tylko wtedy, gdy mają dużą pewność, że widzą rzeczywisty atak, a nie tylko podejrzane działania. Jeśli dostawcy IPS są mniej pewni, że strumień pakietów jest atakiem, mogą ograniczyć ten ruch do pewnego procentu całkowitej przepustowości, aby zminimalizować szkody. Zapory rzadko wykonują bezpośrednie filtrowanie antywirusowe. Jednak zazwyczaj istnieją silne połączenia między zaporami ogniowymi a serwerami antywirusowymi. Gdy informacje wymagające sprawdzenia antywirusowego dotrą do zapory, zapora przekaże je do serwera antywirusowego. Jeśli serwer antywirusowy nie usunie informacji, dostarcza je do hosta docelowego lub zwraca je do zapory w celu dostarczenia (i prawdopodobnie dodatkowego filtrowania). Kilka zapór, zwanych zaporami ujednoliconego zarządzania zagrożeniami (UTM), zapewnia filtrowanie antywirusowe, podobnie jak tradycyjne filtrowanie, ale nie są one obecnie powszechne. Większość głównych zapór granicznych może również wykrywać i powstrzymywać ataki typu „odmowa usługi" (DoS). Ataki DoS są trudne do powstrzymania, ponieważ pakiety DoS mają taką samą formę jak pakiety legalne. Zapory graniczne często odpowiadają na ataki DoS, ograniczając częstotliwość podejrzanego ruchu DoS i chroniąc serwery wewnętrzne przed półotwartymi atakami DoS z fałszywymi otwarciami. Jeśli jednak natężenie ruchu związanego z atakami jest duże, łącze firmy z Internetem zostanie nasycone i firma nie będzie mogła nic zrobić. Dostawcy usług internetowych muszą zapobiegać atakom DoS, a firmy będące właścicielami zainfekowanych komputerów muszą powstrzymać te komputery przed wysyłaniem pakietów ataków DoS. Zazwyczaj router graniczny jest wieloadresowy, co oznacza, że łączy się z wieloma podsieciami. Jedną z nich może być podsieć prowadząca do Internetu. Drugą może być podsieć prowadząca do sieci wewnętrznej firmy. Trzecią podsieć można nazwać strefą zdemilitaryzowaną (DMZ). Firma umieszcza wszystkie serwery, które muszą być dostępne z Internetu w podsieci DMZ. Hosty znalezione w strefie DMZ obejmują publiczne serwery internetowe, serwery proxy aplikacji i serwer DNS, który zna tylko nazwy hostów i adresy IP hostów w strefie DMZ. Firmy muszą agresywnie wzmacniać hosty w strefie zdemilitaryzowanej, ponieważ hosty te będą narażone na ciągłe ataki ze strony napastników w Internecie. Technologia zapory jest bezużyteczna bez silnego zarządzania. Firmy muszą bardzo dokładnie definiować zasady dotyczące zapór sieciowych, a zasady te muszą prowadzić zarówno do testowania konfiguracji, jak i podatności, aby zapewnić prawidłowe działanie zapory. Firma musi stale aktualizować zasady zapory i listy ACL oraz bardzo często czytać pliki dziennika zapory. Wiele firm korzysta z centralnych systemów zarządzania zaporami, które aktywnie zarządzają zaporami z jednego komputera. Zmniejsza to koszty zarządzania. Rozdział zakończył się dwoma trudnymi problemami, z którymi w przyszłości zmierzą się administratorzy firewalli. Pierwsza to śmierć obwodu. Zapory graniczne są przydatne tylko wtedy, gdy atakujący muszą wejść przez router graniczny Internetu. Jednak nie wszyscy napastnicy muszą to zrobić dzisiaj. Osoby atakujące wewnętrznie i osoby atakujące przechodzące przez punkty dostępu już znajdują się w witrynie, podobnie jak pracownicy, którzy przenoszą złośliwe oprogramowanie na nośnikach wymiennych. Ponadto VPN wprowadzają do sieci prace zdalne, konsultantów, outsourcerów i inne strony, co zasadniczo poszerza ich granice. Po drugie, zapory od dawna stosują wykrywanie sygnatur. Ataki są wykrywane i analizowane. Następnie ich sygnatury są umieszczane w bazie reguł filtrowania zapory. Jednak ataki pojawiają się teraz wkrótce po ich odkryciu. W atakach dnia zerowego pojawiają się przed jakimkolwiek wcześniejszym odkryciem. Bez podpisów firmy są niezwykle podatne na takie ataki. Wykrywanie anomalii działa w inny sposób, wykrywając zmiany wprowadzane przez ataki w ruchu.

Wykrywanie anomalii może automatycznie zatrzymać nawet wcześniej niewidziane ataki. Niestety wykrywanie anomalii jest nieprecyzyjne, ale szybkość ataków sprawia, że rozwój skutecznego wykrywania anomalii jest obecnie obowiązkowy w zaporach sieciowych.

Pytania do przemyślenia



1. Zmodyfikuj listę ACL na rysunku, aby zezwolić na zewnętrznie inicjowane połączenia z serwerem zarządzania siecią SNMP, 60.47.3.103, oraz aby zezwolić zarówno na połączenia zwykłe, jak i SSL/TLS z wewnętrznym serwerem sieciowym 60.47.3.137, ale nie z innymi serwerami sieciowymi.

2. ACL na rysunku działa. Pakiet zawierający segment TCP SYN dociera do zapory sieciowej kontroli pakietów na zewnątrz. Jakie działania podejmie zapora sieciowa SPI?

3. Działa lista ACL na rysunku . Pakiet zawierający segment TCP ACK dociera z zewnątrz do zapory sieciowej inspekcji pakietów. Jakie działania podejmie zapora sieciowa SPI? Wyjaśniać.

4. Utwórz egress ACL dla zapory SPI, jeśli polityka zabrania tylko połączeń z zewnętrznymi serwerami FTP.

5. Porównaj to, czego sniffery mogą się dowiedzieć, jeśli atakowana firma używa NAT lub serwera proxy aplikacji.

6. Większość adresów IP jest publicznych, w tym sensie, że mogą pojawiać się w publicznym Internecie. Jednak kilka adresów IP zostało wyznaczonych jako prywatne adresy IP. Jeden zakres prywatnych adresów IP to 172.16.0.0 do 172.31.255.255. Prywatne adresy IP mogą pojawiać się tylko w firmie. Na rysunku 6-20 hosty wewnętrzne mają prywatne adresy IP, z wyjątkiem tych w strefie DMZ, które używają publicznych adresów IP. Wyjaśnij tę rozbieżność, jeśli możesz.

7. (a) Opisz Politykę 5 w bazie danych polityk firewalla pokazanej na rysunku 6-24. (b) Powtórz dla Polityki 6. (c) Powtórz dla Polityki 7. (d) Powtórz dla Polityki 8. (e) Powtórz dla Polityki 9.

8. Posortuj plik dziennika na rysunku 6-25 według źródłowego adresu IP. Co wnioskujesz z analizy? To nie jest banalne pytanie.

9. Firma stosuje następującą politykę zapory sieciowej: Dostęp pracowników do serwerów internetowych powinien być nieograniczony, a klienci zewnętrzni powinni mieć dostęp tylko do

publicznego serwera internetowego firmy, http://www.pukanui.com. Firma posiada również serwer finansowy, który powinien być dostępny tylko dla osób z działu finansowego. Serwer i działy finansowe znajdują się w wewnętrznej podsieci 10.5.4.3. Firma posiada jedną dużą witrynę. Jak byś wdrożył tę politykę? Utwórz zarówno architekturę zapory, jak i listy ACL dla zapory granicznej zarówno dla wewnętrznych, jak i zewnętrznych prób otwarcia połączenia.

10. Zapora sieciowa z kontrolą pakietów stanowych zawiera regułę, która zezwala na połączenia zewnętrzne z wewnętrznym publicznym serwerem sieciowym, http://www.pukanui.com. Jednak zapora nie zezwala na dostęp do tego serwera. Wymyśl co najmniej dwie hipotezy dotyczące przyczyny problem. Opisz, jak przetestowałbyś każdą hipotezę.

UTWARDZANIE HOSTA

WPROWADZENIE

Chociaż zapory sieciowe powstrzymują większość ataków internetowych, nigdy nie powstrzymają ich wszystkich. W związku z tym ochrona pojedynczych serwerów i innych hostów ma kluczowe znaczenie. W rzeczywistości, jeśli zainstalujesz serwer „po wyjęciu z pudełka", to znaczy przy użyciu nośnika instalacyjnego systemu operacyjnego i domyślnych ustawień instalacyjnych, a następnie podłączysz serwer do Internetu, haker prawdopodobnie „posiada" go w ciągu kilku minut, a nawet sekund .

Co to jest host?

W sieci każde urządzenie z adresem IP jest hostem. Ta prosta definicja działa również w zakresie bezpieczeństwa, ponieważ każde urządzenie z adresem IP może znajdować się w sieci. W związku z tym termin host obejmuje serwery, klientów, routery, zapory, a nawet wiele telefonów komórkowych. Chociaż zwykle nie myślimy o firewallach i routerach jako hostach, pomyśl o szkodach, jakie mógłby wyrządzić haker, gdyby przejął firewall lub router.

Każde urządzenie z adresem IP jest hostem.

Elementy hartowania hosta

Proces ochrony hosta przed atakami nazywa się hartowaniem hosta. Hartowanie nie jest pojedynczą ochroną, ale raczej szeregiem zabezpieczeń, które często mają ze sobą niewiele wspólnego. Wśród tych zabezpieczeń są:

• Regularnie twórz kopie zapasowe hosta. Bez tego nic innego się nie liczy.

• Ogranicz fizyczny dostęp do hosta.

• Zainstaluj system operacyjny z bezpiecznymi opcjami konfiguracji. W szczególności upewnij się, że wszystkie domyślne hasła zostały zastąpione silnymi hasłami. Przeciwnicy znają każde domyślne hasło. Jeśli nie zmienisz nawet jednego, mogą go użyć, aby natychmiast dostać się do twojego systemu.

• Zminimalizuj liczbę aplikacji i usług systemu operacyjnego, które działają na hoście, aby ograniczyć możliwość przejęcia hosta przez hakerów przez naruszenie zabezpieczeń aplikacji lub usługi. Minimalizacja liczby uruchomionych programów zmniejsza „powierzchnię ataku" hostów.

• Utwardź wszystkie pozostałe aplikacje na hoście.

• Pobieranie i instalowanie poprawek na znane luki w systemie operacyjnym.

• Zarządzaj użytkownikami i grupami (dodawania, zmiany, usunięcia itp.).

• Bezpieczne zarządzanie uprawnieniami dostępu dla użytkowników i grup.

• W razie potrzeby zaszyfruj dane.

• Dodaj zaporę hosta.

• Regularnie czytaj dzienniki systemu operacyjnego w poszukiwaniu podejrzanych działań.

• Regularnie przeprowadzaj testy podatności systemu w celu zidentyfikowania słabych punktów bezpieczeństwa, które nie zostały wykryte podczas normalnego przebiegu instalacji lub działania.

Bazy bezpieczeństwa i obrazy

W długim i złożonym zestawie działań łatwo coś przeoczyć. W związku z tym firmy przyjmują standardowe poziomy bazowe bezpieczeństwa - zestaw określonych działań, które należy podjąć w celu wzmocnienia wszystkich hostów określonego typu (Windows, Mac OS, Linux itp.) oraz poszczególnych wersji w ramach każdego typu (Windows Vista, Windows 7, Windows Server 2008 itd.). Potrzebujesz również linii bazowych dla serwerów z różnymi funkcjami, takich jak serwery WWW (Apache, IIS, nginx itp.) oraz serwery poczty e-mail (Sendmail, Microsoft Exchange, Exim itp.). Podstawy bezpieczeństwa są jak listy kontrolne dla pilotów samolotów. Nawet doświadczeni piloci popełniają błędy, jeśli nie przestrzegają listy kontrolnej przed startem. Niektóre firmy wykraczają poza poziom odniesienia, tworząc kilka bezpiecznych instalacji oprogramowania i szeroko je testując. Firmy te następnie zapisują obrazy dysków (pełne kopie) tych instalacji. Przyszłe instalacje będą oparte na tych obrazach dysków. Gdy trzeba zainstalować nowy komputer tego typu, firma pobiera obraz systemu operacyjnego bezpośrednio na nowy komputer. Oszczędza to pieniądze przy każdej instalacji. Zapewnia również, że każdy serwer jest odpowiednio skonfigurowany zgodnie z podstawowymi zasadami bezpieczeństwa firmy i ogólnymi zasadami bezpieczeństwa.

Wirtualizacja

W większych środowiskach korporacyjnych firmy zarządzają setkami obrazów dysków wirtualnych. Mogą być niezależnie wdrażane na różnych platformach sprzętowych za pomocą wirtualizacji. Wirtualizacja umożliwia niezależne działanie wielu systemów operacyjnych wraz z powiązanymi z nimi aplikacjami i danymi na jednej fizycznej maszynie. Te maszyny wirtualne mają własny system operacyjny i współdzielą lokalne zasoby systemowe. Wirtualizacja może początkowo wydawać się sprzeczna z intuicją. Większość użytkowników jest przyzwyczajona do tego, że jeden system operacyjny (OS) jest zainstalowany na jednym fizycznym komputerze (np. Microsoft Windows 7 zainstalowany na laptopie Dell). Jednak możliwe jest posiadanie wielu systemów operacyjnych działających na jednym komputerze fizycznym lub dynamicznych działających na wielu komputerach fizycznych.

ANALOGIA WIRTUALIZACJI

Analogia, która pomaga zrozumieć, jak działa wirtualizacja, porównując (1) komputery fizyczne z budynkami i (2) systemy operacyjne z ludźmi. Osoba jest jak system operacyjny (np. Windows 7, Mac lub Linux), ponieważ zarówno wchodzi w interakcję ze sprzętem, jak i zużywa zasoby (pamięć, moc obliczeniowa itp.). Budynek jest jak fizyczny komputer (np. Dell Latitude 630, HP Blade Server) pod tym względem, że pozwala systemom operacyjnym w nim przebywać i zapewniać potrzebne zasoby. Kawalerka. Większość użytkowników końcowych ma odpowiednik „kawalerki" na swoich komputerach osobistych. Jedna osoba żyje w jednej fizycznej strukturze. Odpowiednikiem obliczeniowym jest jeden system operacyjny działający na jednym fizycznym komputerze. Natywny system operacyjny ma pełny dostęp do całej pamięci i mocy obliczeniowej komputera. Dom jednorodzinny. Jeśli mieszkasz w domu z rodziną, prawdopodobnie masz wiele osób dzielących jedną fizyczną strukturę. Odpowiednikiem obliczeniowym jest wiele systemów operacyjnych działających na jednym fizycznym komputerze. Na przykład na jednym MacBooku Pro można jednocześnie uruchomić system Windows 7 i Mac OS. Posiadanie dwóch systemów operacyjnych umożliwia uruchamianie aplikacji, które mogą być zastrzeżone dla każdego systemu operacyjnego. Jednak pamięć RAM, procesor i miejsce na dysku twardym są współdzielone. Do uruchomienia obu systemów operacyjnych w tym samym czasie mogą być potrzebne dodatkowe zasoby.

Hotel

Hotel pozwala wielu osobom przebywać w wielu fizycznych strukturach. Odpowiednikiem obliczeniowym jest stos fizycznych serwerów obsługujących jednocześnie dziesiątki lub setki maszyn wirtualnych. Jeśli jest wystarczający popyt, hotel może się rozwijać, dodając więcej fizycznych struktur,

aby pomieścić więcej gości. To samo dotyczy serwerów. Posiadanie wielu fizycznych maszyn obsługujących wiele maszyn wirtualnych również zwiększa odporność na awarie. Jeśli na maszynie fizycznej wystąpi awaria sprzętowa, wszystkie maszyny wirtualne znajdujące się na tej maszynie zostaną automatycznie przeniesione na inną maszynę fizyczną.

KORZYŚCI Z WIRTUALIZACJI

Wirtualizacja zapewnia wiele korzyści w procesie wzmacniania hosta. Umożliwia administratorom systemów tworzenie jednej linii bazowej bezpieczeństwa dla każdego serwera (lub zdalnego klienta) w organizacji. Kolejne instancje tego serwera można sklonować z istniejącej wzmocnionej maszyny wirtualnej w ciągu kilku minut zamiast godzin lub dni. Klonowanie wzmocnionych maszyn wirtualnych minimalizuje ryzyko nieprawidłowej konfiguracji serwera, skraca czas potrzebny na skonfigurowanie serwera i eliminuje potrzebę instalowania aplikacji, poprawek lub dodatków Service Pack. Oprócz zwiększenia bezpieczeństwa, środowiska wirtualne mogą również przynieść korzyści firmom, zmniejszając koszty pracy związane z administracją serwerami, rozwojem, testowaniem i szkoleniem. Może również zmniejszyć wydatki na media, wyłączając nieużywane serwery fizyczne oraz zwiększając odporność na awarie i dostępność.

Administratorzy systemów

Pracownicy IT, którzy zarządzają poszczególnymi hostami lub grupami hostów, nazywani są administratorami systemów. (Nie, nazwa nie jest zbyt opisowa.) Zazwyczaj zadaniem administratora systemu określonego serwera jest przeprowadzenie prac wzmacniających. Większe firmy mają wielu administratorów systemów, a podstawowe zabezpieczenia pomagają zapewnić jednolitość wysiłków podejmowanych przez administratorów systemów. Administratorzy systemów na ogół nie zarządzają siecią.

Pracownicy IT, którzy zarządzają poszczególnymi hostami lub grupami hostów, nazywani są administratorami systemów. Administratorzy systemów na ogół nie zarządzają siecią.

TEST

a. Jaka jest nasza definicja hosta?

b. Dlaczego konieczne jest utwardzanie hosta?

c. Jakie główne kategorie gospodarzy wymieniono w tej sekcji?

d. Wymień elementy hartowania gospodarza.

ei. Dlaczego ważne jest zastępowanie domyślnych haseł podczas konfiguracji?

f. Co to jest podstawa bezpieczeństwa i dlaczego jest ważna?

g. Dlaczego pożądane jest pobieranie obrazów dysków systemu operacyjnego w porównaniu z konfigurowaniem każdego hosta indywidualnie?

h. Co to jest wirtualizacja?

i. Jakie są zalety korzystania z maszyn wirtualnych?

j. Czym zarządza administrator systemów?

k. Czy administrator systemu na ogół zarządza siecią?

WAŻNE SYSTEMY OPERACYJNE SERWERÓW

W poprzednich częściach przyjrzeliśmy się kilku typom hostów, w tym serwerom, komputerom klienckim, routerom i zaporom ogniowym. W tej sekcji przyjrzymy się kilku bardziej powszechnym systemom operacyjnym dla serwerów. Skoncentrujemy się na systemach operacyjnych dla serwerów, ponieważ są one częstym celem ataków. Atakujący lubią koncentrować swoje wysiłki na serwerach, ponieważ zawierają cenne dane, są krytyczną częścią korporacyjnych systemów informatycznych i stanowią doskonałą platformę, z której mogą przeprowadzać dodatkowe ataki. Ważne jest, aby znać te systemy operacyjne i wiedzieć, jak zabezpieczyć je przed atakami.

Systemy operacyjne Windows Server

Serwerowym systemem operacyjnym firmy Microsoft jest Windows Server. Wczesne wersje, takie jak Windows Server NT, miały słabe zabezpieczenia. Nowsze wersje systemu Windows Server, takie jak Windows Server 2008, są znacznie bezpieczniejsze. Inteligentnie minimalizują liczbę uruchomionych aplikacji i narzędzi, zadając instalatorowi pytania dotyczące sposobu użytkowania serwera. Sprawiają również, że instalacja łatek podatności jest bardzo prosta i zwykle automatyczna. Obejmują one zapory programowe serwera, możliwość szyfrowania danych i wiele innych ulepszeń bezpieczeństwa. Te zabezpieczenia nie są doskonałe. Co najbardziej irytujące, kilka luk w zabezpieczeniach wymaga comiesięcznych poprawek. Jednak inne systemy operacyjne też mają swój problem.

INTERFEJS UŻYTKOWNIKA SERWERA WINDOWS

Wszystkie najnowsze wersje systemu Windows Server mają interfejsy użytkownika, które wyglądają jak interfejsy w klienckich wersjach systemu Windows. To sprawia, że nauka systemu Windows Server jest stosunkowo łatwa. Windows Server 2008 używa przeglądarki Internet Explorer do pobierania i innych operacji internetowych. Używa również Mojego komputera do zarządzania plikami i ma menu Start, w którym większość opcji jest znana użytkownikom komputerów stacjonarnych. Możesz nawet uruchomić standardowe oprogramowanie klienckie w systemie Windows Server.

START : NARZĘDZIA ADMINISTRACYJNE

Windows Server umieszcza większość narzędzi do zarządzania w opcji Narzędzia administracyjne w menu Programy w menu Start. Ułatwia to administratorom systemów odgadnięcie, gdzie znaleźć potrzebne narzędzia.

KONSOLE ZARZĄDZANIA MICROSOFT (MMCS)

Większość narzędzi administracyjnych w systemie Windows Server ma ten sam ogólny format, zwany Microsoft Management Console (MMC).

• Po pierwsze, jest pasek ikon. Gdy użytkownik wybierze obiekt w jednym z dwóch dolnych paneli, ikony określają akcje, które administrator może wykonać na wybranym obiekcie. Jednym z najważniejszych wyborów jest Akcja, która jest specyficzna dla wybranego obiektu.

• Po drugie, w lewym dolnym panelu (panel drzewa) znajduje się drzewo aplikacji administracyjnych.

• Po trzecie, poszczególne aplikacje w panelu drzewa nazywane są przystawkami, ponieważ można je łatwo dodać lub usunąć z listy drzewa. Pozwala to administratorom systemów na łatwe dostosowywanie MMC do ich konkretnych potrzeb. Na rysunku zaznaczona jest przystawka Usługi.

• Po czwarte, w prawym dolnym okienku znajdują się podobiekty dla wybranego narzędzia (Usługi). W takim przypadku wybrana jest usługa Zapora systemu Windows.

Wszystkie konsole MMC mają tę samą ogólną organizację, z paskiem ikon, okienkiem drzewa i okienkiem podobiektów. Czynności, które administrator może wykonać na wybranym obiekcie, są

wyświetlane po kliknięciu ikony Czynność. Ten spójny interfejs użytkownika ułatwia nauczenie się korzystania z nowych konsoli MMC i nowych przystawek.

TEST

a. Jak nazywa się serwerowy system operacyjny firmy Microsoft?

b. Jakie zabezpieczenia oferują najnowsze wersje tego systemu operacyjnego?

c. Dlaczego Microsoft Windows Server jest łatwy do nauczenia?

d. Czym są MMC? (Nie podawaj tylko akronimu.)

e. Na jakim obiekcie działa ikona paska ikon?

f. Co znajduje się w okienku drzewa?

g. Do czego odnoszą się elementy w panelu podobiektów?

h. Co to jest przystawka?

i. Dlaczego nazywa się je „zatrzaskami”?

j. Dlaczego standardowy układ MMC jest korzystny?

k. W jaki sposób administrator systemu uzyskuje dostęp do większości konsoli MMC narzędzi administracyjnych?

l. Co robi wybranie akcji?

Serwery UNIX (w tym Linux)

UNIX to popularny system operacyjny dla największych serwerów. Jest również używany na niektórych komputerach osobistych. UNIX powstał wiele lat temu. Ta długa historia zapewniła mu szeroką funkcjonalność i wysoką niezawodność. W niektórych przypadkach jednak fakt, że jego podstawowa architektura jest bardzo stara, objawia się pewnymi ograniczeniami i archaicznymi sposobami interakcji z użytkownikami.

WIELE WERSJI

Trudno jest szeroko mówić o bezpieczeństwie UNIX, ponieważ UNIX nie jest pojedynczym systemem operacyjnym, takim jak Windows. Zamiast tego istnieje wiele różnych wersji systemu UNIX. Główni dostawcy, w tym IBM, SUN i Hewlett-Packard, mają własne komercyjne wersje systemu UNIX. Firma nie tylko kupuje UNIX; kupuje określoną wersję systemu UNIX. Te różne wersje systemu UNIX mają tendencję do współdziałania na poziomie jądra (podstawowej części systemu operacyjnego). Kompatybilność jądra pozwala im uruchamiać większość tych samych aplikacji. Jednak jądro jest tylko częścią systemu operacyjnego. Różne wersje systemu UNIX mają zwykle różne narzędzia do zarządzania, w tym narzędzia bezpieczeństwa. Może to utrudnić administrowanie systemem UNIX, jeśli firma korzysta z kilku różnych typów systemu UNIX.

LINUX

W przypadku systemu UNIX na komputery PC sytuacja jest jeszcze bardziej chaotyczna. Najpopularniejszą wersją systemu UNIX dla komputerów PC jest Linux. Jednak Linux jest tylko jądrem systemu operacyjnego. To, co faktycznie oferują dostawcy Linuksa, to dystrybucje, które łączą to jądro z innym oprogramowaniem – zwykle oprogramowaniem z projektu GNU. W przypadku większości

funkcji GNU oferuje kilka alternatywnych programów. W związku z tym dystrybucje Linuksa są raczej różne, szczególnie w zakresie zarządzania i bezpieczeństwa. W wielu przypadkach działy kupują wersje systemu Linux na komputery PC bez ogólnej koordynacji ze strony firmy.

Linux to wersja systemu UNIX działająca na zwykłych komputerach PC. W rzeczywistości Linux jest tylko jądrem systemu operacyjnego. Rzeczywiste pakiety dla Linuksa to dystrybucje zawierające jądro i wiele innych programów - najczęściej programy z projektu GNU.

Linux jest popularny, ponieważ jest darmowy, chociaż „darmowy" należy traktować z kilkoma ziarnami soli. Po pierwsze, niektórzy dostawcy Linuksa pobierają opłaty za korzystanie ze swoich wersji Linuksa, niezależnie od tego, czy nazywają to ceną sprzedaży, czy nie. Mimo to Linux jest znacznie tańszy w zakupie niż komercyjne serwerowe systemy operacyjne, a pojedynczą kopię systemu Linux można zainstalować na wielu serwerach bez dodatkowych kosztów. Z pewnością nie dotyczy to Microsoft Windows Server lub wersji UNIX stworzonej przez dostawców serwerów. Jednak cena zakupu to tylko jeden czynnik całkowitego kosztu posiadania (TCO). Wiele firm uważa, że administrowanie Linuksem jest dość drogie, zwłaszcza jeśli używają wielu dystrybucji od wielu dostawców Linuksa. Fakt, że istnieje wiele różnych dystrybucji Linuksa, utrudnia wzmocnienie systemu Linux. Niektóre z bardziej popularnych dystrybucji Linuksa to między innymi Ubuntu, Mint, Fedora, Debian, openSUSE, Mandriva i tak dalej. Ważne jest, aby mieć dobry poziom bezpieczeństwa dla konkretnej używanej wersji dystrybucji UNIX. Chociaż Linux został pierwotnie stworzony dla komputerów osobistych, obecnie wiele dużych serwerów działa na Linuksie. Zakup serwerów jest zwykle scentralizowany, dzięki czemu można kontrolować różnorodność dystrybucji Linuksa na serwerach firmowych.

INTERFEJSY UŻYTKOWNIKA UNIX

Nawet w określonej wersji systemu UNIX oprogramowanie systemu operacyjnego może zawierać kilka alternatywnych interfejsów użytkownika. Niektóre z tych interfejsów będą graficznymi interfejsami użytkownika podobnymi do interfejsu systemu Microsoft Windows. W systemie Linux istnieją dwa popularne GUI: Gnome i KDE. Inne interfejsy będą interfejsami wiersza poleceń (CLI), które UNIX wywołuje powłoki. W CLI użytkownik wpisuje polecenie i naciska Enter. Na przykład, aby zobaczyć pliki w katalogu, użytkownik może wpisać „list-ls[Enter]" w wierszu polecenia. Powłoki poleceń mają zwykle wybredną składnię, a w systemie UNIX wielkość liter ma kluczowe znaczenie. Z drugiej strony powłoki CLI zużywają mniej zasobów systemowych niż GUI. Ponadto każdy proces, który obejmuje sekwencję poleceń, można połączyć w skrypt, który można uruchomić za każdym razem, gdy ta sekwencja działań musi zostać wykonana. Wiele narzędzi zabezpieczających działa tylko w interfejsach CLI, więc specjaliści ds. bezpieczeństwa w systemie UNIX mają tendencję do wpisywania skomplikowanych, wymagających składni poleceń w celu wykonania prac związanych z bezpieczeństwem. Nawet jeśli używany jest graficzny interfejs użytkownika, administratorzy systemów UNIX często schodzą do wiersza poleceń, aby wykonać określone zadania. W użyciu jest kilka popularnych pocisków. Muszla Bourne'a była jedną z pierwszych oryginalnych popularnych muszli. Obecnym liderem rynku jest prawdopodobnie Bourne Again Shell (BASH).

TEST

a. Dlaczego ogólnie bezpieczeństwo systemów UNIX jest trudne do opisania?

b. Rozróżnij UNIX i Linux.

c. Czym jest jądro Linuksa?

d. Co to jest dystrybucja Linuksa?

e. Skomentuj koszt Linuksa.

f. Czy dana wersja systemu UNIX ma pojedynczy interfejs użytkownika?

g. Jak nazywają się UNIX CLI?

h. W jaki sposób CLI są korzystne?

i. Dlaczego interfejsy CLI są trudne w użyciu?

Luki w zabezpieczeniach i łatki

Wyścig zbrojeń między dostawcami systemów operacyjnych a hakerami to niekończąca się bitwa. Wyszukiwacze luk w zabezpieczeniach nieustannie odkrywają nowe luki w zabezpieczeniach, które są lukami w zabezpieczeniach, które otwierają program na atak. Luki w zabezpieczeniach to luki w zabezpieczeniach, które otwierają program na atak. Większość osób, które znajdują luki w zabezpieczeniach, powiadamia dostawców oprogramowania, aby producenci mogli opracować poprawki dla tych luk. Jednak niektórzy znalazcy luk sprzedają swoje luki hakerom, którzy szybko opracowują programy wykorzystujące luki w zabezpieczeniach. Producenci oprogramowania tworzą poprawki, gdy zgłaszane są im luki w zabezpieczeniach. Jednak ataki hakerów mają miejsce przed utworzeniem tych poprawek. Ataki, które pojawiają się przed poprawkami, są uwolnione nazywane są atakami dnia zerowego. Jak na ironię, najniebezpieczniejszy okres zwykle pojawia się natychmiast po wydaniu poprawki przez dostawcę. Atakujący przeprowadzają inżynierię wsteczną poprawki, aby dowiedzieć się o ukrytej luce. Exploity oparte na reengineeringu zwykle pojawiają się w ciągu dnia lub dwóch, a czasami pojawiają się w ciągu kilku godzin. Firmy nie mogą zwlekać z zastosowaniem nowo wydanych poprawek dla krytycznych luk w zabezpieczeniach.

TEST

a. Co to jest luka w zabezpieczeniach?

b. Co to jest exploit?

c. Czym jest atak dnia zerowego?

d. Dlaczego szybkie zastosowanie krytycznych poprawek jest ważne?

Poprawki

Widzieliśmy, że gdy dostawcy odkrywają, że mają luki, tworzą poprawki. Istnieją cztery rodzaje poprawek.

OBEJŚCIA

Najmniej zadowalające rozwiązanie to obejście, które jest serią ręcznych kroków, które administrator systemu musi wykonać, aby złagodzić problem. Nie jest zaangażowane żadne nowe oprogramowanie. Obejścia są zwykle bardzo pracochłonne. Ponadto łatwo jest popełnić błąd podczas wykonywania skomplikowanych ręcznych poprawek; może to mieć katastrofalne skutki, nawet jeśli nie nastąpią żadne ataki.

ŁATY

Lepiej jest, gdy dostawcy tworzą łatkę, czyli mały program, który naprawia konkretną lukę. Administrator systemu musi pobrać, zainstalować i uruchomić poprawkę. Microsoft zazwyczaj publikuje poprawki w drugi wtorek każdego miesiąca. To czule stało się znane jako „łatka we wtorek.

Łatka to mały program, który naprawia konkretną lukę.

Administratorzy systemów muszą zachować ostrożność przy włączaniu automatycznych aktualizacji na wszystkich komputerach z systemem Windows. Biorąc pod uwagę dominację systemu operacyjnego Windows w korporacjach, administratorzy systemów muszą być świadomi, że automatyczna poprawka we wtorek może spowodować znaczne przestoje krytycznych systemów w środę.

PAKIETY SERWISOWE

Okresowo dostawcy zazwyczaj umieszczają poprawki luk w zabezpieczeniach, a czasem ulepszenia funkcjonalności w jednej dużej aktualizacji. W systemie Windows są to tak zwane dodatki Service Pack. Administrator Asystems może instalować nowe dodatki Service Pack, mając pewność, że jego host będzie aktualny po instalacji.

AKTUALIZACJE WERSJI

Często najlepszym rozwiązaniem jest aktualizacja oprogramowania do najnowszej wersji. Zwykle problemy z zabezpieczeniami są rozwiązywane w nowszych wersjach i ogólnie każda nowsza wersja systemu operacyjnego ma lepsze zabezpieczenia. Ponadto, jeśli wersja jest za stara, dostawca przestanie tworzyć dla niej poprawki.

TEST

a. Wymień cztery typy poprawek luk.

b. Rozróżnij obejścia i poprawki.

c. Co to jest dodatek Service Pack w systemie Microsoft Windows?

d. Dlaczego uaktualnienie do nowej wersji systemu operacyjnego jest zwykle dobre dla bezpieczeństwa?

Mechanika instalacji poprawek

SERWER MICROSOFT WINDOWS

W systemie Microsoft Windows Server instalowanie poprawek jest proste. Począwszy od systemu Windows Server 2003, serwery można zaprogramować tak, aby automatycznie sprawdzały dostępność aktualizacji. Nawet w systemie Windows Server 2000 administrator musiał jedynie wybrać pierwszą pozycję w menu Start.

PROGRAM RPM LINUX

Każdy dostawca systemu UNIX ma własne podejście do pobierania poprawek. Dostawcy Linuksa również stosują różne podejścia, chociaż wielu dostawców Linuksa stosuje metodę rpm stworzoną przez Red Hat, który jest wiodącym dostawcą Linuksa. Nazwa tej metody pochodzi od polecenia rpm użytego do zainicjowania pobierania.

TEST

a. W systemie Windows Server 2003 i 2008, jak automatyczne może być stosowanie poprawek?

b. Jaka metoda pobierania poprawek jest powszechnie używana w systemie Linux?

Problemy z łataniem

Chociaż łatanie ma kluczowe znaczenie, wiele firm nie instaluje poprawek na niektórych swoich serwerach, a łatanie klientów jest jeszcze mniej powszechne. Co może tłumaczyć to zaniedbanie?

LICZBA ŁAT

Głównym problemem jest sama liczba łatek generowanych corocznie przez dostawców. Firmy zazwyczaj korzystają z kilku różnych dostawców systemów operacyjnych, z których każdy co roku publikuje wiele raportów o lukach i łat. Ponadto firmy korzystają z wielu programów użytkowych, a większość aplikacji wymaga częstych poprawek. Atakujący często mogą wykorzystać luki w aplikacjach, aby przejąć komputer. Aby wyliczyć te kwestie, Zespół Reagowania na Awarie Komputerowe/Centrum Koordynacji (CERT/CC) naliczył 1090 luk w 2000 roku. W 2007 roku liczba ta wzrosła do 7 236,11 Już w 2001 roku Activis oszacował, że firma posiadająca tylko osiem zapór ogniowych i dziewięć serwerów musiałaby stosować średnio pięć łatek dziennie12. Obecnie sytuacja jest znacznie gorsza.

KOSZT INSTALACJI POPRAWEK

Chociaż same łatki są bezpłatne, praca potrzebna do poznania ich istnienia, pobrania ich i zainstalowania jest kosztowna. Biorąc pod uwagę przytłaczającą liczbę łat wydawanych każdego roku, całkowity koszt zarządzania poprawkami może być ogromny.

NAJWAŻNIEJSZE ŁATKI

W przypadku większości firm koszt instalacji wszystkich poprawek jest zaporowy. Wiele firm sortuje łatki według priorytetów. Oczywiście w pierwszej kolejności należy załatać krytyczne luki, które otworzą firmę na bardzo poważne ataki. To, jak głęboko firma znajdzie się na liście priorytetów luk i poprawek, zależy od analizy ryzyka – równoważenia kosztów z zagrożeniami.

SERWERY ZARZĄDZANIA POPRAWKAMI

W obliczu przytłaczającego obciążenia poprawkami wiele firm korzysta obecnie z wewnętrznych serwerów zarządzania poprawkami. Serwery zarządzania poprawkami dowiadują się, jakie oprogramowanie działa na serwerach firmy. Serwery zarządzania poprawkami następnie aktywnie oceniają, które programy na każdym hoście wymagają poprawek i wysyłają poprawki na serwery. Serwery zarządzania poprawkami mogą znacznie obniżyć koszty poprawek. W środowiskach korporacyjnych korzystających z systemu Windows Server© możliwe jest zarządzanie poprawkami, poprawkami i aktualizacjami za pośrednictwem usług Windows Server Update Services (WSUS). Umożliwia administratorom systemów zarządzanie pobieraniem, dystrybucją i aplikacją z centralnie zarządzanego serwera . Administratorzy mogą się upewnić, że każdy komputer jest aktualizowany i w razie potrzeby stosuje poprawki.

RYZYKO INSTALACJI PATCH

Instalowanie poprawek nie jest pozbawione własnego ryzyka. Po pierwsze, dodatkowe bezpieczeństwo często wiąże się z ograniczeniem funkcjonalności, co może być nieuzasadnione, biorąc pod uwagę stopień dodatkowego bezpieczeństwa oferowany przez poprawkę. Po drugie, niektóre łatki faktycznie zamrażają maszyny lub powodują inne uszkodzenia. Jest to szczególnie złe, jeśli łatka nie ma opcji odinstalowania. Firmy zazwyczaj pobierają łatkę na system testowy i dokładnie badają jej skutki przed wprowadzeniem jej na wszystkie serwery lub klientów. Jeśli firma ma standardową podstawę bezpieczeństwa dla różnych typów hostów, są duże szanse, że doświadczenia z systemem testowym będą odzwierciedlać te na innych hostach.

TEST

a. Dlaczego firmy mają trudności z nakładaniem łatek?

b. Dlaczego wiele firm traktuje poprawki priorytetowo?

c. Jak pomagają serwery zarządzania poprawkami?

d. Jakie dwa zagrożenia niesie ze sobą łatanie?

ZARZĄDZANIE UŻYTKOWNIKAMI I GRUPAMI

Znaczenie grup w zarządzaniu bezpieczeństwem

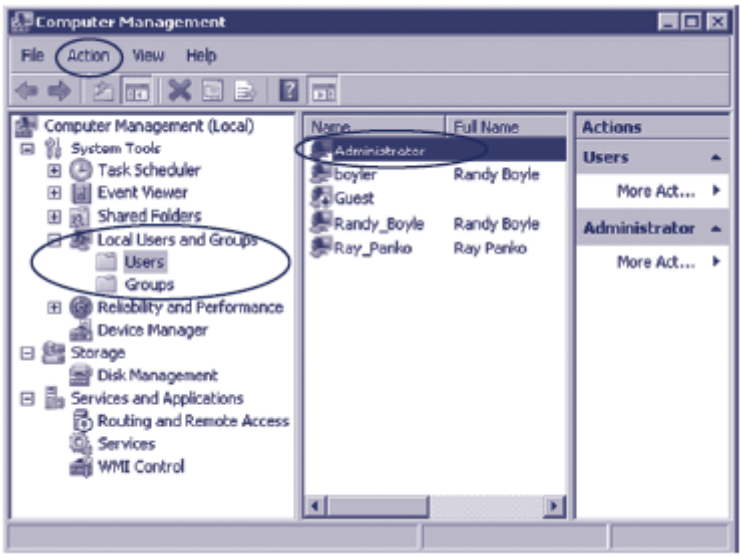
Kolejnym aspektem utwardzania hosta, który omawiamy, jest tworzenie kont i grup użytkowników oraz zarządzanie nimi. Każdy użytkownik musi mieć konto. Ponadto często tworzy się grupy, a następnie dodaje do nich poszczególnych użytkowników. Kiedy środki bezpieczeństwa, takie jak wymaganie długich i złożonych haseł, są stosowane do grup, wszyscy użytkownicy w tych grupach są automatycznie poddawani tym środkom. Stosowanie środków bezpieczeństwa do grup oczywiście wymaga znacznie mniej pracy niż stosowanie tych środków do poszczególnych kont. Stosowanie środków do grup również zmniejsza liczbę błędów, ponieważ większość grup ma dobrze zdefiniowane role, które prowadzą do jasnych wymagań bezpieczeństwa. Z kolei osoby fizyczne mogą pełnić wiele ról o różnych wymaganiach dotyczących bezpieczeństwa, co utrudnia przypisanie odpowiednich ustawień zabezpieczeń do poszczególnych kont.

TEST

a. Podaj dwa powody, dla których przypisywanie środków bezpieczeństwa grupom jest lepsze niż przypisywanie środków bezpieczeństwa poszczególnym osobom w grupach.

Tworzenie i zarządzanie użytkownikami i grupami w systemie Windows

W przypadku samodzielnych serwerów Windows administrator może skorzystać z konsoli MMC do zarządzania komputerem. Jak pokazano na rysunku, istnieje przystawka Użytkownicy i grupy lokalne z dwiema podkategoriami - Użytkownicy i grupy.



Wybrano kategorię Użytkownicy. W prawym okienku wyświetlana jest lista użytkowników. Wybrano użytkownika Administrator. Jeśli administrator systemu wybierze opcję menu Akcja lub kliknie prawym

przyciskiem myszy dowolne konto, będzie mógł zmienić nazwę konta, usunąć je, zmienić jego właściwości zabezpieczeń lub podjąć inne działania.

KONTO ADMINISTRATORA

Każdy system operacyjny ma konto superużytkownika, które ma całkowitą kontrolę nad komputerem. W systemie Windows konto superużytkownika jest administratorem. W systemie UNIX jest to konto root. Każdy, kto loguje się na konto superużytkownika, ma całkowitą kontrolę nad komputerem. On lub ona może wszystko zobaczyć i wszystko zmienić. W związku z tym głównym celem hakerów jest przejęcie konta superużytkownika. Ponieważ hakowanie rozpoczęło się na komputerach z systemem UNIX, przejęcie konta superużytkownika na dowolnym komputerze nazywa się hacking root. Aby zminimalizować zagrożenia, administratorzy systemów powinni jak najmniej korzystać z konta superużytkownika. Gdy nie wymagają uprawnień superużytkownika, powinni pracować z indywidualnymi kontami osobistymi, które mają niewiele uprawnień. Tylko wtedy, gdy potrzebują uprawnień superużytkownika, powinni zalogować się na konto superużytkownika. W systemie Windows Server polecenie RunAs pozwala im przełączać się między pracą jako administrator a pracą z normalnym kontem. W systemie UNIX polecenie su (przełącz użytkownika) może przełączać administratora systemu między kontem root a jego ograniczonymi kontami osobistymi.

ZARZĄDZANIE KONTAMI

Rysunek pokazuje, co się stanie, jeśli administrator systemu kliknie prawym przyciskiem myszy konto (w tym przypadku konto administratora) i wybierze Właściwości.

Ta akcja przeniesie użytkownika do okna dialogowego pokazanego na rysunku. Karta Ogólne (pokazana) umożliwia administratorowi systemu nałożenie ograniczeń hasła na użytkownika. Kolejna zakładka umożliwia administratorowi systemu dodanie konta użytkownika do wielu grup.

TWORZENIE UŻYTKOWNIKÓW

Polecenie Akcja umożliwia tworzenie nowych kont użytkowników. Aby utworzyć nowe konto, administrator systemu wprowadzi nazwę konta, hasło i inne informacje o koncie.

GRUPY WINDOWS

Wybranie opcji Grupy zamiast Użytkownicy spowoduje wyświetlenie listy grup. Administrator systemu będzie mógł przeglądać każdą grupę, aby zobaczyć jej członków, a następnie dodawać lub usuwać członków z grupy.

TEST

a. Jaka przystawka systemu Windows służy do zarządzania użytkownikami i grupami?

b. Na której konsoli MMC jest dostępna ta przystawka?

c. W tej przystawce, jeśli administrator kliknie konto, co może zrobić?

d. Jak administrator tworzy nowe konto?

ei. Jak administrator dodaje konto do grupy?

f. Jak administrator tworzy nową grupę?

a. Jakie uprawnienia ma konto superużytkownika?

b. Co to jest konto superużytkownika w systemie Windows?

c. Co to jest konto superużytkownika w systemie UNIX?

d. Co to jest root hacking i dlaczego jest to pożądane przez hakerów?

e. Kiedy administrator systemów Windows powinien używać konta administratora?

f. W jaki sposób administrator dostaje się do konta superużytkownika w systemie Windows? W UNIX-ie?

ZARZĄDZANIE ZEZWOLENIAMI

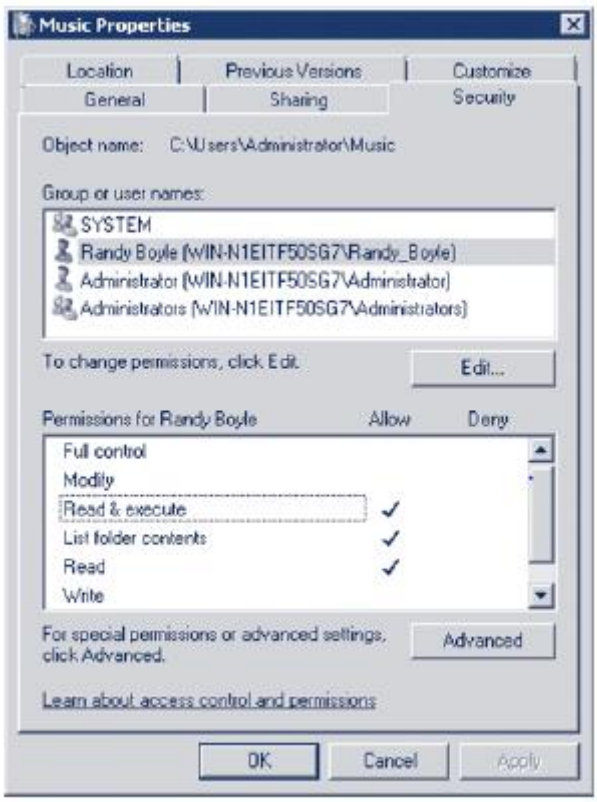
Uprawnienia

Tylko dlatego, że ktoś loguje się poprawnie, nie oznacza, że powinien mieć wolną rękę, aby robić na serwerze wszystko, co zechce. Każdemu kontu i grupie administratorzy systemów przypisują uprawnienia, które określają, co użytkownik lub grupa może robić, a czego nie może robić z plikami, katalogami i podkatalogami. Uprawnienia mogą obejmować nawet brak możliwości zobaczenia katalogu, a także pozwolenie na zrobienie z nim wszystkiego. Uprawnienia określają, co użytkownik lub grupa może robić, a czego nie może robić z plikami, katalogami i podkatalogami.

Przypisywanie uprawnień w systemie Windows

ZEZWOLENIA DO KATALOGU

Aby przypisać uprawnienia w systemie Windows, administrator systemu może kliknąć prawym przyciskiem myszy katalog (folder) lub plik w obszarze Mój komputer lub Eksplorator Windows. Na rysunku 7-20 administrator systemu zrobił to dla katalogu



Moja muzyka i wybrał Właściwości z wyskakującego menu. Administrator systemu wybrał następnie zakładkę Bezpieczeństwo. Zauważ, że górny panel pokazuje wszystkich użytkowników i grupy, którym przypisano uprawnienia do tego katalogu. Wybrano grupę Użytkownicy zaawansowani.

UPRAWNIENIA WINDOWS

Dolny panel pokazuje sześć standardowych uprawnień w systemie Windows i które z tych uprawnień zostały przypisane do grupy Użytkownicy zaawansowani. Jeśli wybrano inną grupę lub użytkownika, pojawiłyby się inne uprawnienia. Chociaż te standardowe uprawnienia dają szeroki zakres opcji, czasami potrzebne są bardziej szczegółowe uprawnienia. Przycisk Zaawansowane na karcie Zabezpieczenia umożliwia bardziej szczegółowe przypisanie uprawnień, jeśli to konieczne. Ten przycisk prowadzi do 13 specjalistycznych uprawnień, z których zbudowanych jest 6 standardowych uprawnień.

DODAWANIE UŻYTKOWNIKÓW I GRUP

Zwróć uwagę, że istnieją przyciski do dodawania nowych użytkowników lub grup oraz do usuwania użytkowników i grup, którym przypisano uprawnienia. Nie ma ograniczeń co do liczby użytkowników i grup, którym można przypisać uprawnienia do katalogu. Ponadto każdemu użytkownikowi i grupie można przypisać inny zestaw uprawnień w katalogu.

DZIEDZICTWO

W systemie Windows dziedziczenie oznacza, że katalog otrzymuje uprawnienia z katalogu nadrzędnego. Oznacza to, że katalog podrzędny ma dokładnie takie same uprawnienia jak katalog nadrzędny dla każdego użytkownika i grupy. Zauważ, że pole Uwzględnij dziedziczone uprawnienia z rodzica tego obiektu musi być zaznaczone, aby umożliwić dziedziczenie uprawnień z katalogu nadrzędnego. Jest to ustawienie domyślne w zaawansowanych ustawieniach zabezpieczeń. Efektywne uprawnienia osoby lub grupy to uprawnienia dziedziczone po rodzicu (jeśli pole dziedziczenia jest

zaznaczone) plus uprawnienia wyraźnie dozwolone, pomniejszone o uprawnienia, które są wyraźnie odmawiane.

ORGANIZACJA KATALOGU

W większości przypadków instalator może zorganizować katalogi najwyższego poziomu, aby proste dziedziczenie stało się normalnym procesem w prawie wszystkich katalogach. Na przykład, jeśli wszystkie programy, które powinny być dostępne dla wszystkich zalogowanych użytkowników, są zgrupowane w jednym katalogu najwyższego poziomu, publicznymi programami, instalator może nadać grupie, wszystkim zalogowanym użytkownikom, uprawnienia do odczytu i wykonywania w miejscach publicznych. katalog programów. Domyślnie odczyt i wykonanie będą dziedziczone dla wszystkich programów we wszystkich podkatalogach. Tylko wtedy, gdy ta wartość domyślna musi zostać pominięta, pola Zezwól i Odmów muszą być zaznaczone.

TEST

a. W jaki sposób uprawnienia są stosowane do katalogu w systemie Windows?

b. Wymień wszystkie standardowe uprawnienia systemu Windows i krótko je wyjaśnij.

c. Do ilu kont i grup można zastosować różne uprawnienia w systemie Windows?

d. Jak dziedziczenie może obniżyć koszty pracy przy przydzielaniu uprawnień?

e. Jak można zmodyfikować dziedziczenie?

f. Jak obliczane są efektywne uprawnienia użytkownika do katalogu?

g. Jak utworzyłbyś katalog najwyższego poziomu dla dokumentów polityki publicznej firmy, które powinny być czytelny dla wszystkich zalogowanych użytkowników?

Przypisywanie grup i uprawnień w UNIX

W porównaniu z uprawnieniami dostępu w systemie Windows uprawnienia w systemie UNIX są ograniczone. Jest to jeden z najpoważniejszych problemów związanych z bezpieczeństwem komputerów z systemem UNIX. Niektóre wersje systemu UNIX przypisują uprawnienia bardziej szczegółowo niż standardowe, ale standard jest normalnym zachowaniem systemu UNIX. Rysunek 7-23 porównuje przydzielanie uprawnień w systemach Windows i UNIX.

LICZBA UPRAWNIEŃ

Jak już wspomniano, system Windows ma sześć różnych uprawnień, które można przypisać użytkownikom i grupom. Jeśli potrzebna jest większa szczegółowość, system Windows ma 13 specjalnych uprawnień do przypisania. W przeciwieństwie do tego, UNIX ma tylko trzy uprawnienia do przypisania. Odczyt to dostęp tylko do odczytu (oznaczony przez r). Zapis umożliwia dokonywanie zmian przez konto lub grupę (oznaczony przez w). Execute umożliwia wykonywanie programów (oznaczonych przez x). Te uprawnienia są zwykle zapisywane jako rwx.

LICZBA KONT LUB GRUP

Jak już wspomniano, system Windows może przypisywać różne uprawnienia do wielu kont i grup. Na przykład w katalogu (folderze) zespołu projektowego różnym członkom i podgrupom w zespole prawdopodobnie należy nadać różne uprawnienia dostępu. Jednak UNIX historycznie może przypisywać różne uprawnienia tylko trzem jednostkom. Jedna jednostka to konto będące właścicielem pliku lub katalogu. Druga to pojedyncza grupa powiązana z katalogiem. Trzeci to wszyscy

inni. Nie ma możliwości przypisania różnych uprawnień do wielu kont lub grup. To ogranicza. Chociaż UNIX generalnie ma dobre zabezpieczenia, jego brak elastyczności w obsłudze uprawnień jest poważnym problemem. Nawet ewangeliści UNIX zachwalający mocne strony systemu UNIX powiedzą: „O tak, to" na pytanie o uprawnienia w systemie UNIX.

TEST

a. Jakie są trzy uprawnienia UNIX?

b. Krótko scharakteryzuj każdy.

c. Porównaj liczbę uprawnień do katalogów i plików w systemie UNIX z uprawnieniami systemu Windows.

d. Do jakich trzech indywidualnych kont lub grup można przypisać uprawnienia do określonego katalogu w systemie UNIX?

e. Jak liczba kont lub grup, do których można przypisać uprawnienia w systemie UNIX, ma się do liczby w systemie Windows?

TWORZENIE SILNYCH HASEŁ

Na tym etapie historii komputerów jednym z najskuteczniejszych sposobów wzmocnienia hosta jest posiadanie silnego, chroniącego hasłem dostępu do systemu bazowego. W Części 5 przyjrzeliśmy się, jak opracować skuteczne polityki haseł w celu kontroli dostępu do systemu. Wymieniliśmy również kilka podstawowych wskazówek dotyczących tworzenia haseł.

• Mieć co najmniej osiem znaków.

• Miej co najmniej jedną zmianę przypadku, nie na początku hasła.

• Mieć co najmniej jedną cyfrę (od 0 do 9), nie na końcu hasła.

• Mieć co najmniej jeden znak niealfanumeryczny, nie na końcu hasła.

Jednak w tym rozdziale przyjrzymy się bliżej tworzeniu, przechowywaniu i łamaniu haseł. Pomimo tego, że wiedzą, co powinni robić, administratorzy systemów często ignorują ustalone zasady dotyczące haseł. Mogą otrzymać negatywne odpowiedzi od użytkowników, gdy próbują wymusić zasady dotyczące haseł. Mogą również nie rozumieć, jak łatwo można ukraść i złamać bazy danych haseł. Proces łamania haseł jest wysoce zautomatyzowany, wyrafinowany i metodyczny. Użytkownicy często są zaskoczeni, jak łatwo można złamać ich hasła. Mamy nadzieję, że zrozumienie sposobu tworzenia, przechowywania i łamania haseł pomoże zilustrować, dlaczego ważne jest egzekwowanie zasad omówionych w rozdziale 5. Przestrzeganie kilku prostych zasad dotyczących haseł może drastycznie zmniejszyć prawdopodobieństwo złamania haseł przez intruza w krótkim czasie czas.

Tworzenie i przechowywanie haseł

W 2009 roku RockYou miał 32 miliony kont użytkowników i haseł skradzionych w wyniku ataku SQL injection. Hakerzy mogli natychmiast uzyskać dostęp do milionów nazw użytkowników, adresów e-mail i haseł. Co gorsza, hasła były przechowywane jako zwykły tekst lub „jasne". Intruzi nie musieli złamać ani jednego hasła. Zazwyczaj hasła nie są przechowywane jako zwykły tekst. Skróty haseł są tworzone, gdy hasło jest przekazywane od użytkownika do funkcji mieszającej. Funkcja mieszająca zwraca skrót hasła o stałym rozmiarze (znany również jako skrót). Skrót hasła jest następnie przechowywany wraz z odpowiednią nazwą użytkownika i innymi informacjami o koncie. Samo hasło nie jest przechowywane. Przechowywany jest tylko skrót hasła.

TWORZENIE HASHA HASŁA

Załóżmy na przykład, że użytkownik chciał użyć „123456” jako swojego hasła. To hasło można następnie przekazać do wielu różnych funkcji haszujących. Poniżej znajduje się lista niektórych typowych funkcji skrótu używanych do tworzenia skrótów haseł. Każdej funkcji skrótu przekazano to samo hasło (123456), a zwrócono inny skrót hasła (rysunek 7-24).13 Z biegiem czasu systemy operacyjne korzystały z coraz bezpieczniejszych funkcji skrótu. Obecnie Microsoft Windows 7 używa NTLM (NT LAN Manager) do tworzenia skrótów haseł. Systemy Linux mogą używać DES, MD5, Blowfish lub SHA.

PRZECHOWYWANIE HASEŁ

Hasła systemu Windows są przechowywane w pliku rejestru menedżera kont zabezpieczeń (SAM) lub w bazie danych usługi Active Directory. Systemy Linux przechowują hasła w plikach tekstowych /etc/passwd lub /etc/shadow. Każdy wiersz pliku tekstowego reprezentuje indywidualne konto użytkownika z wieloma polami oddzielonymi dwukropkiem. Poniższy przykład pokazuje nazwy użytkowników, numery użytkowników, skróty LM (w tym przypadku puste) i skróty haseł NTLM (pogrubione) dla dwóch użytkowników w systemie Microsoft Windows 7.

JohnDoe:1012:BRAK HASŁA:32ED87BDB5FDC5E9CBA88547376818D4:::

JaneDoe:1013:BRAK HASŁA:328727B81CA05805A68EF26ACB252039:::

Poniższy przykład pokazuje nazwy użytkowników, „x” oznacza plik z hasłami w tle, identyfikatory użytkowników, identyfikatory grup, opis (GECOS), katalogi domowe dla każdego użytkownika i powłokę uruchomioną dla dwóch użytkowników w systemie Linux. Poniżej znajduje się zawartość pliku /etc/passwd.

JohnDoe:x:1012:1012:JanKowalski:/dom/JanKowalski:/bin/bash

JohnDoe:x:1013:1013:JaneKowalski:/home/JaneKowalski:/bin/bash

Plik cień (/etc/shadow) oddziela skróty haseł od innych informacji o użytkowniku i ogranicza dostęp, aby tylko superużytkownicy mogli uzyskać dostęp do pliku. Plik /etc/passwd może być odczytywany przez wszystkich użytkowników i modyfikowany przez użytkowników z uprawnieniami administratora. Jednak dostęp do pliku /etc/shadow mają tylko superużytkownicy. Ukrywanie pliku haseł utrudnia osobie atakującej uzyskanie skrótów haseł ze względu na ograniczony dostęp. Osoba atakująca musiałaby mieć uprawnienia administratora, aby uzyskać dostęp do pliku cienia. Poniżej znajduje się zawartość pliku /etc/shadow, w tym zaszyfrowane hasła (pogrubione) dla tych samych dwóch użytkowników pokazanych w powyższym pliku /etc/passwd.

JohnDoe:1teiYJiRh$wcSt61iRv7abpobqbU35z0:0:0:99999:7:::

JaneDoe:1Mj1.UYSq$h9Zgw5afTQCF.DR.KAMmx/:0:0:99999:7:::

KRADZIEŻ HASŁA

W rzeczywistości kradzież skrótów haseł ze zdalnego komputera może być poważną przeszkodą. Zazwyczaj atakujący musi uzyskać dostęp do systemu, uzyskać uprawnienia administratora, a następnie wydobyć kopię bazy haseł. Tylko wtedy atakujący może złamać hasła lokalnie. Zdobycie zestawu umiejętności niezbędnych do zdalnej kradzieży bazy haseł, bez złapania, nie jest trywialne i może zająć wiele lat. Tworzy to barierę opartą na umiejętnościach, która zapobiega wielu atakom. Może jednak również tworzyć fałszywe poczucie bezpieczeństwa. Administratorzy systemów mogą

błędnie założyć, że prawdopodobieństwo kradzieży bazy haseł przez atakującego jest tak niskie, że nie muszą egzekwować zasad dotyczących haseł.

Techniki łamania haseł

Programy do łamania haseł generalnie umożliwiają atakującemu użycie czterech metod łamania haseł. Są to zgadywanie siłowe, ataki słownikowe, hybrydowe ataki słownikowe i tęczowe tablice.

ZGRYWANIE BRUTE-FORCE

Oczywistym podejściem do łamania haseł jest wypróbowanie wszystkich możliwych haseł na wszystkich (lub wybranych) kontach. To podejście brute-force próbuje wszystkich możliwych haseł jednoznakowych, a następnie wszystkich możliwych haseł dwuznakowych i tak dalej. Atakujący może ograniczyć zgadywanie metodą brute-force do 26 liter alfabetu, do 52 wielkich i małych liter, do 62 znaków alfanumerycznych (litery i cyfry od 0 do 9) lub do około 75 znaków, które można wpisać na klawiaturze. Szersze zestawy znaków wymagają, aby cracker wypróbował o wiele więcej kombinacji na znak. Jeśli hasło ma długość N znaków, należy wypróbować 26^N możliwych kombinacji, jeśli użyto prostych małych (lub wielkich) liter. Używanie w hasłach zarówno wielkich, jak i małych liter zwiększa liczbę kombinacji dla N znaków do 52^N. Użycie znaków alfanumerycznych (zarówno liter jak i cyfr) zwiększa ten do 62^N, a użycie wszystkich znaków klawiatury zwiększa liczbę możliwych kombinacji do około 75^N. Hasła wykorzystujące kilka rodzajów znaków klawiaturowych są nazywane hasłami złożonymi

Hasła wykorzystujące kilka rodzajów znaków klawiaturowych są nazywane hasłami złożonymi

Oprócz złożoności hasła, długość hasła jest ważna dla ochrony przed atakami typu brute-force. Dłuższe hasła wymagają, aby program do łamania haseł spróbował więcej kombinacji, aby odnieść sukces. Nawet w prostej sytuacji haseł alfabetycznych bez rozróżniania wielkości liter, liczba możliwości szybko rośnie wraz z długością hasła. W przypadku haseł dwuznakowych istnieje 676 możliwości z hasłami tylko małymi literami. Zwiększenie długości hasła do czterech znaków zwiększa liczbę możliwości do ponad 400 000. Z sześcioma postaciami istnieje ponad 300 milionów możliwości. Biorąc pod uwagę szybkość komputerów, które mogą być używane do łamania haseł, dzisiejsze hasła muszą mieć co najmniej osiem znaków, nawet jeśli hasła różnią się wielkością liter i zawierają cyfry oraz znaki specjalne.

Zwiększenie długości hasła wykładniczo wydłuża czas łamania haseł metodą brute-force.

Przeciętnie atakujący będzie musiał wypróbować połowę wszystkich możliwych kombinacji, zanim znajdzie właściwą. Jednak ze względu na losowość zgadywanie metodą brute-force czasami znajduje hasło po stosunkowo niewielkiej liczbie prób.

ATAKI SŁOWNIKOWE NA WSPÓLNE HASŁA SŁOWNE

Niewiele osób ma hasła, które są prawdziwymi przypadkowymi kombinacjami liter, cyfr i innych znaków klawiatury. Zamiast tego wielu użytkowników tworzy popularne hasła słowne, takie jak benzyna. Mogą również używać imion krewnych lub zwierząt domowych. Mogą nawet użyć najgłupszego hasła ze wszystkich, hasła. Ankieta Pentasafe Security Technologies przeprowadzona wśród 15 000 pracowników w 600 organizacjach w Stanach Zjednoczonych i Europie wykazała, że 25% używało popularnych słów słownikowych. Pięćdziesiąt procent używało imion członków rodziny, przyjaciół lub zwierząt domowych. Trzydzieści procent używało nazwisk popowych idoli lub bohaterów sportu. Dziesięć procent oparło swoje hasła na fikcyjnych postaciach. Tylko 10 procent używało skomplikowanych, trudnych do złamania haseł. Chociaż istnieją miliony losowych kombinacji znaków,

które mają co najmniej osiem znaków, istnieje tylko kilka tysięcy popularnych słów w dowolnym języku. Plik tekstowy pokazany na rysunku 7-27 to plik słownika zawierający 17,5 miliona słów z każdego dostępnego języka pisanego. Użycie obcego słowa w haśle nie zwiększa znacząco jego siły. Ataki słownikowe porównują hasła z listami popularnych słów. Jeśli użytkownik wybierze popularne hasło, złamanie go zwykle zajmie tylko kilka sekund. Powszechnie dostępne są pliki słowników zawierające każde słowo w każdym języku. Istnieją również niestandardowe pliki słowników, które zawierają słowa związane ze sportem, gwiazdami, muzyką, slangiem, wszystkimi możliwymi datami, nazwiskami, wulgaryzmami i tak dalej. Zasadniczo można użyć każdego słowa pisanego. Niektórzy użytkownicy tworzą frazy wielowyrazowe, takie jak Nowisthetime. Ataki słownikowe również wyszukują takie popularne frazy i mogą automatycznie przeszukiwać wszystkie możliwe kombinacje wielowyrazowe. Chociaż wypróbowanie wszystkich możliwych kombinacji wielowyrazowych zajęłoby więcej czasu, całkowity czas wyszukiwania nadal stanowiłby ułamek całkowitego czasu wymaganego do przeszukania całej przestrzeni kluczy.

ATAKI SŁOWNIKA HYBRYDOWEGO

Wielu użytkowników próbuje modyfikować popularne hasła w prosty sposób, na przykład umieszczając pojedynczą cyfrę na końcu słowa lub używając tylko pierwszej litery. Przykładem może być Hasło1. Hybrydowe ataki słownikowe próbują prostych modyfikacji popularnych słów zawartych w pliku słownika. Te predefiniowane modyfikacje nazywane są regułami maglowania. Reguły maglowania można dostosowywać i mogą tworzyć oszałamiającą tablicę możliwych haseł z jednego słowa słownikowego. Hybrydowe ataki słownikowe są skuteczne przeciwko pochodnym popularnych haseł. Niektóre z nich to między innymi:

• Dodawanie numerów (1 hasło, hasło1, 1492hasło itp.)

• Odwrotna pisownia (drowssap)

• Dwukrotne wprowadzenie hasła (hasłohasło)

• Próbowanie hasła ze wszystkimi możliwymi zmianami w przypadku (PaSsWoRd)

• Używanie pisowni leet „l337” (pa55word)

• Usuwanie znaków (pswrd)

• Wypróbowanie kluczowych wzorców (asdfghjkl;, qwertyuiop itp.)

• Dodanie wszystkich prefiksów i sufiksów (hasło, posthasło itp.)

• Próbowanie wyprowadzeń nazwy użytkownika, adresu e-mail lub innych informacji o koncie zawartych w pliku hasła

Hybrydowe ataki słownikowe są skuteczne, ponieważ większość użytkowników wybiera hasła pochodzące ze słowników. Słowa ze słownika są łatwe do zapamiętania i zwykle mają znaczenie dla użytkownika. Niestety, użytkownicy mają tendencję do przekonania, że drobne modyfikacje słów w słowniku uniemożliwią atakującym odgadnięcie ich haseł. Osoby atakujące są już świadome typowych modyfikacji, jakie użytkownicy wprowadzają do swoich haseł.

TĘCZOWE TABELE

Innym sposobem złamania hasła jest sprawdzenie skrótu hasła w tęczowej tabeli. Tęczowa tabela to lista wstępnie obliczonych skrótów haseł, które są indeksowane. Atakujący może stworzyć dużą tabelę możliwych haseł i ich skrótów. Atakujący następnie indeksuje skróty, aby przyspieszyć proces łamania.

Skutkuje to kompromisem między pamięcią czasu i większą ilością pamięci do przechowywania wstępnie obliczonych skrótów haseł, ale czas potrzebny na złamanie hasła jest znacznie skrócony. Na przykład możliwe jest utworzenie kolekcji tęczowych tabel (skróty NTLM) zawierających każdy możliwy skrót hasła dla każdej możliwej kombinacji cyfr, wielkich i małych liter oraz znaków specjalnych (niealfanumerycznych). W przypadku wszystkich haseł zawierających od jednego do sześciu znaków utworzenie 6 GB wstępnie obliczonych i posortowanych skrótów haseł zajęłoby około 37 dni. Jednak każde hasło składające się z sześciu znaków lub mniej może zostać złamane w mniej niż 16 minut. Gdy skradziony skrót hasła pasuje do wstępnie obliczonego skrótu, osoba atakująca zna oryginalne hasło użyte do utworzenia skradzionego hasła.

TEST

a. Co to jest zgadywanie haseł metodą brute-force?

b. Dlaczego ważne jest, aby nie używać tylko małych liter w hasłach?

c. Czym są złożone hasła?

d. Dlaczego długość hasła jest ważna?

e. Co to jest atak słownikowy?

f. Dlaczego ataki słownikowe są szybsze niż zgadywanie metodą brute-force?

g. Czym są hybrydowe ataki słownikowe?

h. W jaki sposób stosuje się reguły manglowania do listy słów słownikowych?

a. Czym są tęczowe tabele?

b. Jak tęczowe tablice skróciłyby czas potrzebny na złamanie hasła?

c. Czy byłoby możliwe stworzenie tęczowych tablic dla wszystkich możliwych haseł o długości od 1 do 20 znaków? Czy byłoby to praktyczne?

PRAWDZIWIE LOSOWE HASŁA

Chociaż tri6#Vial jest dość silnym hasłem, najlepsze hasła to długie i naprawdę losowe ciągi wielkich i małych liter, cyfr i znaków specjalnych. Niestety, takie hasła są prawie niemożliwe do zapamiętania, a niewielu użytkowników nawet spróbuje je zapamiętać. Zamiast tego użytkownicy zapisują je obok komputera, a nawet na krawędzi wyświetlacza. Może to być nawet bardziej niebezpieczne niż użycie nieco znaczącego ciągu, który użytkownicy faktycznie zapamiętają, takiego jak tri6#Vial lub

I82#sofbananas@home. Jednak w przypadku niezwykle ważnych kont, takich jak konta superużytkowników, bardzo długie losowe hasła są koniecznością. Hasła te należy zapisać, a następnie bezpiecznie zablokować.

TESTOWANIE I WYKONYWANIE SIŁY HASŁ

Administratorzy systemów mogą uruchomić program do łamania haseł na swoich własnych serwerach, aby sprawdzić, czy nie doszło do naruszeń zasad dotyczących długości i złożoności haseł. Ponadto większość systemów operacyjnych można teraz skonfigurować tak, aby wymusić wybór stosunkowo silnych haseł przez użytkowników. Testowanie haseł za pomocą programów do łamania haseł nigdy nie powinno odbywać się bez pisemnej zgody przełożonego testera. Nawet jeśli testowanie jest dorozumiane lub jawne w opisie stanowiska testera, tester ryzykuje zwolnieniem, a nawet ściganiem, jeśli firma podejrzewa, że tester wykonuje określony test w nielegalnych celach.

INNE ZAGROŻENIA DOTYCZĄCE HASŁA

Programy do przechwytywania naciśnięć klawiszy i kradzieży haseł.

Program do przechwytywania naciśnięć klawiszy kradnie hasła, gdy użytkownik je wpisuje, i wysyła naciśnięcia klawiszy do atakującego. Atakujący może następnie przeszukać dane dotyczące naciśnięć klawiszy w celu znalezienia nazw kont i haseł. Mówiąc bardziej bezpośrednio, programy kradnące hasła wyświetlają użytkownikowi fałszywy ekran logowania i proszą go o ponowne zalogowanie. Następnie wyśle te informacje do atakującego.

Fizyczne keyloggery również rejestrują naciśnięcia klawiszy. Niektóre fizyczne keyloggery są całkowicie niewykrywalne przez oprogramowanie i mogą przechowywać dane dotyczące naciśnięć klawiszy z kilku lat. Inne można skonfigurować tak, aby uzyskiwały dostęp do lokalnych sieci bezprzewodowych i przesyłały naciśnięcia klawiszy z powrotem do właściciela. Większość fizycznych keyloggerów musi zostać pobrana, aby uzyskać dostęp do zarejestrowanych danych.

Surfowanie na ramieniu.

Powinna istnieć zasada, zgodnie z którą pracownicy nigdy nie powinni pozwalać nikomu na oglądanie podczas wprowadzania hasła – jest to praktyka znana jako „short surfing". Atakujący może nawet skorzystać na uzyskaniu częściowych informacji, takich jak długość hasła (co znacznie skróciłoby czas potrzebny na zgadywanie metodą brute-force) lub o wciskanych klawiszach (takich jak p*ss***d, gdzie gwiazdki wskazać litery, których nie można było odczytać). Surferzy na ramieniu często rozmawiają ze swoimi ofiarami podczas wprowadzania hasła, ponieważ spowalnia to czas pisania, dzięki czemu litery są łatwiejsze do odczytania.

TEST

a. Czy możesz stworzyć naprawdę losowe hasło? Czy będzie używany?

b. Czy hasła powinny być testowane przez administratorów systemów? Czemu?

a. Co robią programy do przechwytywania haseł przez konie trojańskie?

b. Czy oprogramowanie antywirusowe może wykrywać oprogramowanie do przechwytywania naciśnięć klawiszy?

c. Jak wykryłbyś fizyczny keylogger?

d. Czym jest surfing na ramieniu?

e. Czy bark surfera musi przeczytać całe hasło, aby odnieść sukces? Wyjaśniać.

TESTOWANIE POD KĄTEM LUK W ZABEZPIECZENIACH

Nawet jeśli firmy starają się starannie wdrażać zabezpieczenia, planiści i realizatorzy nieuchronnie popełniają błędy ze względu na złożoność wielu zabezpieczeń, które muszą wdrożyć. Testy podatności próbują znaleźć wszelkie słabości w pakiecie ochrony firmy, zanim zrobią to atakujący, dzięki czemu administrator systemu będzie wiedział, jakie prace należy wykonać. Aby przeprowadzić testy podatności, administrator bezpieczeństwa instaluje oprogramowanie do testowania podatności na swoim komputerze, a następnie uruchamia je na serwerach w obszarze zainteresowania administratora bezpieczeństwa. Programy te przeprowadzają serię ataków na serwery, a następnie generują raporty zawierające szczegółowe informacje o lukach w zabezpieczeniach, które wykryły na serwerach. Chociaż oprogramowanie do testowania podatności jest łatwe do uruchomienia, nie ma ono sensu, chyba że tester podatności nie ma gruntownej wiedzy na temat ataków, które

przeprowadza i co oznaczają raporty o podatnościach. To nie są narzędzia do bezmózgiego działania. Testami podatności należy zarządzać bardzo ostrożnie, aby chronić karierę testerów podatności. Atakujący używają również narzędzi do testowania podatności. Wielu administratorów bezpieczeństwa „przeszło na ciemną stronę", używając oprogramowania do testowania luk w zabezpieczeniach, aby pomóc im zaatakować własne firmy. Było kilka przypadków administratorów bezpieczeństwa, którzy stracili pracę, a nawet trafili do więzienia za przeprowadzanie testów podatności bez odpowiedniej autoryzacji. Twierdzenie, że ci administratorzy bezpieczeństwa przeprowadzali testy podatności w ramach swoich opisów stanowisk, nie sprawdziły się w korporacji ani w sądach. Przed przystąpieniem do testowania podatności ważne jest, aby stworzyć plan testowania podatności zawierający szczegółowy opis tego, co zostanie zrobione. Plan powinien również ostrzegać, że testy podatności czasami powodują awarie komputerów i powodują inne szkody. Ważne jest wtedy, aby przełożony testera podpisał plan zatwierdzenia i przyznał, że można wyrządzić szkodę. Testerzy podatności nazywają te podpisane plany kartami „wyjść z więzienia". Ostatnią rzeczą, jaką należy wiedzieć o planach testowania, jest to, że odstępstwo od uzgodnionego planu usuwa wszystkie zabezpieczenia.

TEST

a. Dlaczego pożądane jest testowanie podatności?

b. Jakie dwie rzeczy robi oprogramowanie do testowania podatności?

c. Dlaczego ważne jest uzyskanie pisemnej zgody przed przeprowadzeniem testu podatności?

d. O jakich dwóch rzeczach powinna wyraźnie wspomnieć ta pisemna zgoda?

e. Dlaczego ważne jest, aby nigdy nie odbiegać od planu testów podczas przeprowadzania testów?

Bezpieczeństwo komputera klienckiego z systemem Windows

Jak dotąd w w dużej mierze skupialiśmy się na serwerach. Oczywiście korporacje muszą również zabezpieczyć swoje komputery klienckie, których jest znacznie więcej. Skoncentrujemy się na bezpieczeństwie komputerów klienckich z systemem Windows ze względu na dominację systemu Windows na rynku klienckim.

Podstawy bezpieczeństwa komputera klienckiego

Aby chronić klientów, firmy potrzebują baz bezpieczeństwa dla każdej wersji systemu operacyjnego. Na przykład, firma potrzebuje baz bezpieczeństwa dla Windows XP, Windows Vista i Windows 7. Afirm potrzebuje także baz bezpieczeństwa dla swoich komputerów stacjonarnych Macintosh, Linux i UNIX. Ponadto dla każdego klienckiego systemu operacyjnego firma może mieć wiele punktów odniesienia, takich jak komputery stacjonarne i laptopy, komputery stacjonarne i zewnętrzne oraz zwykłe klienty i komputery o szczególnie wysokich wymaganiach w zakresie bezpieczeństwa.

TEST

a. Jakich różnych poziomów bazowych firma potrzebuje dla swoich komputerów klienckich?

Centrum akcji systemu Windows

Dodatek Service Pack 2 (SP2) dla systemu Windows XP wprowadził Centrum zabezpieczeń systemu Windows, aby umożliwić użytkownikowi szybkie sprawdzenie stanu głównych ustawień stanu zabezpieczeń komputera. System Windows Vista rozszerzył Centrum zabezpieczeń systemu Windows o więcej opcji zabezpieczeń. W systemie Windows 7 Centrum zabezpieczeń systemu Windows zostało

zastąpione szerszym Centrum akcji systemu Windows. Centrum akcji systemu Windows zawiera krótkie podsumowanie wszystkich składników zabezpieczeń potrzebnych do wzmocnienia komputera klienckiego. Rysunek 7-31 przedstawia Centrum akcji systemu Windows w systemie Windows 7. Każdy z tych indywidualnych składników zabezpieczeń można skonfigurować w kategorii System i zabezpieczenia w Panelu sterowania. Aby odpowiednio wzmocnić komputer kliencki, ważne jest, aby każdy składnik zabezpieczeń był włączony. Te składniki obejmują Zaporę systemu Windows, Windows Update, ochronę przed wirusami, ochronę przed oprogramowaniem szpiegującym, ustawienia zabezpieczeń internetowych, kontrolę konta użytkownika i ochronę dostępu do sieci. Razem zapewniają dogłębną obronę i ochronę przed różnymi zagrożeniami.

TEST

a. Jak szybko ocenić stan bezpieczeństwa swojego komputera z systemem Windows?

b. Co zawiera krótkie podsumowanie składników zabezpieczeń potrzebnych do wzmocnienia komputera klienckiego?

c. Dlaczego konieczne są różne rodzaje ochrony?

Zapora systemu Windows

Dodatek SP2 dla systemu Windows XP wprowadził Zaporę systemu Windows. Ta zapora stanowa inspekcji pakietów (SPI) została dołączona do wszystkich kolejnych klienckich wersji systemu Windows. Centrum akcji umożliwia użytkownikom sprawdzanie stanu instalacji Zapory systemu Windows. Windows 7 jest wyposażony w znacznie ulepszoną zaporę sieciową z dodatkowymi funkcjami, takimi jak niestandardowe reguły wejścia/wyjścia, oddzielne profile sieciowe, bardziej szczegółowe reguły i możliwość zarządzania za pomocą zasad grupy.

TEST

a. Jaka zapora sieciowa SPI jest dostarczana z kliencką wersją systemu Windows od czasu wydania dodatku SP2 dla systemu Windows XP?

b. Jakie ulepszenia są dostępne w Zaporze systemu Windows z zabezpieczeniami zaawansowanymi?

Automatyczne aktualizacje

Użytkownik może skonfigurować automatyczne aktualizacje, aby automatycznie pobierać i instalować aktualizacje systemu operacyjnego (poprawki). Posiada również inne opcje, w tym powiadamianie użytkownika o pobranych plikach i pozwalanie użytkownikowi zdecydować, kiedy je zainstalować. Ze względu na krótki czas między wydaniem łatek a powszechnym wykorzystaniem exploitów wykorzystujących załataną lukę, całkowicie automatyczne działanie jest jedyną rzeczą, która ma sens w przypadku komputerów PC w korporacjach.

TEST

22. Dlaczego aktualizacja powinna być wykonywana całkowicie automatycznie na komputerach klienckich?

Ochrona antywirusowa i spyware

Ochrona antywirusowa ma kluczowe znaczenie, ale łatwo jest spowodować, że programy antywirusowe staną się nieskuteczne.

• Użytkownik może wyłączyć program antywirusowy, ponieważ spowalnia on komputer (i to robi) lub ponieważ nie pozwala użytkownikowi na pobranie czegoś lub otwarcie załącznika (prawdopodobnie mądrze).

• Bardziej subtelnie, użytkownik mógł wyłączyć automatyczne pobieranie nowych sygnatur wirusów lub zaplanować aktualizacje na środek nocy, gdy komputer jest wyłączony. To źle, ponieważ użytkownik nadal myśli, że jest chroniony.

• Wreszcie, użytkownik może nie płacić rocznej opłaty; jest to podstępne, ponieważ chociaż ochrona antywirusowa wydaje się działać dobrze, nie będzie aktualizacji dla wirusów i innego złośliwego oprogramowania po zakończeniu umowy.

Centrum zabezpieczeń systemu Windows wskazuje, czy program antywirusowy działa skutecznie. Jednak informacje, które przedstawia, różnią się nieco między dostawcami.

TEST

a. Co może się nie udać z ochroną antywirusową?

Wdrażanie Polityki Bezpieczeństwa

Polityki bezpieczeństwa omówione w Części 2 i polityki haseł omówione w rozdziale 5 niewiele znaczą, jeśli nie zostaną zaimplementowane. Istnieją zasady bezpieczeństwa, które chronią zasoby komputerowe przed uszkodzeniem. Korporacje mogą nawet zostać pociągnięte do odpowiedzialności za niewdrożenie określonych zasad bezpieczeństwa wymaganych przez prawo.

ZASADY HASŁA

Opcje polityki haseł umożliwiają administratorom systemów egzekwowanie wymagań dotyczących złożoności, minimalnej długości hasła, maksymalnego wieku hasła i historii haseł. Wdrożenie tych polityk haseł zwiększa skuteczność haseł jako mechanizmu kontroli dostępu.

ZASADY KONTA

Hosta można zabezpieczyć przed atakami zewnętrznymi, wdrażając podstawowe zasady dotyczące kont. Te zasady kont, zapobiegają niekończącej się próbie odgadnięcia hasła użytkownika przez atakującego. Konto zostanie zablokowane po określonej liczbie niepoprawnych loginów. Konto pozostawałoby również zablokowane przez określony czas. To sprawiłoby, że zgadywanie hasła byłoby nieskuteczne.

POLITYKA AUDYTU

Wreszcie, zasady audytu zapewniłyby ścieżkę audytu dla zdarzeń systemowych. Tymi zdarzeniami systemowymi mogą być ataki, próby wyłączenia zabezpieczeń, zmiany uprawnień i tak dalej. Wdrożenie zasad audytu zapewnia administratorom systemów szczegółowe informacje o tym, kto spowodował te zdarzenia (tj. który użytkownik próbował zalogować się zdalnie), co mogli zmienić (tj. podnieśli uprawnienia użytkownika bez autoryzacji) i kiedy zdarzenie miało miejsce. Rysunek 7-35 przedstawia ustawienia polityki audytu dostępne na każdym hoście Microsoft Windows 7. Administratorzy mogą śledzić zdarzenia logowania do konta, zmiany konta, zmiany zasad, wykorzystanie uprawnień i tak dalej. Informowanie użytkowników, że zdarzenia systemowe są rejestrowane i poddawane audytowi, może zniechęcać do niewłaściwego zachowania. Zasady inspekcji mogą być również używane do zbierania informacji o atakach. Te dzienniki mogą później zostać wykorzystane przeciwko atakującym w postępowaniu sądowym.

TEST

a. Dlaczego ważne jest wdrożenie polityki bezpieczeństwa?

b. Jakie są zalety wdrożenia zasad haseł?

c. Jakie są zalety wdrożenia zasad konta?

d. Jakie są zalety wdrażania zasad audytu?

Ochrona notebooków

Notebooki wymagają specjalnej ochrony, ponieważ każdego roku wiele z nich jest gubionych lub kradzionych.

ZAGROŻENIA

Każdy notebook stanowi znaczną inwestycję kapitałową. Co ważniejsze, wszystkie dane, które nie zostały zarchiwizowane, zostaną utracone. W przypadku kradzieży sprzęt jest drogi, ale wartość utraconych danych zwykle jest znacznie większa. Trzecią kwestią jest to, że komputer może zawierać dane wrażliwe, w tym dane klientów prywatnych lub własność intelektualną; to jest najgorsza sytuacja.

UTWORZYĆ KOPIĘ ZAPASOWĄ

Niewiele skradzionych (lub nawet zgubionych) komputerów zostaje odzyskanych. Kopia zapasowa ma kluczowe znaczenie dla ochrony przed utratą danych roboczych i dokumentów, które będą musiały zostać odtworzone. Przed wywiezieniem notebooka należy wykonać kopię zapasową. Jeśli zostanie zabrany poza witrynę na dłużej niż kilka godzin, należy często tworzyć kopie zapasowe poza siedzibą firmy.

ZASADY DOTYCZĄCE DANYCH WRAŻLIWYCH

W przypadku danych wrażliwych firma musi opracować silne zasady i musi je silnie egzekwować. Poniżej znajdują się cztery zasady, które mogą pomóc w ochronie poufnych danych. Po pierwsze i najważniejsze, zasady powinny zdecydowanie ograniczać, jakie dane wrażliwe mogą być w ogóle przechowywane na komputerach przenośnych. Poufne dane powinny być dozwolone na przenośnych komputerach PC tylko po dokładnym przemyśleniu i najlepiej za podpisaną zgodą przełożonego danej osoby. Mogą nawet istnieć specjalne zasady dotyczące rodzaju informacji, których nie wolno zabierać poza witrynę w ogóle lub tylko po uzyskaniu autoryzacji na bardzo wysokim poziomie. Po drugie, szyfrowanie musi być wymagane na wszystkich komputerach przenośnych, niezależnie od zawartych w nich informacji. Szyfrowanie zmniejszy ryzyko utraty tajemnic handlowych lub prywatnych informacji. W wielu stanach utrata danych osobowych wymaga powiadomienia wszystkich osób, których prywatne informacje zostały ujawnione. Zazwyczaj jednak to powiadomienie nie jest wymagane, jeśli prywatne informacje są odpowiednio zaszyfrowane. Po trzecie, notebooki muszą być chronione silnymi hasłami lub danymi biometrycznymi. W ten sposób, jeśli ktoś wejdzie w posiadanie komputera, nie może z niego korzystać. Większość szyfrowania jest niewidoczna dla zalogowanych użytkowników, co oznacza, że każdy, kto ma hasło logowania do komputera, nie będzie nawet wiedział, że dane są zaszyfrowane. Oczywiście, jeśli atakujący nie może się zalogować, nie może odczytać zaszyfrowanych danych. Po czwarte, dobrą polityką jest wymaganie audytu pierwszych trzech polityk. Te cztery zasady należy stosować do wszystkich danych mobilnych na dyskach notebooków, dyskach RAM USB, odtwarzaczach MP3, a nawet telefonach komórkowych, które mogą przechowywać dane.

SZKOLENIE

Innym zabezpieczeniem jest nauczenie osób korzystających z urządzeń przenośnych o zagrożeniach, jakie stwarzają urządzenia mobilne oraz o tym, jak uniknąć kradzieży i utraty (na przykład podczas meldowania się w hotelu umieść urządzenie przenośne na ladzie, a nie u swoich stóp).

OPROGRAMOWANIE DO ODZYSKIWANIA KOMPUTERÓW

Możliwe jest również zainstalowanie oprogramowania do odzyskiwania komputera na komputerach przenośnych, aby umożliwić odzyskanie niektórych zgubionych lub skradzionych notebooków. Gdy notebook łączy się z Internetem, oprogramowanie do odzyskiwania komputera zgłasza swój adres IP firmie zajmującej się odzyskiwaniem. Firma zajmująca się oprogramowaniem do odzyskiwania współpracuje z lokalną policją w celu odzyskania notebooka.

TEST

a. Jakie są trzy zagrożenia związane z utratą lub kradzieżą notebooka?

b. Kiedy należy wykonać kopię zapasową na komputerach mobilnych?

c. Jakie cztery zasady są niezbędne do ochrony poufnych informacji?

d. Do czego należy stosować te zasady?

e. Jakie szkolenie należy zapewnić?

f. Co robi oprogramowanie do odzyskiwania komputera?

Scentralizowane zarządzanie bezpieczeństwem komputera

Przeszkoleni administratorzy systemów zarządzają serwerami, ale zwykli użytkownicy zazwyczaj zarządzają własnymi komputerami klienckimi. Brak przeszkolenia w zakresie bezpieczeństwa hosta i zasad bezpieczeństwa komputerów firmowych powoduje, że użytkownicy często popełniają błędy w konfiguracji i korzystaniu ze swoich komputerów. W niektórych przypadkach świadomie naruszają firmowe zasady bezpieczeństwa komputerów PC. Firmy muszą mieć możliwość centralnego zarządzania komputerami klienckimi, aby zapewnić zgodność z dobrymi praktykami i politykami korporacyjnymi. Ponadto scentralizowane zarządzanie bezpieczeństwem komputerów PC często zawiera narzędzia do automatyzacji, które mogą zmniejszyć nakład pracy związany z egzekwowaniem zabezpieczeń. Przyjrzymy się trzem głównym podejściom do scentralizowanego zarządzania bezpieczeństwem komputerów PC.

KONFIGURACJE STANDARDOWE

Jedną ze strategii centralnego zarządzania komputerami klienckimi jest narzucanie klientom standardowych konfiguracji. Standardowe konfiguracje szczegółowo opisują sposób, w jaki należy skonfigurować komputery klienckie, w tym ważne opcje, programy użytkowe, a czasami cały interfejs użytkownika. Użytkownicy nie mogą dodawać nieautoryzowanych programów ani zmniejszać ustawień zabezpieczeń. Ogólnie rzecz biorąc, standardowe konfiguracje wymuszają korporacyjne zasady bezpieczeństwa, zmniejszając ryzyko błędów i naruszeń użytkowników. Ponadto standardowe konfiguracje znacznie upraszczają rozwiązywanie problemów z komputerem i ogólną konserwację. Bez standardowych konfiguracji narzędzia do rozwiązywania problemów często muszą radzić sobie z nieznanymi problemami, które obejmują subtelne interakcje między różnymi aplikacjami oraz między aplikacjami a konfiguracją systemu operacyjnego komputera. W standardowych konfiguracjach interakcje te są dobrze znane.

Rząd federalny Stanów Zjednoczonych nakazuje, aby wszystkie komputery PC rządu Stanów Zjednoczonych z systemem Windows XP lub Windows Vista były zgodne ze standardową konfiguracją o nazwie Federal Desktop Core Configuration.

KONTROLA DOSTĘPU DO SIECI

W większości przypadków początkowa kontrola dostępu jest bez znaczenia, jeśli komputery klienckie są zagrożone. Program wykorzystujący exploit będzie miał wszystkie uprawnienia dostępu uprawnionego użytkownika. Pojawiające się rozwiązanie polega na zainstalowaniu oprogramowania do kontroli dostępu do sieci (NAC) na komputerach, które będą łączyć się przez sieć. Jak sugeruje termin kontrola dostępu, NAC skupia się przede wszystkim na kontrolowaniu początkowego dostępu do sieci. Tak jak odwiedzający dany kraj mogą być sprawdzani pod kątem problemów zdrowotnych przed wjazdem do kraju, NAC analizuje stan bezpieczeństwa komputera klienckiego przed udzieleniem mu dostępu do sieci. Przede wszystkim robi to, wysyłając zapytanie do komputera o informacje prezentowane w Centrum zabezpieczeń systemu Windows lub Centrum akcji. Gwarantuje to, że komputer kliencki ma zainstalowaną automatyczną aktualizację, aktualny program antywirusowy i tak dalej. Jeśli komputer kliencki nie przejdzie wstępnej inspekcji NAC, istnieją dwie alternatywy. Jednym z nich jest po prostu zabronienie dostępu do sieci, dopóki użytkownik nie rozwiąże problemu. Częściej użytkownik otrzymuje dostęp do jednego serwera naprawczego. Z serwera naprawczego użytkownik może pobrać potrzebne aktualizacje, a następnie spróbować ponownie zaakceptować go przez punkt kontrolny NAC. Chociaż NAC kiedyś przyglądał się tylko wstępnej ocenie stanu, większość oprogramowania NAC obecnie monitoruje również ruch komputera klienckiego po początkowym dostępie. Jeśli komputer zacznie wysyłać ruch tworzony przez złośliwe oprogramowanie, centralny serwer NAC może odciąć komputer lub odesłać go do naprawy.

OBIEKTY POLITYKI GRUPY WINDOWS

Kontrolery domeny Microsoft Windows mogą przesyłać zestawy zasad, zwane obiektami zasad grupy (GPO), do grup komputerów klienckich. GPO umożliwiają firmie egzekwowanie drobnoziarnistych zasad kontrolowania różnych klas poszczególnych komputerów, takich jak ogólne komputery klienckie, komputery klienckie wysokiego ryzyka i komputery przenośne. Obiekty GPO są bardzo potężne. Na przykład mogą zablokować pulpit klienta, aby nie można go było zmienić. Ponadto mogą zapobiegać podłączaniu nośników wymiennych, takich jak dyski DVD i dyski flash USB. Ogólnie rzecz biorąc, obiekty zasad grupy są bardzo dobre do wymuszania standardowych konfiguracji i innych ważnych zasad. Poniżej znajdują się niektóre z zalet zapewnianych przez obiekty zasad grupy.

Spójność. Polityka bezpieczeństwa może być stosowana w całej organizacji jednolicie iw tym samym czasie.

Zmniejszone koszty administracyjne. Polityki korporacyjne można tworzyć, stosować i zarządzać za pomocą jednej konsoli zarządzania lub delegować do kilku administratorów.

Zgodność. Firma może zapewnić zgodność z prawem i przepisami. Sprawozdawczość i audyt są również znacznie prostsze.

Kontrola. Edytor zarządzania zasadami grupy zawiera dużą liczbę wbudowanych zasad bezpieczeństwa. Zapewnia szczegółowy poziom kontroli nad użytkownikami, komputerami, aplikacjami i zadaniami.

TEST

a. Dlaczego pożądane jest centralne zarządzanie bezpieczeństwem komputera?

b. Dlaczego standardowe konfiguracje są atrakcyjne?

c. Co robi NAC, gdy komputer próbuje połączyć się z siecią?

d. Jeśli komputer nie przejdzie wstępnej oceny stanu zdrowia, jakie są dwie opcje systemu NAC?

e Czy kontrola NAC zwykle zatrzymuje się po przyznaniu dostępu?

f. Jakie rzeczy mogą ograniczać obiekty zasad grupy systemu Windows?

g. Dlaczego obiekty GPO systemu Windows są potężnymi narzędziami do zarządzania zabezpieczeniami na poszczególnych komputerach z systemem Windows?

WNIOSEK

Host jest ostatnią linią obrony dla udaremnienia ataków. Host to dowolne urządzenie z adresem IP i ważne jest, aby wzmocnić wszystkie hosty. Dotyczy to zwłaszcza serwerów, routerów i zapór ogniowych, ale dotyczy to również komputerów klienckich, a nawet telefonów komórkowych. Atakujący może użyć zhakowanego komputera klienckiego do obejścia zapór i wszystkich innych zabezpieczeń. Hartowanie to duży zestaw różnorodnych zabezpieczeń, które należy zastosować, aby zmniejszyć ryzyko w przypadku zaatakowania hosta. Biorąc pod uwagę złożoność utwardzania hosta, ważne jest, aby postępować zgodnie z podstawowymi zasadami bezpieczeństwa dla konkretnej wersji systemu operacyjnego, na którym działa host, chociaż możliwe jest również zapisywanie obrazów dobrze przetestowanych hostów, a następnie pobieranie tych obrazów dysków na inne komputery . Przyjrzeliśmy się systemom operacyjnym Microsoft Windows Server dla serwerów. Najnowsze wersje systemu Microsoft Windows Server mają graficzne interfejsy użytkownika (GUI), które wyglądają jak interfejsy użytkownika w klienckich wersjach systemu Windows. Przyjrzeliśmy się wielu elementom bezpieczeństwa systemu Windows, który wykorzystuje narzędzia GUI, zwłaszcza konsole zarządzania Microsoft (MMC). Trudno mówić ogólnie o wzmacnianiu systemu UNIX, ponieważ istnieje kilka wersji systemu UNIX, które oferują różne narzędzia do administrowania systemami, w tym narzędzia bezpieczeństwa. Na komputerach PC Linux to rodzina wersji UNIX; chociaż wszystkie wersje Linuksa używają tego samego jądra Linuksa, są one oferowane jako „dystrybucje", które korzystają z wielu innych programów, a programy te różnią się w zależności od dystrybucji. Chociaż wersje UNIX (w tym Linux) oferują pewne GUI, wiele narzędzi bezpieczeństwa musi być uruchamianych z powłok wiersza poleceń.

Przyjrzeliśmy się ważnemu tematowi luk i poprawek (zwłaszcza łatek). Biorąc pod uwagę dużą liczbę łat wydawanych każdego roku, firmy mają trudności z łataniem luk w zabezpieczeniach i często muszą ustalać priorytety łatek, które będą stosowane. W przypadku serwerów ważne jest, aby przetestować poprawki na maszynach testowych przed zainstalowaniem ich na serwerach produkcyjnych. Serwery zarządzania poprawkami automatyzują część prac związanych ze znajdowaniem poprawek i rozsyłaniem tych poprawek na serwery, które ich wymagają. Przyjrzeliśmy się, jak najnowsze wersje systemu Microsoft Windows Server tworzą konta użytkowników i grup oraz zarządzają nimi. Zobaczyliśmy też, jak można przypisywać uprawnienia użytkownikom i grupom w katalogach i poszczególnych plikach. Microsoft Windows oferuje 6 standardowych uprawnień, które można podzielić na 13 bardziej precyzyjnych uprawnień. W pliku lub katalogu system Windows może przypisywać różne uprawnienia wielu różnym użytkownikom i grupom. W przeciwieństwie do tego, UNIX ma tylko trzy uprawnienia i może je przypisać tylko właścicielowi, jednej grupie i reszcie świata. Uprawnienia we wszystkich systemach operacyjnych są dziedziczone z katalogów wyższego poziomu, więc inteligentny wybór struktury katalogów najwyższego poziomu dysku twardego w celu wykorzystania dziedziczenia może znacznie ograniczyć pracę związaną z przypisywaniem uprawnień. Przypisywanie uprawnień grupom zamiast poszczególnym osobom upraszcza również przypisywanie

uprawnień i ma dodatkową zaletę polegającą na zmniejszeniu liczby błędów. Krótko przyjrzeliśmy się bezpieczeństwu komputerów klienckich z systemem Windows, koncentrując się na systemie Windows

Action Center, czyli pulpit nawigacyjny różnych ustawień bezpieczeństwa na komputerze. Omówiliśmy zalety wdrożenia zasad dotyczących haseł, kont i audytów. Przyjrzeliśmy się w szczególności ochronie komputerów przenośnych poza siedzibą firmy, a także scentralizowanemu zarządzaniu bezpieczeństwem komputerów PC, które może egzekwować zasady na wielu komputerach. Scentralizowane zarządzanie bezpieczeństwem komputerów PC obejmuje korzystanie ze standardowych konfiguracji, kontroli dostępu do sieci (NAC) i obiektów zasad grupy systemu Windows (GPO). Jednym z aspektów utwardzania gospodarza, który nie został uwzględniony w tym rozdziale, jest bezpieczeństwo aplikacji. Jeśli atakujący mogą przejąć aplikację, zazwyczaj mogą wykonywać polecenia za zgodą zhakowanej aplikacji — często z uprawnieniami superużytkownika. Utwardzanie aplikacji jest obecnie prawdopodobnie najważniejszym aspektem utwardzania hosta. Z tego powodu ma swój własny rozdział, któremu przyjrzymy się dalej.

Pytania do przemyślenia

1. Jak myślisz, dlaczego firmy często nie odpowiednio wzmacniają swoje serwery?

2. Jak myślisz, dlaczego firmy często nie są w stanie odpowiednio zahartować swoich klientów?

3. (a) Jak zła jest różnorodność ofert Linux/UNIX? (b) Jak to jest dobre?

4. Jak myślisz, dlaczego UNIX ma tak ograniczone możliwości przypisywania uprawnień w porównaniu z Windows?

5. Katalog DunLaoghaire ma kilka podkatalogów. Każdy z tych podkatalogów zawiera bardzo wrażliwe informacje, które powinny być dostępne dla jednego użytkownika. Jakie uprawnienia nadałbyś w katalogu najwyższego poziomu DunLaoghaire grupie wszystkim zalogowanym użytkownikom, jeśli nie chcesz zmieniać domyślnej opcji Zezwalaj na propagowanie uprawnień dziedzicznych z obiektu nadrzędnego do tego pola obiektu w podkatalogach? (b) Co byś wtedy zrobił w każdym podkatalogu?

6. W swojej najczystszej postaci netbooki to komputery PC zaprojektowane tak, aby przechowywać na nich niewiele oprogramowania lub wcale. Zamiast tego są zaprojektowane do korzystania z chmury komputerowych, w których oprogramowanie i dane są przechowywane na serwerach internetowych. Netbooki w tej czystej postaci mogą działać tylko wtedy, gdy mają połączenie z Internetem. Opierając się na tym, czego nauczyłeś się, omów implikacje bezpieczeństwa dla netbooków, zarówno za, jak i przeciw?

7. Jaka metoda łamania haseł zostałaby użyta dla każdego z poniższych haseł? (a) miecznik, (b) Lt6^, (c) Przetwarzanie1 i (d) nitt4aGm^.

8. Oceń bezpieczeństwo każdego z poniższych haseł, podając swoje konkretne uzasadnienie. (a) miecznik, (b) Lt6^, (c) Przetwarzanie1 i (d) nitt4aGm^.

BEZPIECZEŃSTWO APLIKACJI

BEZPIECZEŃSTWO APLIKACJI I UTWARDZANIE

W Części 7 przyjrzeliśmy się utwardzaniu hosta, skupiając się na systemie operacyjnym. Jednak równie ważne jest wzmocnienie aplikacji działających na hoście. Bezpieczeństwo aplikacji w rzeczywistości wymaga więcej pracy niż wzmacnianie systemu operacyjnego, ponieważ klienci i serwery uruchamiają wiele aplikacji. Każda aplikacja może być tak trudna do utwardzenia jak system operacyjny.

Wykonywanie poleceń z przywilejami zhakowanej aplikacji

Jeśli atakujący przejmie aplikację, zwykle może wykonać polecenia z uprawnieniami dostępu zaatakowanej aplikacji. Wiele aplikacji działa z rootem (uprawnienia superużytkownika), więc przejęcie ich daje atakującemu całkowitą kontrolę nad hostem. Często osoby atakujące mogą przejąć aplikację za pomocą jednej wiadomości, więc uzyskanie uprawnień roota jest znacznie łatwiejsze dzięki wykorzystaniu luk w aplikacjach niż w przypadku tradycyjnie trudnych ataków na system operacyjny. Chociaż hakerzy nadal atakują systemy operacyjne, włamywanie się poprzez przejmowanie aplikacji jest obecnie dominującym wektorem hakerskim.

TEST

a. Co mogą zyskać hakerzy przejmując programy użytkowe?

b. Jaki jest najpopularniejszy sposób przejmowania hostów przez hakerów?

Ataki przepełnienia bufora

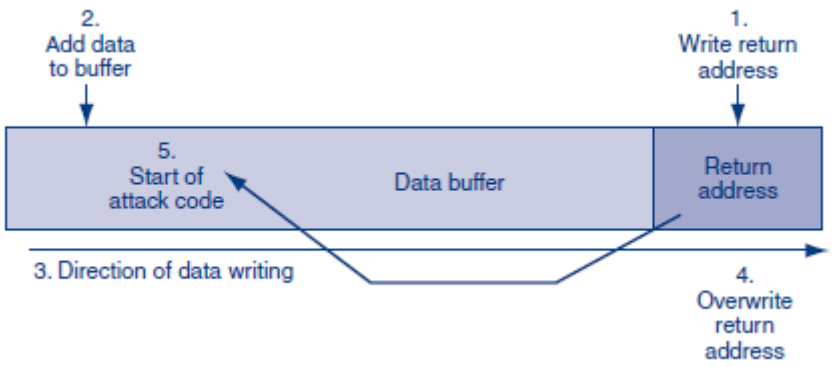
Jak omówiono wcześniej, gdy luki w aplikacjach zostaną znalezione, osoby atakujące tworzą oprogramowanie wykorzystujące exploity. Dostawcy oferują poprawki, takie jak ręczne obejścia, poprawki oprogramowania lub aktualizacje. Ważne jest posiadanie w miarę aktualnego oprogramowania aplikacyjnego i stosowanie wszystkich poprawek.

BUFORY I PRZEPEŁNIENIE

Wśród najbardziej rozpowszechnionych luk w aplikacjach są luki przepełnienia bufora. Programy często przechowują informacje tymczasowo w obszarach pamięci RAM zwanych buforami. Jeśli atakujący wyśle wiadomość z większą liczbą bajtów niż programista przeznaczył na bufor, informacje atakującego rozleją się na inne obszary pamięci RAM. To jest przepełnienie bufora. Wpływ przepełnienia bufora może wahać się od zera do awarii serwera lub uzyskania możliwości wykonania dowolnego polecenia na serwerze.

STOS

Przyjrzymy się bardziej szczegółowo popularnemu typowi przepełnienia bufora, przepełnieniu stosu. Często systemy operacyjne uruchamiają kilka programów. Ilekroć system operacyjny musi wstrzymać program, aby uruchomić inny, zapisuje informacje o zawieszonym programie we wpisie na stosie. Rysunek przedstawia pojedynczy wpis na stosie.



ADRES POWROTU

Adres powrotu wpisu stosu (1) wskazuje na lokalizację w pamięci RAM, która przechowuje adres następnego polecenia do wykonania w zawieszonym programie. (Programy są przechowywane w pamięci RAM podczas ich wykonywania.) Gdy wpis jest pobierany (wypychany) ze stosu, program, który umieścił tam wpis, przekaże kontrolę do polecenia w lokalizacji wskazanej w adresie powrotu. Adres powrotu jest zapisywany we wpisie stosu przed zapisaniem danych do bufora.

BUFOR I PRZEPEŁNIENIE BUFORA

Następnie system operacyjny dodaje dane do bufora danych stosu (2). Zapisuje te informacje od dołu bufora danych do góry (3). Jeśli system operacyjny zapisze zbyt dużo informacji do bufora, spowoduje to przepełnienie bufora, nadpisując adres powrotu (4).

WYKONYWANIE KODU ATAKU

Gdy wpis zostanie usunięty ze stosu, program, który go wywołał, przekaże kontrolę na adres powrotny tego wpisu. Jeśli atakujący umiejętnie nadpisał adres zwrotny, adres zwrotny będzie wskazywał z powrotem na „dane” w buforze (5). Jeśli te dane rzeczywiście są kodem programu, ten kod ataku zostanie wykonany zamiast kodu legalnego programu.

PRZYKŁAD: ATAK PRZEPEŁNIANIA BUFORA IIS IPP

Oprogramowanie serwera WWW firmy Microsoft to Internet Information Server (IIS). IIS oferuje szereg usług, w tym usługę IPP (Internet Printing Protocol). Chociaż niewielu użytkowników kiedykolwiek korzysta z tej usługi, była ona domyślnie włączona we wczesnych wersjach IIS. Zgłaszający luki odkryli, że IPP był podatny na atak przepełnienia bufora. Niedługo potem osoba atakująca stworzyła program jill.c, aby wykorzystać tę lukę. Ten exploit został napisany w języku programowania C. W swoim sercu jill.c wysyła następujący komunikat żądania HTTP do usług IIS. Żądania HTTP zaczynają się od linii wskazującej, co należy zrobić - w tym przypadku wykonanie żądania drukowania. Kolejny wiersz wskazuje hosta, do którego ma trafić żądanie. Nazwa hosta jest zastępowana 420-znakowym ciągiem, który powoduje przepełnienie buforu.

POBIERZ /NULL.printer HTTP/1.0

Host: 420-znakowe wejście do uruchomienia powłoki poleceń

Następna linia, pokazana poniżej, to odpowiedź z serwera WWW. Kod ataku został wykonany, gdy nadeszło żądanie i spowodował, że system Windows utworzył nową powłokę poleceń — co kiedyś nazywano monitem systemu DOS. Atakujący znajduje się teraz w wrażliwym katalogu. Ponadto atakujący ma uprawnienia systemowe, co oznacza, że może robić wszystko, co chce, w tym katalogu i większości innych katalogów.

C:\WINNT\system32\>

TEST

a. Co to jest bufor?

b. Co to jest atak przepełnienia bufora?

c. Jakie skutki mogą mieć przepełnienia bufora?

d. W przypadku przepełnienia stosu, co jest zastępowane przez przepełnienie?

e. Dokąd wskazuje nadpisany adres zwrotny?

f. Jaki bufor jest przepełniony w ataku na przepełnienie bufora IIS IPP?

Kilka systemów operacyjnych, wiele aplikacji

Mechanika luk w zabezpieczeniach, exploitów, łat i obejść nie różni się zasadniczo w przypadku systemów operacyjnych i aplikacji. Główną różnicą jest niewielka liczba systemów operacyjnych obsługiwanych przez większość firm w porównaniu z dużą liczbą aplikacji, z których zwykle korzystają. W przypadku systemów operacyjnych większość firm ma do czynienia tylko z raportami o podatnościach, łatami i obejściami od kilku dostawców. Jednak firmy mogą uruchamiać programy użytkowe od kilkudziesięciu dostawców oprogramowania aplikacyjnego. W większości firm lwia część wszystkich luk i poprawek dotyczy aplikacji. Samo znalezienie informacji o lukach w zabezpieczeniach i poprawkach może być irytującym obowiązkiem, ponieważ każdy dostawca publikuje informacje o lukach i poprawkach swoich produktów na swój własny sposób. Chociaż pomagają różne usługi śledzenia podatności (zwłaszcza BugTraq na SecurityFocus.com), administratorzy serwerów muszą często odwiedzać witryny swoich dostawców aplikacji. Gdy firma znajdzie poprawki, musi je pobrać i zainstalować. Dodając do tego zamieszania, każdy sprzedawca ma inne mechanizmy pobierania i instalowania poprawek.

SPRAWDŹ SWOJE ZROZUMIENIE

a. Dlaczego łatanie aplikacji jest bardziej czasochłonne niż łatanie systemów operacyjnych?

Aplikacje do hartowania

Jak firmy mogą wzmocnić aplikacje, aby były trudne do zaatakowania? Odpowiedź brzmi, że firmy muszą podjąć kilka działań, aby chronić swoje aplikacje.

ZROZUM ROLĘ SERWERA I ZAGROŻENIA W ŚRODOWISKU

Pierwszym zadaniem w bezpieczeństwie jest zrozumienie środowiska, które ma być chronione. Jeśli na przykład usługa taka jak poczta elektroniczna działa na jednym komputerze, to administrator systemu może rygorystycznie wyciąć wszystko, co nie zajmuje się bezpośrednio pocztą elektroniczną i być może administracją zdalną. Jeśli jednak serwer musi obsługiwać wiele aplikacji, wycięcie usług będzie mniej opłacalną opcją.

Ważne jest również środowisko zagrożenia. Jeśli środowisko zagrożenia jest bardzo niebezpieczne, konieczne może być odcięcie nawet zdalnej administracji.

PODSTAWY

Jak omówiono w rozdziale 5, serwery i klienci muszą być chronione za pomocą zabezpieczeń fizycznych. Jak widzieliśmy w rozdziale 7, ich systemy operacyjne muszą zostać wzmocnione za pomocą poprawek i ustawień konfiguracyjnych o wysokim poziomie bezpieczeństwa.

ZMINIMALIZUJ APLIKACJE

Zminimalizuj główne aplikacje.

Jak wspomniano w rozdziale 7, firmy powinny minimalizować aplikacje uruchamiane przez hosta. Mniej aplikacji oznacza mniej możliwości przejęcia komputera. Wiele zainstalowanych aplikacji jest skonfigurowanych do uruchamiania przy każdym uruchomieniu komputera. Aplikacje te zarówno zużywają zasoby systemowe, jak i stanowią potencjalny punkt ataku. Można uniemożliwić uruchamianie aplikacji za pośrednictwem usług systemu Windows. Usługi znajdują się w Panelu sterowania w obszarze System i zabezpieczenia: Narzędzia administracyjne. Apache2.2 jest ustawiony na automatyczne uruchamianie się przy starcie. Menu Akcja umożliwia dostęp do właściwości każdej usługi. Typ uruchamiania można zmienić z automatycznego na ręczny lub wyłączony. Jeśli usługa jest ustawiona na ręczną, uruchomi się tylko wtedy, gdy zostanie zainicjowana przez użytkownika. Usługę można również uruchomić lub zatrzymać ręcznie. Wyłączenie zbędnych usług może zwolnić zasoby systemowe i chronić hosta przed atakami z zewnątrz. Wyłączenie krytycznych usług bez zrozumienia ich funkcji może spowodować niezamierzone problemy systemowe.

Zminimalizuj aplikacje pomocnicze.

Hakerzy często atakują niejasne programy, które są uruchamiane automatycznie, gdy system operacyjny jest zainstalowany z domyślnymi ustawieniami lub gdy złożona aplikacja jest zależna od aplikacji pomocniczych, tak jak robią to wszystkie programy serwera WWW. Na przykład, gdy użytkownicy wielu starszych wersji systemu Windows 2000 uruchamiali serwer sieciowy IIS, system operacyjny również automatycznie uruchamiał usługę Gopher w ramach instalacji domyślnej. Nigdy nie słyszałeś o Gopherze? Dołączyć do klubu. Gopher był usługą, która wykazywała wielkie nadzieje w zakresie wyszukiwania informacji tuż przed uderzeniem fali pływowej w sieci World Wide Web. Dziś nikt tego nie używa. Jednak gdy atakujący wykryli problem z mało znanym programem Gopher, prawie każda implementacja IIS była natychmiast podatna na atak, dopóki firma nie zainstalowała poprawki.

PODSTAWY BEZPIECZEŃSTWA DLA MINIMALIZACJI APLIKACJI

Ponownie, podstawa bezpieczeństwa powinna nas kierować. Instalator musi wiedzieć, które opcjonalne programy pomocnicze zainstalować dla danej aplikacji, a które są instalowane automatycznie i które należy usunąć po instalacji.

UTWÓRZ BEZPIECZNĄ KONFIGURACJĘ

Plany bazowe opisują ogólnie, jak utworzyć bezpieczną konfigurację. Co najważniejsze, aplikacja nigdy nie powinna brakować hasła ani mieć dobrze znanego hasła domyślnego.

ZAINSTALUJ POPRAWKI I AKTUALIZACJE DO APLIKACJI

Co najważniejsze, instalator powinien upewnić się, że zainstalował wszystkie poprawki aplikacji. Jak wspomniano wcześniej, zwykle wiąże się to ze śledzeniem luk w zabezpieczeniach i raportami o poprawkach od wielu różnych dostawców aplikacji. Ponadto firma powinna zainstalować najnowszą wersję oprogramowania, w razie potrzeby aktualizując oprogramowanie. Nowsze wersje aplikacji, po przekroczeniu początkowego „okresu ząbkowania”, zwykle są znacznie bezpieczniejsze niż starsze wersje.

ZMINIMALIZUJ ZEZWOLENIA APLIKACJI

Jak wspomniano wcześniej, jeśli atakujący mogą przejąć aplikację, mogą wykonywać polecenia z uprawnieniami programu. Niektóre programy muszą działać z uprawnieniami administratora. Jednak wiele programów może działać z niższymi poziomami uprawnień i należy je uruchamiać z minimalnymi możliwymi uprawnieniami do wykonywania swojej pracy.

DODAJ UWIERZYTELNIANIE NA POZIOMIE WNIOSKU, ZEZWOLENIA I AUDYT

Jednym ze sposobów powstrzymania atakujących jest zignorowanie danych wejściowych od każdego, kto nie został prawidłowo uwierzytelniony. Aby włamać się do systemu, atakujący musiałby mieć zarówno exploit, jak i uwierzytelniony dostęp do systemu. System haseł do kont systemu operacyjnego zapewnia pewną ochronę, ale wiele aplikacji zapewnia również własne uwierzytelnianie. Zamiast szerokiego dostępu do komputera, uwierzytelnianie aplikacji może być specyficzne dla potrzeb aplikacji, na przykład akceptować tylko osoby z listy kontroli dostępu i nadawać różnym osobom uprawnienia, które są istotne dla aplikacji. Program użytkowy może wymagać własnego hasła — jednego o dużej złożoności. Lub program aplikacji może wymagać karty inteligentnej lub innej formy silnego uwierzytelniania, takiej jak uwierzytelnianie kluczem publicznym. Uwierzytelnianie dwuskładnikowe jest jeszcze lepsze. Chociaż dodanie uwierzytelniania na poziomie aplikacji jest trudne, a czasem niemożliwe, firmy powinny to robić wszędzie tam, gdzie to możliwe. Dotyczy to zwłaszcza bardzo wrażliwych aplikacji, takich jak bazy danych zasobów ludzkich i bazy danych informacji o klientach.

WDRAŻANIE SYSTEMÓW KRYPTOGRAFICZNYCH

W rozdziale 3 widzieliśmy silne zabezpieczenia oferowane przez systemy kryptograficzne, takie jak SSL/TLS i IPsec. Pomiędzy użytkownikiem a aplikacją należy zawsze stosować zabezpieczenia systemu kryptograficznego.

TEST

a Dlaczego musisz znać rolę serwera, aby wiedzieć, jak go chronić?

b. Dlaczego ważne jest, aby zminimalizować zarówno aplikacje główne, jak i aplikacje pomocnicze?

c. Dlaczego do instalowania aplikacji potrzebne są podstawy bezpieczeństwa?

d. Dlaczego ważne jest minimalizowanie uprawnień dla aplikacji?

e. Dlaczego uwierzytelnianie na poziomie aplikacji jest lepsze od uwierzytelniania systemu operacyjnego?

f. Dlaczego należy stosować zabezpieczenia kryptograficzne?

Zabezpieczanie niestandardowych aplikacji

Komercyjne, gotowe oprogramowanie prawdopodobnie zostało napisane z pewną starannością, w tym sprawdzanie pod kątem luk w zabezpieczeniach. Jednak niestandardowe aplikacje budowane w firmie na własny użytek i na użytek jej klientów rzadko są konstruowane tak starannie. Problem polega na tym, że zwykli programiści prawdopodobnie nie byli dobrze przeszkoleni w zakresie bezpiecznego kodowania w ogóle lub dobrych praktyk bezpieczeństwa niezbędnych dla danych języków programowania.

NIGDY NIE UFAJ WPROWADZENIA UŻYTKOWNIKA

W przypadku wszystkich aplikacji podstawowa zasada brzmi: „Nigdy nie ufaj wprowadzaniu przez użytkownika”. Jeśli użytkownik ma wprowadzić tekst, sprawdź, czy dane wejściowe rzeczywiście są tekstem i upewnij się, że nie jest zbyt długi, nie zawiera niewłaściwego adresu URL, nie zawiera skryptu, nie zawiera instrukcji SQL ani części instrukcji SQL , i tak dalej. W dalszej części tego rozdziału przyjrzymy się, w jaki sposób atakujący mogą użyć niewłaściwych danych wejściowych do uszkodzenia lub zhakowania komputera.

Nigdy nie ufaj danym wprowadzanym przez użytkownika.

ATAKI PRZEPEŁNIANIA BUFORA

Z powyższej dyskusji wynika, że oczywistym problemem związanym z danymi wejściowymi użytkownika są ataki przepełnienia bufora przeciwko programowi. W niektórych językach, takich jak C, jedynym zabezpieczeniem jest używanie funkcji wejściowych, które sprawdzają długość na wejściu.

EKRAN LOGOWANIA ATAKU BYPASS

W przypadku programów dostępu do stron internetowych istnieje wiele potencjalnych problemów. Na przykład w przypadku ominięcia ekranu logowania atakujący wpisuje adres URL do strony poza ekranem logowania, gdy pojawia się ekran logowania. Jeśli aplikacja nie zostanie poprawnie zaprogramowana, obejście zadziała, dając nieuwierzytelnionemu użytkownikowi dostęp do informacji, do których dostęp powinni mieć tylko uwierzytelnieni użytkownicy.

CROSS-SITE SCRIPTING ATAKI

Innym niebezpieczeństwem programowania stron internetowych jest przypadkowe dopuszczenie cross-site scripting (XSS), w którym dane wejściowe jednego użytkownika mogą pojawić się na stronie innego użytkownika. Stanowi to niebezpieczeństwo na każdej stronie internetowej, która odzwierciedla wkład użytkownika. Na przykład odbicie istnieje, jeśli wpiszesz nazwę użytkownika, a następna strona internetowa zawiera „Witaj, nazwa użytkownika”. Rozważmy następujący przykład. Atakujący wysyła zamierzonej ofierze wiadomość e-mail. Wiadomość zawiera łącze do legalnej witryny, która zawiera odbicie. Link jest długi i rozciąga się poza okno adresu URL. W części, której użytkownik nie widzi, ponieważ znajduje się poza oknem adresu URL, adres URL zawiera skrypt. Gdy użytkownik kliknie adres URL, żądanie GET zawierające skrypt trafia do legalnej witryny. Prawidłowa strona internetowa odzwierciedla legalne informacje oraz skrypt. Skrypt zostanie wykonany bez interwencji użytkownika. Jeśli przeglądarka zamierzonej ofiary ma lukę, którą skrypt ma wykorzystać, zamierzona ofiara staje się faktyczną ofiarą. To tylko jeden przykład ataku XSS. Za każdym razem, gdy strona internetowa odzwierciedla dane wprowadzone przez użytkownika, prawdopodobnie możliwy jest atak XSS. W związku z tym dane wejściowe HTML muszą być filtrowane, aby upewnić się, że nie zawierają skryptów.

ATAKI WTRYSKU SQL

Podczas wdrażania dostępu do bazy danych użytkownik może zostać poproszony o podanie pewnych informacji, takich jak nazwa użytkownika, hasło lub kod konta. W wielu przypadkach dane wejściowe zostaną przetestowane za pomocą zapytania SQL. Na przykład, jeśli wpiszesz swoje nazwisko, wpisany ciąg, $name, może zostać wprowadzony do zapytania SQL, aby znaleźć Twój numer telefonu. Jeśli sprawdzanie danych wejściowych nie zostało wykonane lub zostało wykonane źle, osoba atakująca może użyć wstrzykiwania SQL, aby wprowadzić ciąg zawierający zarówno nazwę użytkownika, jak i inne zapytanie SQL. Gdy program wprowadzi ciąg wejściowy do zapytania SQL, może nieświadomie wykonać zarówno zapytanie o numer telefonu, jak i zapytanie wprowadzone przez użytkownika. To drugie zapytanie może wyszukać informacje, które nie powinny być dostępne dla atakującego. Istnieje

wiele rodzajów ataków typu SQL injection. W niektórych przypadkach „wejście” może nawet zawierać pełną instrukcję SQL, która zostanie wykonana w celu wykonania tego, czego chce napastnik.

MANIPULACJA AJAX

Ajax, który jest skrótem od Asynchronous JavaScript XML, wykorzystuje wiele technologii do tworzenia dynamicznych aplikacji po stronie klienta. Korzystanie z Ajax jest korzystne, ponieważ umożliwia lokalnym stronom internetowym dynamiczne zmiany bez konieczności interakcji z serwerem za każdym razem, gdy wprowadzana jest zmiana. Jednak dynamiczna natura Ajax sprawia, że jest on podatny na wstrzykiwanie złośliwego kodu, zmieniony XML, manipulację walidacją po stronie klienta i tak dalej.

SZKOLENIE Z BEZPIECZEŃSTWA KOMPUTERÓW

Weryfikacja danych wejściowych użytkownika może udaremnić tylko niektóre ataki. Programiści, którzy tworzą niestandardowe programy, muszą zostać przeszkoleni w zakresie bezpiecznego programowania w ogóle oraz dla konkretnego języka programowania i aplikacji. Wyjaśnienie, jak działa każda z tych licznych wad i jak się przed nimi chronić, zajęłoby kilka podręczników. Niektóre z najczęstszych błędów w aplikacjach internetowych obejmują niewłaściwe zarządzanie sesjami, przekazywanie nieprawidłowych parametrów i błędy współbieżności. Istnieją platformy szkoleniowe, które pozwalają programistom i administratorom systemów dowiedzieć się więcej o tym, jak można wykorzystać te wady. OWASP-WebGoat (OWASP.org) i seria Hacme firmy Foundstone (Foundstone.com) zostały zaprojektowane w celu zapewnienia bezpiecznego środowiska szkoleniowego ze znanymi słabościami aplikacji.

TEST

a. Co to jest atak polegający na omijaniu ekranu logowania?

b. Co to jest atak XSS (cross-site scripting)?

c. Co to jest atak typu SQL injection?

d. Jaką postawę powinni mieć programiści w kwestii wkładu użytkownika?

e. Jakie szkolenie powinni odbyć programiści, którzy zajmują się programowaniem na zamówienie?

BEZPIECZEŃSTWO WWW I E-COMMERCE

Znaczenie bezpieczeństwa WWW i e-commerce Firmy słusznie troszczą się o swoje serwery internetowe i bezpieczeństwo e-commerce. Ataki mogą zakłócić działanie usług, zaszkodzić reputacji firmy i ujawnić prywatne informacje, co ma poważne konsekwencje dla firmy. Może również umożliwić skuteczniejsze oszustwo klientów przeciwko firmie.

TEST

a. Jakie zagrożenia stwarzają usługi webservice i e-commerce dla korporacji?

Usługa WWW a usługa e-commerce

Pewne zamieszanie pojawia się w odniesieniu do terminów usługa WWW i usługa e-commerce. USŁUGA WWW Terminem usługa WWW będziemy używać określenia podstawowej funkcjonalności serwerów HTTP, w tym pobierania plików statycznych (strony stałe) oraz tworzenia stron dynamicznych (stron utworzonych w odpowiedzi na określone zapytanie) za pomocą oprogramowania na serwerze. W systemie Microsoft Windows natywnym programem serwera WWW jest Internet

Information Server (IIS). To oprogramowanie dominuje w korzystaniu z serwera WWW na hostach Windows Server - po części dlatego, że jest częścią podstawowego oprogramowania Windows Server, a zatem jest bezpłatne. Na hostach LINUX i UNIX dominującym oprogramowaniem jest darmowy program serwera WWW Apache. W styczniu 2011 r. Apache posiadał 59 procent udziału w rynku serwerów internetowych w porównaniu z 21 procentami posiadanymi przez IIS.1 Więksi dostawcy, tacy jak Google czy SUN, oferują własne oprogramowanie serwera internetowego. Programy serwera WWW, jak pokazuje Rysunek 8-9, często zawierają komponenty pochodzące od różnych firm. Na przykład oprogramowanie do tworzenia aplikacji PHP jest wbudowane w wiele serwerów internetowych. W 2002 roku poważna luka w PHP zagroziła oprogramowaniu niemal wszystkich dostawców serwerów internetowych.

USŁUGA E-COMMERCE

Będziemy używać terminu usługa e-commerce w odniesieniu do dodatkowego oprogramowania potrzebnego do kupowania i sprzedawania, w tym katalogów online, koszyków na zakupy, funkcji kasowych, połączeń z wewnętrznymi bazami danych w firmie oraz linków do organizacji zewnętrznych, takich jak banki . Będziemy używać terminu e-commerce w odniesieniu do dodatkowego oprogramowania potrzebnego do kupowania i sprzedawania.

DOSTĘP ZEWNĘTRZNY

Serwer handlu elektronicznego musi mieć dostęp sieciowy do wielu zewnętrznych systemów, w tym serwerów w firmach (do wprowadzania zamówień, księgowania, wysyłki itp.) oraz serwerów poza firmą w bankach handlowych i firmach, które sprawdzają numery kart kredytowych dla ważności. Webmaster lub administrator e-commerce często nie ma kontroli nad bezpieczeństwem innych systemów.

PROGRAMY NIESTANDARDOWE

Wiele firm korzystających z oprogramowania do handlu elektronicznego tworzy własne programy, które uzupełniają możliwości kupowanego oprogramowania w pakietach. Jak zauważono wcześniej w tym rozdziale, większość firm nie radzi sobie z nadzorowaniem rozwoju tych programów niestandardowych. W związku z tym osoby atakujące często mogą wykorzystywać luki w niestandardowych programach lub, co jeszcze bardziej podstępnie, tworzyć własne niestandardowe programy, które mogą uruchamiać na serwerze ofiary, aby wspomóc swoje ataki. Wiele firm uważa, że napastnicy nie będą znali ich niestandardowego oprogramowania i będą mieli trudności z włamaniem się do tych programów. Jednak większość języków programowania tworzy programy, które mają typowe tryby awarii zabezpieczeń, które są dobrze znane hakerom. Przykład tego widzieliśmy wcześniej w tym rozdziale, kiedy przyjrzeliśmy się skryptowi cross-site. Atakujący musiał tylko wiedzieć, że witryna odzwierciedla dane wprowadzone przez użytkownika. Aby się tego dowiedzieć, atakujący musiał tylko wysłać dane wejściowe i sprawdzić, czy zostało to odzwierciedlone.

TEST

a. Rozróżnij serwis WWW i serwis e-commerce.

b. Jakie rodzaje dostępu zewnętrznego są potrzebne do e-commerce?

c. Czy webmaster lub administrator e-commerce ma kontrolę nad bezpieczeństwem innych serwerów?

d. Dlaczego programy niestandardowe są szczególnie podatne na ataki?

Niektóre ataki na serwer WWW

Jak atakujący atakują serwery internetowe? W tej sekcji przyjrzymy się kilku atakom na serwery internetowe.

ZNIEKSZTAŁCENIE STRONY INTERNETOWEJ

Częstym atakiem jest przejmowanie witryny pod kątem oszpecania komputera i umieszczanie strony stworzonej przez hakerów zamiast zwykłej strony głównej. Chociaż generalnie jest to tylko uciążliwość, może być znacznie gorzej. Na przykład po śmiertelnej katastrofie lotniczej hakerzy splamili witrynę ValueJet stwierdzeniem: „Więc zabiliśmy kilka osób". Co gorsza, hakerzy czasami instalują strony główne „Poza biznesem", aby skłonić klientów do odejścia i trzymania się z daleka.

ATAK PRZEPEŁNIENIE BUFORA W CELU URUCHOMIENIA POWŁOKI POLECENIA

Wcześniej omówiliśmy lukę przepełnienia bufora IIS IPP oraz program jill.c wykorzystywany do wykorzystania tej luki. Zauważyliśmy, że atakujący otrzymuje powłokę poleceń i silne uprawnienia (systemowe). Usługi IIS były przedmiotem wielu innych ataków przepełnienia bufora z równie niszczycielskimi skutkami. Podobnie jak inne programy serwerowe.

ATAK PRZEJAZDU KATALOGU

Czasami atakujący wie, że pewien poufny plik, taki jak plik haseł, jest zwykle przechowywany w określonym katalogu pod określoną nazwą. Atakujący chciałby pobrać wiele z tych wrażliwych plików. Kiedy użytkownicy wysyłają żądanie pobrania pliku, „główny" jest w rzeczywistości konkretnym katalogiem należącym do serwera WWW. Nazwiemy ten katalog katalogiem głównym WWW. Rysunek 8-11 ilustruje katalog główny WWW. Tutaj katalog główny WWW znajduje się jeden poziom niżej od prawdziwego katalogu głównego komputera. Jeśli użytkownik wpisze ścieżkę /Projects/Bak.doc, żądanie nie trafia do katalogu głównego serwera, a następnie przechodzi o jeden poziom w dół do katalogu Projects. Zamiast tego zaczyna się w katalogu głównym WWW i przechodzi o jeden poziom w dół do podkatalogu Projects. Następnie pobiera plik Bak.doc przechowywany w tym katalogu. Jednak osoby atakujące dowiedziały się, że gdyby w ścieżce zaczynały się od „../", niektóre programy serwera WWW pozwoliłyby im wyrwać się z głównego katalogu WWW i dostać się do katalogu znajdującego się powyżej katalogu głównego WWW. W systemach operacyjnych „.." oznacza przejście o jeden poziom wyżej. Aby zejść o jeden poziom niżej, polecenie podaje nazwę katalogu. Na przykład, aby przejść o jeden poziom w górę i w dół do katalogu etc, ścieżka będzie miała postać „../etc". Wpisanie adresów URL z „.." w nich może dać dostęp do poufnych katalogów, w tym do katalogu wiersza poleceń. To jest podstawowy atak z przechodzeniem katalogów. Przy przechodzeniu katalogów ścieżka ../etc/passwd umożliwiłaby atakującemu pobranie pliku passwd z katalogu etc (na komputerze z systemem Unix).

PRZEJAZD PRZEZ KATALOGÓW Z UCIECZKAMI ZNAKÓW SZESNASTKOWYCH

Jak to zwykle bywa, dostawcy odpowiedzieli łatką, która odrzucała wiadomości żądań HTTP zawierające serię dwóch kropek. Atakujący wkrótce znaleźli wariant podstawowego ataku, który odniósłby sukces w walce z tym środkiem zaradczym. Na przykład IIS zezwala na wprowadzanie szesnastkowe, w którym po % następuje dwa symbole od 0 do F. Każdy symbol reprezentuje cztery bity, więc oba symbole razem reprezentują bajt. Następnie osoby atakujące wysyłały wiadomości o przejściu do katalogu HTTP z dwoma kodami szesnastkowymi dla kropki. Przez jakiś czas ten atak z przechodzeniem przez katalog szesnastkowy był udany. Następnie sprzedawcy wydali łatkę, aby to powstrzymać.

PRZEJAZD DO KATALOGU UNICODE

Ta gra w kotka i myszkę trwała dalej. Na przykład system kodowania UNICODE może reprezentować języki inne niż angielski. Każdemu znakowi w każdym języku przypisana jest sekwencja kodu. Niektóre z tych ciągów kodu w różnych językach reprezentują kropki. Wkrótce atakujący wykorzystali kilka reprezentacji UNICODE, aby obejść łaty szesnastkowe. Z kolei dostawcy stworzyli łatkę dla ataków typu directory traversal UNICODE.

TEST

a. Co to jest zniszczenie strony internetowej?

b. Dlaczego to szkodzi?

c. Co oznacza „..” w poleceniach dostępu do katalogu i adresach URL?

d. Co to są ataki z przechodzeniem katalogów?

e. Utwórz adres URL, aby pobrać plik aurigemma.htm w katalogu rainbow na hoście www.pukanui.com. Katalog główny WWW znajduje się trzy poziomy poniżej prawdziwego katalogu głównego systemu i katalogu tęczy, który znajduje się w katalogu projektów, który znajduje się bezpośrednio pod katalogiem głównym. (Wskazówka: narysuj obrazek.)

f. Na jakie dwa sposoby osoby atakujące ominęły filtrowanie mające na celu powstrzymanie ataków przechodzenia przez katalogi?

Łatanie oprogramowania serwera WWW i handlu elektronicznego oraz jego komponentów

LUKI W OPROGRAMOWANIU E-COMMERCE

Firma hostingowa MindSpring wpadła w zakłopotanie, gdy okazało się, że jej serwery ujawniają hasła do niektórych hostowanych stron internetowych. Problem został wyśledzony do pojedynczej witryny, która korzystała z komercyjnego programu e-commerce i nie zarejestrowała go. Właściciele serwisu nie zostali powiadomieni o ważnej łatce z powodu braku rejestracji produktu. Dwa lata później hakerzy odkryli luki w zabezpieczeniach oprogramowania. Witryna była jedną z kilku witryn działających na jednym serwerze Sun Solaris (UNIX) w firmie hostingowej. Ten serwer został nieprawidłowo skonfigurowany, a luka w pojedynczej witrynie spowodowała otwarcie dostępu do plików haseł na innych witrynach hostowanych na tym samym komputerze. Ten przykład podkreśla znaczenie łatania komercyjnego oprogramowania serwera handlu elektronicznego (oraz prawidłowej konfiguracji współdzielonych maszyn). Oprogramowanie e-commerce jest złożone i ma wiele podsystemów. Głupotą byłoby zakładać, że luki w zabezpieczeniach nigdy nie zostaną znalezione w komercyjnym oprogramowaniu e-commerce firmy. Wiele z tego oprogramowania działa jako root, dając atakującym otwarty dostęp do całego serwera, jeśli złamią komponenty oprogramowania WWW lub oprogramowania e-commerce. Nawet jeśli serwer WWW lub serwer handlu elektronicznego generuje czysty kod, niektóre podsystemy często są narażone na atak ze strony swoich dostawców. Na przykład wiele programów serwerowych obsługuje programowanie PHP. Seria luk w PHP wykrytych w styczniu 2002 roku umożliwiła atakującym przejęcie strony internetowej, czasami z łatwością. Więcej luk w PHP zostało znalezionych później w tym samym roku, ponieważ łowcy błędów coraz częściej zwracali uwagę na PHP po początkowych ujawnieniach. W innym przypadku luka w komponencie OpenSSL spowodowała, że większość serwerów Apache stała się podatna na ataki później w 2002 roku.

Inne zabezpieczenia stron internetowych

NARZĘDZIA DO OCENY PODATNOŚCI STRONY INTERNETOWEJ

Opracowano kilka narzędzi do oceny podatności serwerów WWW. Niektóre z szerzej stosowanych narzędzi do oceny podatności witryn internetowych to Nikto, Paros Proxy, Acunetix i IBM Rational AppScan. Częste uruchamianie narzędzia oceny podatności na stronie internetowej należy traktować jako normalną konserwację.

DZIENNIKI BŁĘDÓW STRONY INTERNETOWEJ

Ponadto strony internetowe zwykle rejestrują odpowiedzi zawierające komunikaty o błędach. Przeglądy dzienników należy wykonywać często, aby szukać oznak ataków. Na przykład nadmierna liczba 500 komunikatów o błędach może wskazywać, że osoba atakująca próbuje wysłać na serwer nieprawidłowe dane. Z kolei nadmierna liczba błędów 404 może wskazywać, że atakujący szuka na ślepo plików w Twojej witrynie. Dziennik błędów na rysunku 8-13 pokazuje wewnętrznego pracownika (10.10.10.10) szukającego na ślepo katalogów (pogrubioną czcionką) na wewnętrznym serwerze WWW (10.0.0.1). Wszystkie odpowiedzi są błędami 404 wskazującymi, że nie znaleziono katalogu lub pliku. W tym przypadku pracownik prawdopodobnie szuka planów dotyczących nowego produktu, który ma zostać wydany. Sprawdzanie dzienników błędów pozwala administratorom systemów zobaczyć, kto atakuje ich serwery i jakiego typu ataku mogą używać.

ZAPORY ZAPOROWE SPECYFICZNE DLA APLIKACJI SERWERA WEBSERVER

Jedną z metod ochrony jest użycie zapory proxy aplikacji dla serwera WWW. Ta zapora znajduje się między serwerem WWW a resztą sieci. Sprawdza przychodzące wiadomości z żądaniami pod kątem oznak ataków przepełnienia bufora i innych problemów. Zatrzymuje również wychodzące wiadomości odpowiedzi, które są nieodpowiednie.

TEST

a. Jakie oprogramowanie należy załatać na serwerze e-commerce?

b. Jakie trzy inne zabezpieczenia serwera WWW zostały wymienione w tekście?

c. Gdzie jest umieszczona zapora proxy aplikacji względem serwera WWW?

Kontrolowanie wdrażania

Bardzo ważne jest również kontrolowanie wdrażania nowych aplikacji po stronie serwera. Firmy stosujące rygorystyczne zasady wdrażania używają trzech typów serwerów: serwerów deweloperskich, serwerów testowych i serwerów produkcyjnych.

SERWERY ROZWOJOWE

Programy po stronie serwera powinny być tworzone na dedykowanych do tego celu serwerach deweloperskich. Deweloperzy potrzebują szerokich uprawnień na tych serwerach.

SERWERY TESTOWE

Po opracowaniu program jest przenoszony na serwer testowy w celu przetestowania. Deweloperzy nie powinni mieć uprawnień dostępu do tego serwera. Tylko testerzy powinni mieć uprawnienia dostępu do wprowadzania zmian, aby programiści nie wślizgiwali się w backdoory i nie wprowadzali zmian w ostatniej chwili. („To tylko kilka linijek kodu”).

SERWERY PRODUKCYJNE

Po pełnym przetestowaniu programu na serwerze pomostowym należy go przenieść na serwer produkcyjny, który będzie świadczyć usługi użytkownikom. Tylko administratorzy systemów potrzebni

do uruchomienia serwera produkcyjnego powinni mieć uprawnienia wykraczające poza odczyt i wykonanie. Testerzy nie powinni mieć możliwości wprowadzania zmian na serwerach produkcyjnych.

TEST

a. Z jakich trzech serwerów korzystają firmy w rozwoju etapowym?

b. Jakie uprawnienia ma programista na serwerze deweloperskim?

c. Na serwerze testowym?

d. Na serwerze produkcyjnym?

e. Na jakich serwerach tester ma uprawnienia dostępu?

ATAKI NAPRZEGLĄDARKI INTERNETOWE

Chociaż wiele ataków World Wide Web/e-commerce koncentruje się na serwerach, przeglądarki na klientach są również popularnymi celami. Ponieważ wiele firm zwiększa bezpieczeństwo swoich serwerów, przeglądarki mogą stać się jeszcze bardziej popularnym celem.

ZAGROŻENIA PRZEGLĄDARKI

Bezpieczeństwo przeglądarki w sieci World Wide Web i bezpieczeństwo handlu elektronicznego są ważne, ponieważ, jak wspomniano w Części 7, atakujący mogą chcieć przechowywać dane na kliencie i ponieważ atakujący mogą użyć zhakowanego klienta do zaatakowania innych systemów, do których klient ma dostęp referencje.

KOD MOBILNY

Kod mobilny składa się z poleceń zapisanych na stronie internetowej. Po pobraniu strony internetowej skrypt może wykonać się automatycznie. (Kod jest „mobilny", ponieważ przemieszcza się z serwera internetowego do komputerów użytkowników.) Chociaż kod mobilny może poprawić wrażenia użytkownika podczas surfowania w przeglądarce, może również powodować duże dziury w zabezpieczeniach klienta.

Aplety Java.

W kodzie mobilnym używanych jest wiele języków. Aplety Java (małe programy Java) są prawdopodobnie najbezpieczniejsze, ponieważ wiele działań związanych z atakiem jest wyłączonych; jednak ta ochrona jest daleka od doskonałości.

Active X.

Innym ważnym językiem dla aktywnej zawartości stron internetowych jest Active-X, technologia stworzona przez firmę Microsoft. Active-X jest potężny i może zrobić prawie wszystko na komputerze klienta. Ta moc, w połączeniu z faktem, że Active-X nie zapewnia prawie żadnej ochrony przed niewłaściwym użyciem, sprawia, że Active-X jest niezwykle niebezpieczny. Niestety wiele stron internetowych wymaga od użytkowników włączenia Active-X. Microsoft początkowo powiedział, że komponenty Active-X są bezpieczne, ponieważ muszą być podpisane kryptograficznie przez programistę, a jeśli możesz ufać programiście, powinieneś być w stanie zaufać jego programom. Jednak użytkownicy często nie znają programisty, a nawet dobrzy programiści mogą tworzyć produkty z lukami.

Języki skryptowe: VBScript i JavaScript.

Atakujący używają również języków skryptowych, które są łatwiejsze w użyciu niż pełne języki programowania, takie jak Java i Active-X. Bardziej popularne języki skryptowe dla kodu mobilnego to VBScript i JavaScript (pomimo swojej nazwy nie jest to skryptowa wersja Javy). Te języki skryptowe, choć łatwiejsze w użyciu niż Java, nie mają zabezpieczeń Java. Rysunek 8-16 to przykładowy kod JavaScript, który wyświetla „Hello World, from:", po którym następuje nazwa użytkownika.

SZKODLIWE LINKI

Przeglądarki często są podatne na złośliwe łącza na stronach internetowych iw treści wiadomości e-mail. Jeśli użytkownik kliknie złośliwy link i pobierze stronę internetową, zostanie uruchomiony skrypt ataku na pobranej stronie. Czasami skrypt aktywuje się, nawet jeśli użytkownik go nie kliknie, w zależności od tego, jak działa przeglądarka lub program pocztowy. W jaki sposób osoby atakujące skłaniają użytkowników do odwiedzania witryn internetowych, które dostarczają skrypty ataku? Czasami robią to poprzez socjotechnikę. Na przykład możesz otrzymać pilną wiadomość informującą, że Twój komputer jest zainfekowany wirusem i że powinieneś natychmiast przejść do określonego adresu URL, aby dowiedzieć się, jak usunąć wirusa z systemu.

Czasami inżynier socjalny każe przejść do popularnej witryny, takiej jak CNN.com. Jednak chociaż na ekranie pojawia się napis CNN.com, w rzeczywistości może to być link do strony atakującej. Ponadto wielu atakujących rejestruje nazwy domen, które są typowymi błędami pisowni w przypadku legalnych nazw domen witryn internetowych, na przykład micosoft.com. W niektórych przypadkach po prostu znajdują witrynę non-profit „.org" i rejestrują wersję „.com" jej nazwy. (Przez wiele lat whitehouse.com była witryną pornograficzną). Użytkownicy znajdujący się na tych stronach często czytają strony ze złośliwymi skryptami.

INNE ATAKI PO STRONIE KLIENTA

Możliwych jest wiele innych ataków po stronie klienta. Omówimy tylko kilka, aby dać Ci pojęcie o możliwościach.

Czytanie plików. W 2000 r. aplet Java dostarczany głównie za pośrednictwem poczty e-mail zasadniczo zmienił komputer kliencki użytkownika w niechętny serwer plików, dzięki czemu wszystkie jego pliki są łatwo dostępne dla atakującego.

Wykonywanie pojedynczego polecenia. Co gorsza, kilka typowych złośliwych ataków skryptowych umożliwia atakującym wykonanie dowolnego polecenia na komputerze ofiary. Czasami pojedyncze polecenie może być użyte do otwarcia powłoki poleceń; jeśli tak, atakujący będzie mógł wykonać wiele poleceń w powłoce poleceń.

Automatyczne przekierowywanie użytkowników na niechciane strony internetowe. Szereg skryptów na stałe zmienia ustawienia przeglądarki, a nawet rejestr komputera. Przy następnym użyciu komputera może się okazać, że domyślna strona główna została zmieniona na witrynę z pornografią lub inną witrynę zawierającą treści, których nie chcesz oglądać. Mówiąc bardziej subtelnie, gdy popełnisz błąd podczas wpisywania adresów URL, może się okazać, że zostaniesz przeniesiony do jednej z kilku nieautoryzowanych witryn, ponieważ skrypt ten trojanizował twoją procedurę obsługi błędów DNS.

Ciasteczka. Niektóre strony internetowe używają plików cookie. Plik cookie to mały ciąg tekstowy, który właściciel witryny może umieścić na komputerze klienta. Właściciel witryny może później odzyskać zapisane przez siebie pliki cookie (ale nie pliki cookie napisane przez inne witryny). Pliki cookie są cenne w transakcjach, które wymagają wymiany kilku wiadomości, ponieważ mogą śledzić, gdzie

znajduje się użytkownik. Pliki cookie mogą również zapamiętać nazwę użytkownika i hasło, aby ułatwić dostęp do stron internetowych wymagających autoryzacji.

Niestety pliki cookie mogą również śledzić, gdzie byłeś na stronie internetowej (i robić inne rzeczy, które są sprzeczne z pragnieniami użytkowników). Użytkownicy mogą wyłączyć pliki cookie, aby zapobiec śledzeniu, ale to uniemożliwia korzystanie z wielu stron internetowych. Pliki cookie mogą również zawierać wysoce prywatne informacje, o których nie chcesz, aby atakujący dowiedział się, jeśli włamie się do Twojego komputera. Programy antyszpiegowskie mogą identyfikować niebezpieczne pliki cookie.

TEST

a. Dlaczego hakerzy atakują przeglądarki?

b. Co to jest kod mobilny?

c. Dlaczego nazywa się to kodem mobilnym?

d. Co to jest skrypt po stronie klienta?

e. Co to jest aplet Java?

f. Dlaczego Active-X jest niebezpieczny?

g. Jak wypada porównanie języków skryptowych z pełnymi językami programowania?

h. Czy JavaScript jest oskryptowaną formą Javy?

a. Dlaczego odwiedzanie złośliwej witryny jest złe?

b. W jaki sposób można wykorzystać socjotechnikę, aby nakłonić ofiarę do przejścia na złośliwą witrynę?

c. Dlaczego atakujący chcą uzyskać nazwy domen, takie jak micosoft.com?

d. Dlaczego złośliwe oprogramowanie, które umożliwia atakującemu wykonanie pojedynczego polecenia na komputerze użytkownika, nie ogranicza się tak naprawdę do wykonania pojedynczego polecenia?

e. Co może się stać na zhakowanym komputerze, jeśli użytkownik błędnie wpisze nazwę hosta w adresie URL?

f. Jakie zagrożenia stwarzają pliki cookie?

Zwiększanie bezpieczeństwa przeglądarki

PATCHING I UAKTUALNIANIE

Wszystkie opisane właśnie ataki można powstrzymać, instalując poprawki w Internet Explorerze (IE) i innych przeglądarkach. Jednak stosunkowo niewielu użytkowników łata swoje przeglądarki, dając atakującym długie okna możliwości. W rzeczywistości wielu użytkowników ma wersje tak stare, że nie są tworzone dla nich łatki, gdy zostaną znalezione nowe luki.

KONFIGURACJA

Zatrzymanie ataków na przeglądarkę obejmuje również zmianę ustawień konfiguracyjnych przeglądarki w celu zmniejszenia prawdopodobieństwa uszkodzenia. Niestety, różne przeglądarki robią to inaczej, a nawet różne wersje IE robią to inaczej.

OPCJE INTERNETOWE

W IE użytkownicy zaczynają zmieniać swoje ustawienia, wybierając Opcje internetowe w menu Narzędzia. Spowoduje to otwarcie okna dialogowego

ZAKŁADKA BEZPIECZEŃSTWO

Okno dialogowe pokazuje kartę Zabezpieczenia. Z tej zakładki użytkownik może wybrać ustawienia zabezpieczeń dla ogólnych witryn internetowych, witryn intranetowych, witryn zaufanych i witryn z ograniczeniami. Wszystkie strony internetowe są początkowo w kategorii Internet. Użytkownik może je jednak umieścić w inne kategorie — intranet dla wewnętrznych witryn firmowych, zaufane witryny dla witryn cieszących się dużym zaufaniem oraz witryny z ograniczeniami dla podejrzanych witryn. Wartości domyślne w każdej kategorii są ogólnie dobrym wyborem ze względu na bezpieczeństwo, ale użytkownik może również wybrać przycisk Poziom niestandardowy, aby zmienić ustawienia dla czterech typów witryn internetowych w celu dokładniejszego kontrolowania zawartości. Na przykład w ogólnej strefie Internet podpisane formanty Active-X (formanty Active-X z podpisami cyfrowymi) są domyślnie wykonywane po wyświetleniu monitu identyfikującego twórcę formantu Active-X. Pracownicy mogą nie mieć wystarczającej wiedzy, aby zrozumieć niebezpieczeństwo używania nawet podpisanych formantów Active-X. Ponadto aktywne skrypty są domyślnie włączone, w tym skrypty Java. To przynajmniej nieco ryzykowne wybory.

ZAKŁADKA PRYWATNOŚĆ

Oprócz zakładki Bezpieczeństwo znajduje się zakładka Prywatność. Zakładka Prywatność, pokazana na Rysunku 8-19, pozwala użytkownikowi kontrolować, jakie informacje są udostępniane na stronach internetowych, w tym w jaki sposób wykorzystywane są pliki cookie. IE ma przesuwaną skalę, którą użytkownik może podnieść, aby uzyskać większą prywatność, a w dół, aby zmniejszyć prywatność. Wartość domyślna to średnia prywatność. Przycisk Zaawansowane umożliwia bardziej precyzyjną kontrolę nad plikami cookie. Karta Prywatność kontroluje również blokadę wyskakujących okienek witryny, która jest domyślnie włączona. Pod przyciskiem Ustawienia użytkownik może ustawić różne domyślne ustawienia wyskakujących okienek dla poszczególnych witryn.

TEST

a. Co użytkownicy mogą zrobić, aby zwiększyć bezpieczeństwo przeglądarki?

b. Co użytkownik może zrobić na karcie Zabezpieczenia w obszarze Opcje internetowe w IE?

c. Jakie są ustawienia komputera dla czterech stref?

d. W której zakładce kontrolowane są pliki cookie?

BEZPIECZEŃSTWO POCZTY

Przyglądaliśmy się bezpieczeństwu serwisów WWW/e-commerce oraz bezpieczeństwu przeglądarek. Inną dużą aplikacją w Internecie jest poczta elektroniczna (e-mail).

Filtrowanie treści wiadomości e-mail

Wiele firm filtruje obecnie przychodzące wiadomości e-mail (a czasem wiadomości wychodzące) pod kątem niebezpiecznych lub nieodpowiednich treści.

ZŁOŚLIWY KOD W ZAŁĄCZNIKACH I CIAŁACH HTML

Jak widzieliśmy w rozdziale 1, załączniki wiadomości e-mail mogą zawierać wirusy, robaki i inny złośliwy kod. Ponadto, teraz, gdy wiele systemów poczty e-mail może wyświetlać wiadomości z treścią HTML, skrypty w treści mogą wykonywać złośliwy kod, jak widzieliśmy wcześniej w tym rozdziale.

SPAM

Jednym z najbardziej irytujących aspektów poczty e-mail jest to, że większość użytkowników jest zasypywana spamem2 – niechcianymi, komercyjnymi wiadomościami e-mail. Obecnie spam stanowi 60-90% całego ruchu poczty internetowej każdego dnia. Spam zapycha skrzynki pocztowe, spowalnia komputery użytkowników, denerwuje użytkowników i wymaga poświęcenia czasu na usuwanie niechcianych wiadomości.

Ponadto wielu spamerów używa obecnie spamu graficznego, który przedstawia ich wiadomość jako obraz graficzny. To frustruje większość filtrowania treści. Powoduje to również, że każda wiadomość spamowa jest znacznie większa, zużywając jeszcze więcej przepustowości i przestrzeni dyskowej niż tradycyjny spam tekstowy.

Filtrowanie spamu. Biorąc pod uwagę dużą ilość spamu, większość firm filtruje przychodzącą pocztę e-mail w celu odrzucenia spamu. Jednak firmy, które filtrują przychodzący spam, czasami stwierdzają, że przefiltrowały przychodzącą pocztę e-mail. Coraz więcej wiarygodnych wiadomości jest odrzucanych jako spam, a kilka systemów filtrowania spamu ostrzega nadawcę lub odbiorcę, jeśli wiadomość zostanie odrzucona. Firmy, które filtrują spam, powinny umieszczać wiadomości w kwarantannie, aby później je przeanalizować i zająć się skargami odbiorców i nadawców dotyczących utraconych wiadomości.

NIEWŁAŚCIWA ZAWARTOŚĆ

W niektórych przypadkach pracownicy wysyłają współpracownikom e-maile zawierające treści seksualne lub rasowe. Jeśli firma nie podejmie żadnych działań, aby temu zapobiec, będzie odpowiedzialna za procesy sądowe. W związku z tym coraz więcej firm skanuje wszystkie wiadomości e-mail pod kątem treści o charakterze seksualnym, rasowym lub obraźliwym. Wielu już zwolniło pracowników za wysyłanie nieodpowiednich wiadomości e-mail.

ZAPOBIEGANIE WYCISKANIU

Można również przeprowadzić filtrowanie, aby uniemożliwić pracownikom wysyłanie własności intelektualnej poza korporację. Filtrowanie zapobiegające wyciskaniu zaczyna się od prostego przeszukiwania dokumentów w poszukiwaniu słów takich jak „poufne”. W praktyce wykracza to daleko poza to.

DANE OSOBOWE

Innym celem jest powstrzymanie wysyłania informacji umożliwiających identyfikację osoby (PII), takich jak prywatne informacje o pracownikach i prywatne informacje o klientach. W opiece zdrowotnej dane osobowe muszą być chronione prawem. Ogólnie przekazywanie numerów ubezpieczenia społecznego i inne wrażliwe dane osobowe mogą prowadzić do procesów sądowych, jeśli mogą potencjalnie prowadzić do kradzieży numeru karty kredytowej lub kradzieży tożsamości.

TEST

a. Dlaczego treści HTML w wiadomościach e-mail są niebezpieczne?

b. Co to jest spam?

c. Jakie trzy problemy stwarza spam?

d. Dlaczego filtrowanie spamu jest niebezpieczne?

e. Z jakich powodów prawnych firmy powinny filtrować treści wiadomości o charakterze seksualnym lub rasowym?

F. Co to jest zapobieganie wyciskaniu?

g. Dlaczego zapobieganie ekstruzji jest potrzebne w przypadku własności intelektualnej?

h. Co to są PII i dlaczego należy zapobiegać opuszczeniu firmy?

Gdzie zrobić filtrowanie złośliwego oprogramowania i spamu w wiadomościach e-mail

Jednym z problemów, z którymi borykają się firmy, jest to, gdzie robić złośliwe oprogramowanie i filtrowanie spamu w wiadomościach e-mail. Tradycyjnie filtrowanie to odbywało się na komputerach klienckich, jak pokazano na rysunku 8-21. Filtrowanie klientów ma kilka problemów. Użytkownicy często wyłączają filtry antywirusowe i antyspamowe. Często nie potrafią prawidłowo skonfigurować swoich systemów do automatycznego pobierania. Mogą nawet nie utrzymać subskrypcji na otrzymywanie aktualizacji. Jeśli zrobią którąkolwiek z tych rzeczy, nadal będą mieli oprogramowanie antywirusowe i antyspamowe w swoich systemach, ale nie będą mieli ochrony przed nowymi atakami.

W świetle problemów z filtrowaniem opartym na kliencie większość firm używa obecnie filtrowania na firmowym serwerze poczty e-mail jako podstawowej linii obrony dla poczty e-mail. To spycha filtrowanie klientów do drugorzędnego znaczenia jako środka obrony w głąb. Administratorzy poczty e-mail posiadają dyscyplinę i wiedzę niezbędną do zarządzania filtrowaniem poczty e-mail. W rzeczywistości administratorzy poczty e-mail zwykle spędzają większość czasu na filtrowaniu antywirusowym, filtrowaniu spamu i innych kwestiach związanych z bezpieczeństwem. Ze względu na obciążenie pracą związane z bezpieczeństwem poczty e-mail, niektóre firmy przenoszą całkowicie filtrowanie z firmy na dostawców usług zarządzanych pocztą e-mail. Dostawcy usług zarządzanych obniżają koszty pracy. Mają też doświadczenie w filtrowaniu poczty e-mail.

Wiele firm filtruje we wszystkich trzech lokalizacjach, aby zwiększyć poziom ochrony. Na firmowym serwerze poczty e-mail mogą oni używać innego programu filtrującego niż ich dostawcy usług zarządzanych. Różne programy antywirusowe i antyspamowe wyłapują nieco inne zagrożenia.

Szyfrowanie wiadomości e-mail

E-mail jest idealnym kandydatem do ochrony kryptograficznej. Jednak stosunkowo niewiele firm wymaga od swoich pracowników szyfrowania wiadomości e-mail w celu zapewnienia poufności, autentyczności, integralności wiadomości lub ochrony przed powtórkami. Jednym z powodów jest trudność korzystania z metod szyfrowania typu end-to-end. Opcje szyfrowania i podpisywania wiadomości e-mail w Microsoft Outlook, popularny klient poczty e-mail, znajduje się w Centrum zaufania. Większość klientów poczty e-mail ma podobne opcje zabezpieczeń.

SZYFROWANIE TRANSMISJI

Wiele firm szyfruje transmisję między klientem poczty e-mail a jego serwerem pocztowym za pomocą protokołu SSL/TLS. Jednak o ile serwery SMTP nie stosują również szyfrowania transmisji podczas wysyłania i odbierania wiadomości e-mail oraz o ile odbiorca nie komunikuje się również bezpiecznie ze swoim serwerem poczty, szyfrowanie typu end-to-end nie będzie możliwe.

SZYFROWANIE WIADOMOŚCI

Aby zapewnić pełne bezpieczeństwo, nadawca musi zaszyfrować wiadomość, w tym nagłówek, treść i załączniki. Dwa popularne standardy tego szyfrowania typu end-to-end to S/MIME i PGP (wraz z OpenPGP). Szyfrowanie S/MIME i PGP wykorzystują podpisy cyfrowe, które wymagają od odbiorcy znajomości klucza publicznego nadawcy. S/MIME (Secure/Multipurpose Internet Mail Extensions) wymaga tradycyjnej infrastruktury klucza publicznego z centralnym urzędem certyfikacji i certyfikatami cyfrowymi. Rysunek 8-24 przedstawia ustawienia zabezpieczeń poczty e-mail w programie Microsoft Outlook przy użyciu protokołu S/MIME. Zamiast PKI, PGP (Pretty Good Privacy) używa kręgów zaufania. Jeśli ufasz Patowi, a jeśli Pat ufa Leo, możesz zaufać Leo. Jest to niebezpieczne, ponieważ jeśli niewłaściwie umieszczone zaufanie jest obecne w dowolnym miejscu w systemie, fałszywe pary klucz publiczny/nazwa mogą krążyć w szerokim obiegu. PGP odniosła największy sukces w komunikacji międzyludzkiej bez kontroli korporacyjnej.

TEST

a. Czy szyfrowanie jest szeroko stosowane w e-mailach?

b. Jaką część procesu poczty e-mail zazwyczaj zabezpiecza SSL/TLS?

c. Czy to kompleksowe zabezpieczenie? Wyjaśniać.

d. Jakie standardy zapewniają kompleksowe bezpieczeństwo?

e. Porównaj PGP i S/MIME pod kątem tego, jak kandydaci poznają klucz publiczny prawdziwej strony.

f. Opisz zalety i wady każdego podejścia.

BEZPIECZEŃSTWO GŁOSOWE PRZEZ IP

Wysyłanie głosu między telefonami

Idea Voice over IP (VoIP) jest prosta. Zamiast dzwonić do kogoś innego przez publiczną komutowaną sieć telefoniczną, dzwonisz do niego przez Internet IP. Użytkownik VoIP posiada dedykowany telefon IP (1) lub telefon programowy - komputer z oprogramowaniem VoIP (2). Będziemy używać ogólnego terminu telefon VoIP. Kiedy osoba mówi, sprzęt lub oprogramowanie zwane kodekiem w telefonie VoIP przekształca głos tej osoby w strumień cyfrowych bajtów. Telefon VoIP umieszcza te bajty w pakietach i wysyła je do drugiego telefonu (3). Każdy pakiet przenoszący cyfrowe dane głosowe ma nagłówek IP, po którym następuje nagłówek protokołu UDP (User Datagram Protocol), nagłówek RTP (omówiony dalej) i grupa oktetów głosowych. Pakiety te trafiają bezpośrednio między dwoma telefonami. Transmisja głosu VoIP wykorzystuje UDP do przenoszenia cyfrowych danych głosowych. W przypadku transmisji głosu VoIP w przypadku utraty pakietu nie ma czasu na oczekiwanie na retransmisję w celu skorygowania utraty. W związku z tym nie ma powodu do TCP. Kodek odbierający po prostu wstawia wartość fałszywego dźwięku pakietu na podstawie poprzedniego dźwięku. RTP to protokół czasu rzeczywistego. To nadrabia dwie największe słabości UDP. Po pierwsze, nagłówek RTP ma numer sekwencyjny, dzięki czemu odbiorca może uporządkować oktety głosowe, jeśli ich pakiety dotrą nie w porządku. Po drugie, nagłówek RTP zawiera znacznik czasu, dzięki czemu kodek odbiornika odtwarza dźwięki w pakiecie we właściwym czasie w porównaniu z dźwiękami poprzedniego pakietu.

TEST

a. Co to jest VoIP?

b. Rozróżnij telefony IP i telefony programowe.

c. Wymień, w kolejności pojawiania się w odbiorniku, nagłówki i wiadomość pakietu przenoszącego głos między telefonami.

d. Co dodaje RTP, aby zrekompensować ograniczenia UDP?

Transport i sygnalizacja

W telefonii ważne jest zrozumienie podstawowego rozróżnienia między transportem a sygnalizacją. Transport to przenoszenie głosu między obiema stronami. Po prostu, kiedy rozmawiasz z kimś tam i z powrotem, to jest transport.

Transport to przenoszenie głosu między obiema stronami.

Sieć telefoniczna musi również zapewniać sygnalizację, która polega na komunikacji w celu zarządzania siecią. Gdy wybierzesz inny numer na swoim zwykłym telefonie, inicjuje to proces sygnalizacji w celu zlokalizowania wywoływanego abonenta i wywołanie jego dzwonka. Oprócz konfiguracji połączenia sygnalizacja obsługuje informacje o bilingu, czysto kończy połączenie i wykonuje kilka innych rzeczy.

Sygnalizacja polega na komunikacji w celu zarządzania siecią.

SIP i H.323

W Voice over IP istnieją dwa główne standardy sygnalizacji. Starsze systemy zwykle są zgodne ze standardem sygnalizacji H.323 OSI. Nowsze systemy zwykle są zgodne ze standardem sygnalizacji IETF Session Initiation Protocol (SIP). Skoncentrujemy się na sygnalizacji SIP, ale zagrożenia dla sygnalizacji H.323 są podobne.

Rejestracja

Pierwszy aspekt sygnalizacji polega na rejestracji. Telefon użytkownika łączy się z serwerem rejestratora i przedstawia poświadczenia użytkownika (takie jak hasło, kod PIN lub coś silniejszego). Serwer rejestratora dodaje następnie użytkownika i jego lokalizację do swojej bazy danych rejestracji. Serwery proxy, które zobaczymy dalej, wykorzystują informacje rejestracyjne do kierowania połączeń.

Serwery proxy SIP

Użytkownik telefonu IP na rysunku wysyła wiadomość SIP INVITE do softphonu PC, aby zażądać połączenia. Oczywiście dzwoniący telefon nie wie, jak dodzwonić się do wywoływanego telefonu. W konsekwencji telefon IP wysyła wiadomość INVITE do serwera proxy SIP nadawcy. Ten serwer proxy sprawdza informacje rejestracyjne telefonu IP, a następnie kontaktuje się z serwerem proxy w sieci strony wywoływanej. Ten serwer proxy przekazuje wiadomość INVITE do wywoływanego telefonu programowego. Jeśli wywoływany telefon VoIP odeśle komunikat OK, komunikacja SIP będzie kontynuowana do momentu nawiązania sesji. Po ustanowieniu sesji dwa telefony VoIP komunikują się ze sobą bezpośrednio w trybie transportu za pomocą pakietów RTP. Serwery proxy SIP nie są zaangażowane w tryb transportu, chyba że potrzebna jest dodatkowa sygnalizacja nadzorcza.

Bramka PSTN

Co się stanie, jeśli telefon IP lub telefon programowy musi zadzwonić do kogoś w publicznej komutowanej sieci telefonicznej (lub odwrotnie)? VoIP i PSTN wykorzystują różne kodeki, technologię transportu i systemy sygnalizacji. W związku z tym połączenie wzajemne wymaga użycia bramy PSTN, która może dokonywać translacji między różnymi technologiami.

TEST

a. Rozróżnij transport i sygnalizację.

b. Na rysunku 8-25, czy pakiet jest pokazany jako pakiet transportowy czy pakiet sygnalizacyjny?

c. Jakie są dwa główne standardy sygnalizacji w VoIP?

d. Co robi serwer rejestratora? (Wskazówka: nie mów: „Rejestruje rzeczy").

e. Jakiego typu wiadomości SIP używa telefon VoIP, gdy chce połączyć się z innym telefonem VoIP?

f. W jaki sposób ta wiadomość jest kierowana do wywoływanego telefonu VoIP?

g. Czy serwery proxy SIP są zaangażowane w transmisje transportowe? Wyjaśniać.

h. Jakie dwa rodzaje komunikacji obsługuje brama medialna między siecią VoIP a siecią PSTN?

Zagrożenia VoIP

Technologia VoIP napotyka wiele zagrożeń, ponieważ nie jest systemem zamkniętym, takim jak publiczna komutowana sieć telefoniczna. Atakujący zazwyczaj mogą dostać się do sieci VoIP za pośrednictwem Internetu i punktów dostępu do bezprzewodowej sieci LAN.

Podsłuchiwanie

Słuchanie połączenia głosowego bez pozwolenia to podsłuchiwanie. Jest to bardzo łatwe w tradycyjnej telefonii. Operatorzy telefoniczni z prostymi krokodylkami mogą z łatwością podłączyć słuchawkę do fizycznej linii telefonicznej i słuchać rozmów. Podsłuchiwanie jest trudniejsze w sieciach VoIP. Interceptory zazwyczaj muszą wybrać konkretne połączenie z dużego strumienia połączeń, a następnie odszyfrować pakiety. Jednak technologia to ułatwia.

Ataki typu „odmowa usługi"

Przeciwnicy mogą wykorzystywać ataki typu „odmowa usługi" (DoS) na telefony, serwery proxy, serwery rejestratorów, bramy PSTN i inne elementy sieci VoIP. Ataki DoS są zwykle bardzo skuteczne, ponieważ nawet niewielki wzrost opóźnień (opóźnień), fluktuacji (zmienne opóźnienie między pakietami) lub zmniejszonej przepustowości może spowodować, że połączenie stanie się niezrozumiałe. Ruch VoIP jest szczególnie wrażliwy na opóźnienia. Jeśli opóźnienie wzrośnie do zaledwie 150 ms do 250 ms, odbieranie połączeń staje się prawie niemożliwe. Właśnie wtedy, gdy myślisz, że druga osoba przestała mówić, a ty zaczynasz mówić, słyszysz więcej jej głosu, przerywając ci.

Podszywanie się pod rozmówcę

Przez telefon dzwoniący może udawać, że jest kimś, kim nie jest. W sieci PSTN identyfikator dzwoniącego zmniejsza nieco to ryzyko, podając rzeczywisty numer dzwoniącego. Podszywanie się pod dzwoniącego jest również możliwe w przypadku telefonów IP i telefonów programowych. W rzeczywistości może być bardziej skuteczny. Jeśli identyfikacja połączeń w VoIP podaje nazwisko osoby lub stanowisko w organizacji, a także numer telefonu IP, podszywanie się wydaje się jeszcze bardziej uzasadnione. Jeśli zadzwoni do ciebie prezes firmy lub szef ochrony, prawdopodobnie zrobisz to, co ci każą.

Hakowanie i ataki złośliwego oprogramowania

Jeśli atakujący włamie się do telefonu VoIP lub serwera VoIP lub z powodzeniem umieści na nim złośliwe oprogramowanie, stanie się on „właścicielem" urządzenia. Dodatkowe ataki z wykorzystaniem

zhakowanego urządzenia stają się trywialne. Na przykład atakujący może wysyłać polecenia SIP BYE do wielu telefonów, powodując zakończenie rozmów.

Oszustwo związane z opłatami drogowymi

Do tej pory przyglądaliśmy się wyrafinowanym atakom wymierzonym w duże złośliwe cele. Mniejszym, ale wciąż ważnym zagrożeniem jest oszustwo związane z opłatami drogowymi – włamanie się do korporacyjnego systemu VoIP w celu wykonywania bezpłatnych połączeń międzymiastowych i międzynarodowych. Chociaż może się to wydawać trywialnym zagrożeniem, włamanie, po którym następuje udostępnienie exploita wielu atakującym, może prowadzić do znacznych strat w dolarach.

Spam przez telefonię IP

Jednym z pojawiających się zagrożeń jest spam w telefonii IP (SPIT). Korporacje poświęcają już dużo czasu i wysiłku na kontrolowanie spamu w wiadomościach e-mail. VoIP może być jeszcze łatwiejszym sposobem dostarczania spamu, a SPIT byłby znacznie bardziej zakłócający niż spam e-mailowy, ponieważ dzwoniący telefon jest trudny do zignorowania.

Nowe zagrożenia

Przyjrzeliśmy się dzisiaj głównym zagrożeniom dla VoIP, ale wciąż pojawiają się nowe zagrożenia. Na przykład teoretyczny exploit RTP może umożliwić hakerowi wprowadzenie swojego głosu do strumienia docierającego do odbiorcy. Zwiększając szkody, prawdziwy mówca nie słyszałby dodatkowego głosu docierającego do odbiorcy.

TEST

a. Co to jest podsłuchiwanie?

b. Dlaczego ataki DoS mogą być skuteczne, nawet jeśli tylko nieznacznie zwiększają opóźnienie?

c. Dlaczego podszywanie się pod rozmówcę jest szczególnie niebezpieczne w VoIP?

d. Dlaczego hakerstwo i złośliwe oprogramowanie są niebezpieczne w VoIP?

e. Co to jest oszustwo związane z opłatami drogowymi?

f. Co to jest SPIT?

g. Dlaczego SPIT jest bardziej uciążliwy niż SPAM w e-mailach?

Wdrażanie bezpieczeństwa VoIP

Pierwszym krokiem w tworzeniu bezpieczeństwa VoIP jest dobre zabezpieczenie podstawowe. Jeśli podstawowe zabezpieczenia firmy są silne, dodanie środków bezpieczeństwa VoIP będzie stosunkowo proste. Jeśli podstawowe zabezpieczenia firmy są słabe, bezpieczeństwo VoIP będzie prawie niemożliwe.

Uwierzytelnianie

Sposobem radzenia sobie z zagrożeniami związanymi z podszywaniem się jest wymaganie silnego uwierzytelniania. Wewnętrznie firmy mogą wdrażać własne systemy uwierzytelniania. Na przykład korzystanie z telefonu IP lub telefonu programowego może wymagać od użytkownika wprowadzenia nazwy użytkownika i hasła lub kodu PIN. Firmy mogą również używać silniejszego uwierzytelniania. A co z połączeniami VoIP między firmami? IETF opracowała tożsamość SIP (RFC 4474) do uwierzytelniania w domenach drugiego poziomu. Serwery proxy podpisują wiadomości SIP (takie jak INVITE) za pomocą

własnych kluczy prywatnych serwerów. Serwery odbierające wiadomości SIP mogą zapewnić, że pochodzą one z domeny drugiego poziomu, z której twierdzą, że pochodzą, sprawdzając podpis cyfrowy za pomocą klucza publicznego domeny drugiego poziomu znajdującego się w jej certyfikacie cyfrowym.

Szyfrowanie w celu zachowania poufności

Oczywistym sposobem udaremnienia podsłuchu jest szyfrowanie zarówno ruchu transportowego, jak i komunikatów sygnalizacyjnych. Na przykład telefony IP i telefony programowe mogą szyfrować ruch przed jego wysłaniem. Alternatywnie firma może szyfrować tylko ruch przechodzący niezabezpieczone łącza, takie jak Internet. W takim przypadku firma korzystałaby z wirtualnej sieci prywatnej (VPN). Szyfrowanie zawsze dodaje niewielkie opóźnienie. Na przykład szyfrowanie programowe zwykle dodaje opóźnienie od 5 ms do 15 ms. To dodatkowe opóźnienie może pogorszyć jakość głosu, dlatego pożądane jest szyfrowanie sprzętowe.

Zapory sieciowe

VoIP rzuca wyzwanie technologii firewall. Najwyraźniej ruch VoIP składa się z wielu małych pakietów. Zapory sieciowe często mają trudności z tego typu ruchem. Zapory sieciowe muszą również mieć możliwość ustalania priorytetów ruchu VoIP, aby zminimalizować opóźnienia. Co najważniejsze, filtrowanie zapory nie może powodować znacznego opóźnienia w dostarczaniu pakietów. Niektóre firmy w niewielkim stopniu lub wcale nie filtrują pakietów transportowych przez firewall, skupiając się zamiast tego na rzadszych (ale bardziej niebezpiecznych) pakietach sygnalizacyjnych. VoIP stanowi wyzwanie dla filtrowania zapory opartej na portach. Najwyraźniej zapora musi zezwalać na ruch przychodzący na porty sygnalizacyjne. W przypadku SIP jest to port 5060. H.323 natomiast używa do sygnalizacji portów 1719 i 1720. Sygnalizacja jest złożona, a zapora powinna znać protokół sygnalizacyjny w celu wykrywania zagrożeń, takich jak ryzykowne polecenia SIP, które powinny być blokowane. W przypadku połączeń transportowych VoIP wymaga otwarcia osobnego portu dla każdego połączenia transportowego między użytkownikami. Zapory sieciowe muszą być w stanie odczytać protokół SIP (i H.323), aby dowiedzieć się, jaki port protokół sygnalizacyjny przypisuje do każdego połączenia transportowego. Musi następnie otworzyć ten port na bardzo krótki czas, zamykając port natychmiast po zakończeniu połączenia, aby zmniejszyć ryzyko.

Problemy z translacją NAT

Jak zauważono w rozdziale 6, NAT powoduje problemy z niektórymi protokołami. Protokoły te zawierają w swoich komunikatach adresy IP warstwy 3. Jeśli NAT zmieni adres docelowy IP, protokół przestanie działać poprawnie. Sygnalizacja VoIP ma tego rodzaju problem z zaporami NAT. Ponadto translacja adresów IP i numerów portów NAT zająć niewielką ilość czasu, która zwiększa opóźnienie.

Separacja: antykonwergencja

Jednym z celów VoIP jest zapewnienie konwergencji przy użyciu jednej sieci IP zarówno dla głosu, jak i danych. Jednak bezpieczeństwo może wymagać ograniczonego rozdzielenia ruchu głosowego i transmisji danych. Najważniejszym aspektem separacji jest wykorzystanie wirtualnych sieci LAN (VLAN). Umieszczenie głosu i danych w oddzielnych sieciach VLAN utrudnia atakującym przechodzącym przez stronę danych atakowanie usług VLAN. Nawet w ramach technologii głosowej dobrym pomysłem jest umieszczenie serwerów w innych sieciach VLAN niż telefony IP i telefony programowe, aby ograniczyć ataki na serwery z telefonów, które są łatwiejsze do złamania niż serwery. Jeśli firma korzysta z serwerów opartych na systemie Windows, może nawet umieścić wszystkie serwery VoIP w jednej domenie Windows w celu zarządzania przez specjalnie przeszkoloną grupę pracowników VoIP.

TEST

a. Jakie mechanizmy uwierzytelniania są wspólne w telefonach IP?

b. Co zapewnia tożsamość SIP?

c. Jak można udaremnić podsłuchiwanie?

dD. Jakie problemy z jakością dźwięku może powodować szyfrowanie?

e. Dlaczego firewalle mają problemy z typowym ruchem VoIP?

f. Dla sygnalizacji SIP, jaki port musi być otwarty na firewallach?

g. Opisz otwory portów zapory dla transportu VoIP.

h. Dlaczego przechodzenie przez NAT jest problematyczne?

i. Jak przydatne są sieci VLAN w VoIP?

Usługa Skype VoIP

Publiczna usługa VoIP Skype oferuje obecnie bezpłatne rozmowy telefoniczne wśród klientów Skype przez Internet oraz obniżone koszty połączeń do i od klientów PSTN. Skype jest niezwykle popularny wśród konsumentów. Jednak niektóre korporacje zakazują Skype'a. Skype używa zastrzeżonego oprogramowania i protokołów, które nie zostały zbadane przez specjalistów ds. bezpieczeństwa. Powoduje to, że specjaliści ds. bezpieczeństwa obawiają się istnienia luk, tylnych drzwi i innych zagrożeń bezpieczeństwa. Chociaż Skype używa szyfrowania w celu zachowania poufności, jego metoda jest nieznana. Co gorsza, Skype kontroluje klucze szyfrowania, dzięki czemu może odczytywać ruch, jeśli chce.

Szczególnie ważną kwestią jest to, że Skype nie zapewnia odpowiedniego uwierzytelniania. Chociaż Skype uwierzytelnia użytkowników za każdym razem, gdy wchodzą do sieci Skype, początkowa rejestracja jest otwarta i niekontrolowana, więc nazwy użytkowników nic nie znaczą z punktu widzenia bezpieczeństwa. Atakujący może rejestrować imiona innych osób i podszywać się pod nie. Innym problemem jest to, że Skype jest usługą peer-to-peer (P2P), która jest prawie niemożliwa do kontrolowania na zaporach ogniowych, ponieważ protokół Skype jest nieznany i często się zmienia, aby uniknąć analizy. Skype wykorzystuje swoją strukturę, aby pomóc użytkownikom w komunikacji przez zapory NAT. Jest to dobre dla użytkownika, ale złe dla bezpieczeństwa firmy. Mechanizm przesyłania plików Skype nie musi również działać z produktami antywirusowymi. Ogólnie rzecz biorąc, chociaż większość tych obaw dotyczących Skype'a ma charakter teoretyczny, fakt, że Skype nie może być dobrze kontrolowany przez korporacyjne zasady bezpieczeństwa, czyni go nie do przyjęcia w wielu firmach.

TEST

a. Co to jest Skype?

b. Dlaczego korzystanie przez Skype z zastrzeżonego oprogramowania jest problematyczne?

c. Jaki jest problem z szyfrowaniem Skype'a dla zachowania poufności?

d. Czy Skype kontroluje, kto może zarejestrować nazwisko konkretnej osoby?

e. Dlaczego zapory mają trudności z kontrolowaniem Skype'a?

f. Czy transfer plików przez Skype ogólnie działa z programami antywirusowymi?

g. Ogólnie rzecz biorąc, jaki jest duży problem ze Skype'em?

INNE APLIKACJE UŻYTKOWNIKA

Przyjrzeliśmy się kilku ważnym aplikacjom korporacyjnym. Jest jednak wiele innych. Przyjrzymy się kilku pokrótce. Wiadomości błyskawiczne Większość ludzi myśli o wiadomościach błyskawicznych (IM) jako o komunikacji przejściowej. Jednak większość tych samych przepisów, które wymagają przechowywania wiadomości e-mail, wymaga również przechowywania wiadomości błyskawicznych. Wiele systemów komunikatorów korzysta tylko z serwerów obecności. Serwery obecności umożliwiają obu stronom wzajemne zlokalizowanie się (podobnie jak serwery proxy SIP w VoIP). Następnie komunikacja odbywa się w trybie peer-to-peer między dwoma użytkownikami IM. Serwery nie są już w ogóle zaangażowane. Inną opcją jest użycie serwera przekazującego IM. Wszystkie wiadomości przechodzą przez serwer przekazujący. Pozwala to firmie filtrować komunikatory internetowe pod kątem nieodpowiednich treści. Pozwala to również firmie spełnić wymogi prawne dotyczące przechowywania i inne wymogi dotyczące zgodności. W związku z tym korporacyjne systemy IM powinny używać serwera przekazującego, a nie serwera obecności.

TEST

a. W komunikatorze, co robi serwer obecności?

b. Co robi serwer przekazujący?

c. W przypadku korporacyjnych wiadomości błyskawicznych, jakie są zalety korzystania z serwera przekazującego zamiast samego serwera obecności?

Szczególnie ważną kwestią jest to, że Skype nie zapewnia odpowiedniego uwierzytelniania. Chociaż Skype uwierzytelnia użytkowników za każdym razem, gdy wchodzą do sieci Skype, początkowa rejestracja jest otwarta i niekontrolowana, więc nazwy użytkowników nic nie znaczą z punktu widzenia bezpieczeństwa. Atakujący może rejestrować imiona innych osób i podszywać się pod nie. Innym problemem jest to, że Skype jest usługą peer-to-peer (P2P), która jest prawie niemożliwa do kontrolowania na zaporach ogniowych, ponieważ protokół Skype jest nieznany i często się zmienia, aby uniknąć analizy. Skype wykorzystuje swoją strukturę, aby pomóc użytkownikom w komunikacji przez zapory NAT. Jest to dobre dla użytkownika, ale złe dla bezpieczeństwa firmy. Mechanizm przesyłania plików Skype nie musi również działać z produktami antywirusowymi. Ogólnie rzecz biorąc, chociaż większość tych obaw dotyczących Skype'a ma charakter teoretyczny, fakt, że Skype nie może być dobrze kontrolowany przez korporacyjne zasady bezpieczeństwa, czyni go nie do przyjęcia w wielu firmach.

TEST

a. Co to jest Skype?

b. Dlaczego korzystanie przez Skype z zastrzeżonego oprogramowania jest problematyczne?

c. Jaki jest problem z szyfrowaniem Skype'a dla zachowania poufności?

d. Czy Skype kontroluje, kto może zarejestrować nazwisko konkretnej osoby?

e. Dlaczego zapory mają trudności z kontrolowaniem Skype'a?

f. Czy transfer plików przez Skype ogólnie działa z programami antywirusowymi?

g. Ogólnie rzecz biorąc, jaki jest duży problem ze Skype'em?

INNE APLIKACJE UŻYTKOWNIKA

Przyjrzeliśmy się kilku ważnym aplikacjom korporacyjnym. Jest jednak wiele innych. Przyjrzymy się kilku pokrótce. Wiadomości błyskawiczne Większość ludzi myśli o wiadomościach błyskawicznych (IM) jako o komunikacji przejściowej. Jednak większość tych samych przepisów, które wymagają przechowywania wiadomości e-mail, wymaga również przechowywania wiadomości błyskawicznych. Wiele systemów komunikatorów korzysta tylko z serwerów obecności. Serwery obecności umożliwiają obu stronom wzajemne zlokalizowanie się (podobnie jak serwery proxy SIP w VoIP). Następnie komunikacja odbywa się w trybie peer-to-peer między dwoma użytkownikami IM. Serwery nie są już w ogóle zaangażowane. Inną opcją jest użycie serwera przekazującego IM. Wszystkie wiadomości przechodzą przez serwer przekazujący. Pozwala to firmie filtrować komunikatory internetowe pod kątem nieodpowiednich treści. Pozwala to również firmie spełnić wymogi prawne dotyczące przechowywania i inne wymogi dotyczące zgodności. W związku z tym korporacyjne systemy IM powinny używać serwera przekazującego, a nie serwera obecności.

TEST

a. W komunikatorze, co robi serwer obecności?

b. Co robi serwer przekazujący?

c. W przypadku korporacyjnych wiadomości błyskawicznych, jakie są zalety korzystania z serwera przekazującego zamiast samego serwera obecności?

Aplikacje nadzoru TCP/IP

TCP/IP obsługuje wiele protokołów nadzorczych, w tym między innymi ARP, ICMP, DNS, DHCP, LDAP, RIP, OSPF, BGP i SNMP. Te protokoły nadzorcze są ulubionymi celami atakujących, ponieważ zakłócenie protokołów nadzorczych może zakłócić działanie całego Internetu. Mamy tylko miejsce, by przyjrzeć się jednemu protokołowi nadzorczemu, ale IETF ma długoterminowy program zwany Doktryną Danversa. Celem jest dodanie silnych zabezpieczeń do wszystkich protokołów nadzorczych i protokołów aplikacji. Przyjrzymy się protokołowi Simple Network Management Protocol (SNMP), który pozwala firmie kontrolować wiele zdalnie zarządzanych urządzeń z centralnego menedżera. Polecenie SNMP GET umożliwia menedżerowi proszenie zarządzanych urządzeń o przesłanie informacji o ich stanie. Z kolei polecenie SNMP SET umożliwia menedżerowi polecenie zdalnie zarządzanym urządzeniom, aby zmieniły swoją konfigurację. Ze względu na szkody, jakie atakujący mogą wyrządzić za pomocą polecenia SET, jeśli zabezpieczenia nie są doskonałe, wiele firm wyłącza polecenie SET. W ten sposób tracą oszczędności wynikające ze zdalnej konfiguracji, zamiast podróżować do każdego zarządzanego urządzenia w celu zmiany konfiguracji. SNMP w wersji 1 nie posiadał żadnych zabezpieczeń, co sprawiało, że protokół był wyjątkowo niebezpieczny, biorąc pod uwagę jego moc. SNMP w wersji 2 miał dodać zabezpieczenia, ale brak możliwości wyrównania różnic w ramach IETF zapobiegał silnemu zabezpieczeniu. Wersja 2 wprowadziła ciąg społeczności. To „sekret” wspólny dla menedżera i wszystkich zarządzane urządzenia. Wspólna tajemnica rzadko pozostaje tajemnicą. W rzeczywistości SNMP V2 wysyła wspólne hasło w postaci jawnej w wiadomościach. Co najgorsze, większość dostawców używa domyślnego ciągu społeczności „public”. Wersja 3 w końcu dodała indywidualne sekrety dzielone między menedżerem a każdym zarządzanym urządzeniem. SNMP V3 oferował również poufność (opcjonalnie), integralność wiadomości i znaczniki czasu w celu ochrony przed atakami typu powtórka. Mamy nadzieję, że nowsza wersja doda uwierzytelnianie za pomocą klucza publicznego. Rozwój bezpieczeństwa w SNMP jest powtarzany w innych protokołach

nadzorczych TCP/IP. Specjaliści ds. bezpieczeństwa IT muszą ściśle współpracować z personelem sieci korporacyjnej, aby zapewnić firmie odpowiednie zabezpieczenia protokołu nadzoru sieci. Osoby zajmujące się bezpieczeństwem IT tradycyjnie nie były aktywne w tym obszarze.

TEST

a. Czym jest doktryna Danversa?

b. Rozróżnij bezpieczeństwo w SNMP V1 i bezpieczeństwo w SNMP V2.

c. Rozróżnij zabezpieczenia w SNMP V2 i zabezpieczenia w SNMP V3.

d. Co jeszcze należy zrobić, aby zapewnić bezpieczeństwo SNMP?

WNIOSEK

Przyjrzeliśmy się utwardzaniu aplikacji. Na początku tego rozdziału przyjrzeliśmy się ogólnym zasadom aplikacji hartowania. Należą do nich:

• Zrozumienie roli serwera i środowiska zagrożeń

• Podstawy: bezpieczeństwo fizyczne, tworzenie kopii zapasowych, wzmacnianie systemu operacyjnego

• Minimalizuj aplikacje

• Twórz bezpieczne konfiguracje

• Zainstaluj poprawki

• Zminimalizuj uprawnienia aplikacji

• Dodaj uwierzytelnianie, autoryzacje i audyt w warstwie aplikacji

• Wdrażanie systemów kryptograficznych

• Bezpieczne aplikacje niestandardowe

Przyjrzano się następnie kwestiom bezpieczeństwa związanym z siecią i handlem elektronicznym. Skupiono się na skutkach przepełnienia bufora i ataków przekrojowych. Podkreślono również potrzebę narzędzi do oceny podatności, odczytywania dzienników oraz posiadania oddzielnych środowisk produkcyjnych i testowych. Kolejna sekcja skupiała się na atakach specyficznych dla przeglądarek internetowych. Omówiono potencjalne złośliwe zastosowania kodu mobilnego, Active-X, Javascript, plików cookie i złośliwych linków. Ta sekcja zawierała artykuł dotyczący zatruwania wyszukiwarek, spamu linkami, farm linków, pająków i strategii wyszukiwarek. Następnie przyjrzeliśmy się lukom w aplikacjach związanym z pocztą e-mail i VoIP. Poczta e-mail stała się centralnym punktem w kwestiach bezpieczeństwa ze względu na możliwość przesyłania aktywnej zawartości za pomocą załączników do wiadomości e-mail i kodu HTML. Wszechobecny charakter wiadomości e-mail zmusił firmy do inwestowania zasobów w środki ochronne, takie jak filtrowanie spamu, szyfrowanie wiadomości e-mail i narzędzia zapobiegające ekstruzji. VoIP jest atrakcyjny dla korporacji, ponieważ może zapewniać obsługę głosu w sieci danych. Może to obniżyć koszty operacyjne, ponieważ eliminuje potrzebę oddzielnej sieci głosowej i tradycyjnych opłat telefonicznych. Może również zapewniać bezpieczne połączenia głosowe i jest niezależny od lokalizacji. Ponieważ jednak VoIP działa w sieci danych, to jest potencjalnie podatny na ataki DoS, podszywanie się, złośliwe oprogramowanie, oszustwa związane z opłatami, spam i podsłuchiwanie. Na koniec, w tym rozdziale przyjrzyliśmy się pokrótce dwóm różnym

typom serwerów wiadomości błyskawicznych — serwerom obecności i serwerom przekazującym - i omówiono ich wpływ na korporację. Zakończyliśmy dyskusją na temat złośliwego wykorzystania protokołów nadzorczych TCP/IP.

Pytania do przemymyślenia

1. Czy uważasz, że programiści powinni mieć możliwość tworzenia dynamicznych stron internetowych po stronie serwera, biorąc pod uwagę związane z tym niebezpieczeństwa?

2. Ataki skryptowe po stronie klienta zwykle wymagają, aby klient odwiedził serwer sieciowy ze złośliwą zawartością. Jak myślisz, w jaki sposób atakujący skłaniają użytkowników do odwiedzania takich stron internetowych?

3. Jakie trzy główne tematy wybralibyście na jednogodzinną sesję szkoleniową dla użytkowników na temat bezpieczeństwa poczty e-mail? To pytanie wymaga, abyś był

selektywny. Nie twórz tematów, które są bardzo szerokie, aby uniknąć selektywności.

4. Jakie trzy główne tematy wybralibyście na jednogodzinną sesję szkoleniową dla menedżerów wyższego szczebla na temat bezpieczeństwa poczty e-mail? To pytanie wymaga selektywności. Nie twórz tematów, które są bardzo szerokie, aby uniknąć selektywności.

5. Pracownik pracujący w domu skarży się, że niektóre z jej wiadomości do współpracowników w siedzibie firmy nie docierają. Co może być problemem?

6. Firma jest ostrzegana przez wydawców kart kredytowych, że zostanie zaklasyfikowana jako firma wysokiego ryzyka, chyba że natychmiast zmniejszy liczbę nieuczciwych zakupów dokonywanych przez swoich klientów handlu elektronicznego. Opracuj plan, aby uniknąć tego wyniku.

OCHRONA DANYCH

WPROWADZENIE

W poprzednich częściach koncentrowaliśmy się na ochronie danych przesyłanych przez sieci, wzmacnianiu hostów przechowujących dane oraz zabezpieczaniu aplikacji przetwarzających dane. Tylko pokrótce przyjrzeliśmy się ochronie danych przechowywanych na hostach. W tym rozdziale położymy szczególny nacisk na dane i znaczenie ochrony danych. Zrobiono to raczej, aby poczekać, aż dane będą mogły być uwypuklone.

Rola danych w biznesie

Dane są ważne, ponieważ stanowią główny element każdego systemu informacyjnego. Systemy informacyjne nie mogą bez niego funkcjonować. Systemy informacyjne istnieją w celu przechowywania, przesyłania i przetwarzania danych. W rzeczywistości ostatecznym celem wszystkich poprzednich rozdziałów tej książki była ochrona danych. Współczesne firmy gromadzą ogromne ilości danych lub surowych faktów, które muszą być chronione. Informacja, czyli wyekstrahowana z danych, ma kluczowe znaczenie dla podejmowania dobrych decyzji na wszystkich poziomach organizacji. Jest to również cenny zasób wykorzystywany w ramach większej strategii korporacyjnej. Ochrona danych jest jeszcze ważniejsza dla firm z branż opartych na informacjach. Firmy te muszą przechowywać poufne informacje, takie jak kod źródłowy, własność intelektualna i dane użytkowników, ponieważ stanowią one część ich podstawowej przewagi konkurencyjnej. Niepodjęcie niezbędnych kroków wymaganych do odpowiedniej ochrony danych firmowych może prowadzić do utraty przychodów, zirytowania użytkowników, negatywnych relacji prasowych, zerwania relacji partnerskich i procesów sądowych.

NARUSZENIA DANYCH SONY

Przykładem tego, jak szkodliwa może być utrata danych, jest seria ataków na Sony Corp. Po wielokrotnych atakach hakerzy byli w stanie tymczasowo zmusić Sony do zamknięcia PlayStation Network oraz wielu firmowych witryn internetowych. Sony straciło również dane klientów dla ponad 100 milionów kont użytkowników. Kazuo Hirai, wiceprezes wykonawczy Sony, skomentował ciąg wydarzeń ataków. „Ten czyn przestępczy przeciwko naszej sieci miał znaczący wpływ nie tylko na naszych konsumentów, ale na całą naszą branżę. Te nielegalne ataki w oczywisty sposób podkreślają powszechny problem związany z cyberbezpieczeństwem. Bardzo poważnie traktujemy bezpieczeństwo informacji naszych konsumentów i zobowiązujemy się pomagać naszym konsumentom w ochronie ich danych osobowych”. W kolejnym ataku typu SQL injection hakerzy umieścili część 1 miliona skradzionych nazw użytkowników i haseł na popularnej witrynie do udostępniania plików. Niestety skradzione hasła były przechowywane jako zwykły tekst. Osoby atakujące opublikowały również dane zawierające imiona i nazwiska, adresy e-mail, numery telefonów, daty urodzenia, kupony muzyczne, układ bazy danych oraz mapy wewnętrznej sieci korporacyjnej Sony.

Zabezpieczanie danych

Ataki na dane mogą mieć miejsce podczas ich przechowywania, przesyłania lub przetwarzania. Korzystanie z bezpiecznego systemu kryptograficznego może zapobiec atakom podczas przesyłania danych. Odpowiednio wzmocnione hosty i bezpiecznie zakodowane aplikacje mogą pomóc chronić dane podczas ich przetwarzania.

Skupimy się przede wszystkim na zabezpieczaniu danych podczas ich przechowywania. Przyjrzymy się bliżej (1) w jaki sposób tworzenie kopii zapasowych może zapobiec przypadkowej utracie danych, (2)

jak bezpiecznie przechowywać dane w bazie danych, (3) jak zapobiec wyjęciu danych z firmy oraz (4) jak bezpiecznie usuwać dane.

TEST

a. Jaka jest różnica między danymi a informacjami?

b. Jak chronić dane podczas ich przesyłania?

c. Jak chronić dane w trakcie ich przetwarzania?

d. W jaki sposób dane mogą zostać zaatakowane podczas ich przechowywania?

e. Jak chronić dane podczas ich przechowywania?

OCHRONA DANYCH: KOPIA ZAPASOWA

Znaczenie kopii zapasowej

W pierwszej części poświęconej bezpieczeństwu danych zajmiemy się tworzeniem kopii zapasowych, dzięki czemu kopie plików danych są bezpiecznie przechowywane i przetrwają nawet w przypadku utraty lub uszkodzenia danych na hoście. Kopia zapasowa ma kluczowe znaczenie, ponieważ inne zabezpieczenia nieuchronnie ulegną awarii, a Twoje praktyki tworzenia kopii zapasowych określą, ile stracisz. Pod wieloma względami trzy najważniejsze elementy wzmacniania hosta to kopia zapasowa, kopia zapasowa i kopia zapasowa.

Kopia zapasowa zapewnia, że kopie plików danych są bezpiecznie przechowywane i przetrwają, nawet jeśli dane na hoście zostaną utracone, skradzione lub uszkodzone.

Zagrożenia

Istnieje wiele sposobów na utratę danych. Awarie mechanicznych dysków twardych zdarzają się często, a pożary i powodzie mogą zniszczyć dane na wielu komputerach. Oprócz tych zagrożeń niezwiązanych z bezpieczeństwem złośliwe oprogramowanie może usuwać lub zmieniać dane, a urządzenia mobilne mogą zostać skradzione lub zgubione. Niezależnie od tego, w jaki sposób dane zostaną utracone, jedynym wyjściem dla firmy jest przywrócenie danych z ostatniej kopii zapasowej. Kopia zapasowa pomaga osiągnąć cel bezpieczeństwa dostępności. Tworzenie kopii zapasowych danych na nośnikach pamięci zapewnia, że dane będą nadal dostępne w przypadku katastrofalnej awarii hosta.

TEST

a. Wymień sposoby utraty danych, dodając własne.

b. W jaki sposób kopia zapasowa zapewnia dostępność?

c. Czy kiedykolwiek musiałeś użyć kopii zapasowej, aby przywrócić plik? Wyjaśniać.

Zakres kopii zapasowej

Zakres kopii zapasowej to ilość informacji na dysku twardym, która jest objęta kopią zapasową. Trzy stopnie kompletności to (1) tylko pliki danych i katalogi, (2) kopia zapasowa obrazu całego dysku twardego oraz (3) tworzenie cienia każdego pliku, nad którym pracujemy. Każdy jest odpowiedni w różnych okolicznościach.

KOPIA ZAPASOWA PLIKU/KATALOGU

Najpopularniejszym typem kopii zapasowej jest kopia zapasowa danych pliku/katalogu. Jak sama nazwa wskazuje, to podejście tworzy kopie zapasowe tylko danych z programów komputerowych, ustawień rejestru i innych informacji dotyczących dostosowywania. W rzeczywistości może nawet nie wykonać kopii zapasowej wszystkich danych. Może tworzyć kopie zapasowe danych tylko w określonych katalogach. Pod względem zakresu kopii zapasowej znajduje się w środku z trzech podejść. Na komputerze z systemem Windows typowym podejściem do tworzenia kopii zapasowych katalogów/plików jest tworzenie kopii zapasowych Dokumentów (lub Moich dokumentów) oraz innych katalogów wysokiego poziomu, takich jak Muzyka i Obrazy . Jest to stosunkowo proste w konfiguracji. Jednak wielu użytkowników przechowuje aktywne pliki danych na swoich komputerach stacjonarnych i w innych lokalizacjach i muszą wykonać ich kopię zapasową, ponieważ często są to najbardziej aktualne pliki użytkownika. Które katalogi danych powinni tworzyć użytkownicy i administratorzy systemów? Kiedy pacjenci pytają dentystów, które zęby powinni nitkować, powszechna odpowiedź brzmi: „Tylko te, które chcesz zachować”. Porada jest również dobra dla plików danych. Biorąc pod uwagę, że odbudowanie nawet jednego pliku danych od zera zajmie godziny lub dni, o ile w ogóle można go odbudować, wymaganie tworzenia kopii zapasowych wszystkich plików danych jest dobrą zasadą firmy.

KOPIA ZAPASOWA OBRAZU

W przypadku tworzenia kopii zapasowej obrazu cała zawartość dysku twardego jest kopiowana na nośnik kopii zapasowej. Obejmuje to programy, dane, ustawienia personalizacji i wszystkie inne dane. (Innymi słowy, „wszystko” oznacza wszystko.) Nawet jeśli cały dysk twardy zostanie utracony, jego zawartość można przywrócić na tym samym lub innym komputerze. Tworzenie kopii zapasowych plików i katalogów nie zapewnia takiego stopnia ochrony przed utratą. Jednak kopia zapasowa obrazu jest najwolniejszą formą tworzenia kopii zapasowej. Ze względu na tę powolność większość firm wykonuje kopie zapasowe obrazów rzadziej niż kopie zapasowe danych plików/katalogów. Ma to również sens, ponieważ dane zwykle zmieniają się znacznie szybciej niż programy i ustawienia konfiguracyjne. Oczywiście przed zainstalowaniem nowego programu lub modyfikacją konfiguracji innego programu zawsze należy wykonać kopię zapasową obrazu.

ŚLEDZENIE

Trzecim zakresem kopii zapasowej jest shadowing. Podczas tworzenia cienia kopia zapasowa każdego pliku, nad którym pracujemy, jest zapisywana co kilka minut na dysku twardym lub w innej lokalizacji, takiej jak dysk USB (Rysunek 9-4). Jest to ważne, ponieważ w przypadku kopii zapasowej danych pliku/katalogu lub kopii zapasowej obrazu wszystko od ostatniej kopii zapasowej zostanie utracone. Jest to okno straty trwające od kilku godzin do kilku dni, a czasem dłużej. W przypadku cieniowania okno czasowe utraty danych jest bardzo krótkie.

Podczas tworzenia cienia kopia zapasowa każdego pliku, nad którym pracujesz, jest zapisywana co kilka minut na dysku twardym lub w innej lokalizacji, takiej jak dysk flash USB.

Zazwyczaj przestrzeń do przechowywania w cieniu jest bardzo ograniczona. Po przekroczeniu najstarsze pliki są usuwane, aby zrobić miejsce na najnowsze (Rysunek 9-5). Zwykle nie jest to takie złe, ponieważ większość uzupełnień z obszaru cienia wykonuje się w ciągu kilku minut lub dni. Posiadanie wystarczającej ilości miejsca na kopie zapasowe w tle przez kilka dni jest wystarczające — o ile firma wykonuje również regularne kopie zapasowe danych plików/katalogów, kopie zapasowe obrazów lub obie te funkcje częściej niż kopia zapasowa w tle odrzuca pliki.

TEST

a. Rozróżnij kopię zapasową danych pliku/katalogu i kopię zapasową obrazu.

b. Dlaczego kopia zapasowa pliku/katalogu jest atrakcyjna w porównaniu z kopią zapasową obrazu?

c. Dlaczego kopia zapasowa obrazu jest atrakcyjna w porównaniu z kopią zapasową danych plików/katalogów?

d. Co to jest cień?

ei. Jaka jest zaleta tworzenia cienia nad tworzeniem kopii zapasowych plików/katalogów?

f. W jaki sposób ogranicza się cieniowanie?

Pełne i przyrostowe kopie zapasowe

W przypadku tworzenia kopii zapasowych plików/katalogów pełne kopie zapasowe, które rejestrują wszystkie dane na komputerze, mogą zająć dużo czasu. W związku z tym większość firm wykonuje pełną kopię zapasową tylko raz w tygodniu. Wykonują również codzienne przyrostowe kopie zapasowe, które zapisują tylko dane zmienione od czasu ostatniej kopii zapasowej (pełnej lub przyrostowej). Na przykład, jeśli pełna kopia zapasowa ma miejsce w niedzielę, poniedziałkowa przyrostowa kopia zapasowa zapisze tylko informacje zmienione od czasu pełnej kopii zapasowej z niedzieli. Z kolei wtorkowa kopia zapasowa zapisze tylko dane zmienione od poniedziałkowej przyrostowej kopii zapasowej. Środowa przyrostowa kopia zapasowa zapisze dane zmienione od wtorkowej przyrostowej kopii zapasowej. W następną niedzielę ponownie zostanie wykonana pełna kopia zapasowa.

Pełne kopie zapasowe rejestrują wszystkie dane na komputerze. Przyrostowe kopie zapasowe zapisują tylko dane zmienione od czasu ostatniej kopii zapasowej (pełnej lub przyrostowej).

Zaletą wykonywania okresowych pełnych kopii zapasowych, a następnie częstszych kopii przyrostowych jest po prostu to, że tworzenie przyrostowych kopii zapasowych zajmuje mniej czasu. W przypadku dużych dysków twardych z wieloma katalogami danych bardzo ważna jest dzienna prędkość tworzenia kopii zapasowych. Dlatego prawie wszystkie firmy mieszają kopie pełne i przyrostowe. Jednak w przypadku przyrostowych kopii zapasowych przywracanie musi być wykonane ostrożnie. W omówionym wcześniej przykładzie załóżmy, że dysk twardy ulegnie awarii w środę. Odtwarzający musi najpierw przywrócić pełną kopię zapasową z niedzieli, następnie przyrostową kopię zapasową z poniedziałku, a następnie przyrostową kopię zapasową z wtorku. Innymi słowy, kopie zapasowe muszą być przywracane w kolejności, w jakiej zostały utworzone. W przeciwnym razie nowsze pliki mogą zostać nadpisane przez starsze pliki.

Pełne i przyrostowe kopie zapasowe należy przywracać w kolejności, w jakiej zostały utworzone.

Zwykle przechowywanych jest kilka generacji pełnych kopii zapasowych, aby można było odzyskać przypadkowo zmienione pliki jakiś czas temu. W przypadku cotygodniowej kopii zapasowej oznacza to przechowywanie kilku tygodni lub nawet miesięcy pełnych kopii zapasowych. Jednak przyrostowe kopie zapasowe są zwykle odrzucane po wykonaniu następnej pełnej kopii zapasowej.

TEST

a. Dlaczego większość firm nie wykonuje pełnej kopii zapasowej każdej nocy?

b. Co to jest przyrostowa kopia zapasowa (dokładnie)?

c. Pewnej nocy firma wykonuje pełną kopię zapasową. Przez trzy kolejne noce robi przyrostowe kopie zapasowe, które określa jako Greenwich, Dublin i Paris. W przypadku przywracania, jakie kopie zapasowe muszą zostać przywrócone jako pierwsze i drugie?

Technologie tworzenia kopii zapasowych

Istnieje kilka popularnych technologii tworzenia kopii zapasowych, a na horyzoncie pojawiają się kolejne.

LOKALNA KOPIA ZAPASOWA

Tradycyjnie firmy tworzyły kopię zapasową lokalnie, co oznacza, że kopia zapasowa każdego komputera była tworzona indywidualnie. W przypadku lokalnej kopii zapasowej zwykle nie ma możliwości wyegzekwowania zasad. Ponadto nie ma sposobu, aby dowiedzieć się, które komputery zostały zarchiwizowane zgodnie z zasadami tworzenia kopii zapasowych, w jaki sposób wykonano kopie zapasowe ani w jaki sposób dane były chronione.

Scentralizowana kopia zapasowa

Aby uniknąć tych problemów, wiele firm korzysta ze scentralizowanego tworzenia kopii zapasowych. Jak pokazano na rysunku 9-8, kopia zapasowa jest wykonywana przez sieć z centralnej konsoli kopii zapasowych. Ta konsola to zwykle komputer PC. Centralna konsola tworzenia kopii zapasowych ma taśmę magnetyczną lub inny sprzęt pamięci masowej. W ustalonym czasie centralna konsola kopii zapasowych „wyciąga" dane, które mają zostać zarchiwizowane, z każdego serwera (a czasem każdego klienta), za który jest odpowiedzialna. Scentralizowana kopia zapasowa oznacza, że tylko jeden lub dwa komputery muszą mieć sprzęt do tworzenia kopii zapasowych. Dzięki temu opłacalne jest kupowanie bardzo dobrego sprzętu do tworzenia kopii zapasowych. Scentralizowana kopia zapasowa ułatwia ustalenie, czy przestrzegane są zasady tworzenia kopii zapasowych. Scentralizowana kopia zapasowa ma również tendencję do przynoszenia korzyści płynących z pojedynczego, dobrze zorganizowanego i dobrze utrzymanego repozytorium nośników kopii zapasowych.

CIĄGŁA OCHRONA DANYCH

Opcją dostępną dla firm, które mają dwie serwery, jest ciągła ochrona danych (CDP), w której każda witryna tworzy kopię zapasową drugiej. Ponadto, jak wskazuje nazwa, CDP wykonuje kopie zapasowe w czasie rzeczywistym. Jeśli jedna strona ulegnie awarii, druga strona może natychmiast przejąć obciążenie przetwarzania, z niewielką utratą danych lub bez utraty danych. W przypadku odzyskiwania po awarii, protokół CDP jest postrzegany jako obowiązkowy. Oczywiście CDP wymaga bardzo szybkiego (a zatem drogiego) łącza transmisji danych między tymi dwoma lokalizacjami.

INTERNETOWA USŁUGA KOPII ZAPASOWEJ

Wielu dostawców kopii zapasowych oferuje obecnie usługę tworzenia kopii zapasowych przez Internet. Jest to stosunkowo wygodne dla użytkowników komputerów klienckich, którzy w przeciwnym razie nie mogliby tworzyć kopii zapasowych swoich komputerów. Jednak szybkość dostępu do Internetu jest niska w porównaniu z szybkością transmisji sieciowej, więc wysyłanie dużych części dysku twardego przez Internet do dostawcy pamięci masowej będzie wymagało dużo czasu. Ponadto istnieje obawa, że firma będąca właścicielem komputera straci kontrolę nad swoimi danymi, co może być katastrofalne.

KOPIA ZAPASOWA SIATKI

Nową opcją dla komputerów klienckich jest tworzenie kopii zapasowych typu mesh, w którym komputery klienckie w organizacji tworzą kopie zapasowe. Jak pokazano na rysunku 9-9, tworzenie kopii zapasowych w sieci mesh to aplikacja typu peer-to-peer. Każdy komputer wysyła paczki swoich plików kopii zapasowych do kilku innych komputerów klienckich. Oczywiście pokazany klient wysyłający swoją paczkę zapasową do innych komputerów otrzyma również paczki zapasowe z innych komputerów. Tworzenie kopii zapasowych w sieci mesh stwarza ogromne problemy techniczne. Po pierwsze, operacja tworzenia kopii zapasowej typu mesh nie może spowalniać komputera, na którym zapisywane są pakiety lub z którego pakiety są pobierane. Po drugie, określone komputery klienckie nie zawsze są dostępne do pobierania pakietów, więc paczki muszą być wysyłane nadmiarowo. Najtrudniejszym problemem technicznym jest bezpieczeństwo. Gdy komputer kliencki otrzymuje przesyłkę zapasową, jego użytkownik nie może jej czytać, modyfikować ani usuwać. Pomimo tych problemów, tworzenie kopii zapasowych w postaci siatki jest pożądane. Większość organizacji odniosła niewielki sukces w zachęcaniu użytkowników do tworzenia kopii zapasowych swoich komputerów. Tworzenie kopii zapasowych w sieci mesh może sprawić, że tworzenie kopii zapasowych na komputerze klienckim będzie automatyczne i wyeliminować błędy użytkowników podczas regularnego tworzenia kopii zapasowych.

TEST

a. Jakie są zalety scentralizowanej kopii zapasowej w porównaniu z kopią lokalną?

b. Zdefiniuj CDP.

c. Dlaczego CDP jest atrakcyjny?

d. Dlaczego to jest drogie?

e. Dlaczego tworzenie kopii zapasowych przez Internet u dostawcy przechowywania kopii zapasowych jest atrakcyjne dla użytkowników komputerów klienckich?

f. Jakie zagrożenie bezpieczeństwa stwarza?

g. Co to jest kopia zapasowa siatki?

h. Jakie są jego wyzwania techniczne?

i. Dlaczego kopia zapasowa siatki jest pożądana?

NOŚNIKI ZAPASOWE I RAID

Dane z kopii zapasowej muszą być na czymś fizycznie przechowywane. Fizyczne opcje przechowywania są nazywane nośnikami kopii zapasowych.

TAŚMA MAGNETYCZNA

Tradycyjnym nośnikiem kopii zapasowych była taśma magnetyczna. (Jeśli widziałeś starą kasetę muzyczną lub VHS, masz pojęcie, jak wygląda taśma magnetyczna.) Taśma magnetyczna może przechowywać ogromne ilości danych przy najniższym koszcie na bit wszystkich nośników kopii zapasowych. Jednak nagrywanie i odczytywanie na taśmie magnetycznej jest niesamowicie powolne. To oznacza, że kopie zapasowe na taśmach są zwykle wykonywane w nocy. Chociaż szybkość tworzenia kopii zapasowych na taśmach stale się poprawia, za każdym razem zwiększa się również ilość informacji, które są zapisywane. Biorąc pod uwagę potrzebę szybszego tworzenia kopii zapasowych, popularne staje się przechowywanie kopii zapasowych na innych dyskach twardych. Skraca to czas tworzenia kopii zapasowych, ale dyski twarde są zbyt drogie na dłuższą metę w składowaniu. W

związku z tym wiele firm stosuje dwuwarstwowe tworzenie kopii zapasowych, przechowując informacje na dysku tak długo, jak to możliwe, a następnie archiwizując (przechowując kopie zapasowe danych przez dłuższy czas) na taśmie.

KOPIA ZAPASOWA NA KOMPUTERZE KLIENTA

Użytkownicy komputerów klienckich zazwyczaj zapisują kopie zapasowe na dyskach DVD. Główną zaletą używania dysków optycznych do przechowywania jest to, że prawie wszystkie komputery PC mają nagrywarki dysków optycznych. Jednak nawet w przypadku dwuwarstwowych (lub dwuwarstwowych) dysków DVD, które przechowują około 8 GB danych, wielu użytkowników potrzebuje wielu dysków do jednej kopii zapasowej. Wielu użytkowników komputerów PC używa teraz drugiego dysku twardego w swoich systemach do tworzenia kopii zapasowych. Jest to znacznie szybsze niż tworzenie kopii zapasowych na dysku optycznym, ale dyski twarde, jak już wspomniano, nie nadają się do długoterminowego przechowywania archiwalnego. Ponadto, jeśli komputer zostanie skradziony lub zgubiony w pożarze, oba dyski zostaną utracone. W związku z tym nawet użytkownicy, którzy wykonują kopie zapasowe na drugim dysku twardym, muszą wykonywać okresowe kopie zapasowe na dyskach DVD. Jak długo trwają płyty CD i DVD, zanim ich dane zaczną się pogarszać? W przypadku krótkotrwałego użytkowania wydają się być w porządku, ale niektóre badania sugerują, że nawet przechowywanie dłużej niż dwa lata może być problematyczne.

TEST

a. Dlaczego taśma magnetyczna jest pożądana jako nośnik kopii zapasowej?

b. Dlaczego taśma nie jest pożądana?

c. Dlaczego tworzenie kopii zapasowych na innym dysku twardym jest atrakcyjne?

d. Dlaczego nie jest to kompletne rozwiązanie do tworzenia kopii zapasowych?

e. Jak można rozwiązać to ograniczenie?

f. Ile danych można zapisać na dwuwarstwowej płycie DVD?

g. Jaka jest zaleta nagrywania danych kopii zapasowych na dyskach optycznych?

h. Czy przechowywanie kopii zapasowych na dyskach optycznych przez kilka lat będzie bezpieczne?

Macierze dyskowe-RAID

Powszechną metodą zwiększania zarówno niezawodności, jak i szybkości tworzenia kopii zapasowych jest skonfigurowanie wielu dysków twardych jako tablicy w ramach jednego systemu (tj. serwera). Zapisywanie danych na tablicy dysków twardych lub macierzy dyskowej ma kilka zalet w porównaniu z zapisem danych na pojedynczym dysku.

W systemie z jednym dyskiem twardym awaria dysku może prowadzić do katastrofalnej utraty danych. Brak niezawodnego nośnika kopii zapasowej sprzętu może spowodować trwałą niedostępność danych. Jednak system wykorzystujący macierz dysków zwiększa niezawodność, ponieważ nadmiarowe dane są przechowywane na wielu dyskach. Awaria pojedynczego dysku w macierzy nie przyspieszyłaby utraty danych. Szereg dysków może również zwiększyć wydajność odczytu i zapisu. Wydajność dysku jest zwiększona, ponieważ dane mogą być zapisywane lub odczytywane z wielu dysków jednocześnie. Ten wzrost wydajności dysków oznacza, że macierze dyskowe są powszechne w korporacyjnych środowiskach obliczeniowych, które wymagają niemal natychmiastowego dostępu. Pomimo

dodatkowych kosztów macierze dyskowe pomagają efektywnie i niezawodnie zarządzać ogromnymi ilościami danych.

Poziomy najazdów

Macierze dyskowe można konfigurować na różne sposoby w zależności od konkretnych potrzeb w zakresie wydajności i niezawodności. Te różne konfiguracje wielodyskowe są znane jako poziomy RAID (nadmiarowa tablica niezależnych dysków). W tej sekcji przyjrzymy się trzem bardziej powszechnym poziomom RAID.

BEZ RAID

Większość komputerów użytkowników końcowych ma jeden dysk twardy. Jeśli nie pracowałeś w korporacyjnym środowisku komputerowym, prawdopodobnie nie skonfigurowałeś macierzy RAID. Zrozumienie konfiguracji RAID może być mylące, jeśli czytasz o nich po raz pierwszy. Pomocna jest analogia porównująca poziomy RAID do czegoś bardziej znanego. W tym przypadku posłużymy się analogią do wysyłki. W systemie z jednym napędem, dane są wysyłane z działającego hosta systemu na dysk twardy .Duże pliki można podzielić na „części", które są przechowywane w różnych lokalizacjach na dysku. Prędkości dostępu do dysków są wolniejsze w porównaniu z innymi poziomami RAID, ale koszty są niskie. Główną wadą systemu z jednym dyskiem jest to, że nie można go odzyskać po awarii dysku bez dodatkowej kopii zapasowej. Podobnie, posługując się analogią do wysyłki, pudełka (części) mogą być wysyłane do magazynu (dysk twardy) ze sklepu (system operacyjny). Posiadanie jednego magazynu jest niedrogie, ale jeśli spłonie, stracisz cały swój towar. Wysyłka między sklepem a magazynem jest powolna, ponieważ każde pudełko musi być wysyłane pojedynczo.

RAID 0

Szybkość wysyłania pudełek do i z magazynu może znacznie wzrosnąć, jeśli wykorzystanych zostanie więcej magazynów. Większa liczba pudełek może być wysyłana jednocześnie do trzech różnych magazynów. Zakup dodatkowych magazynów jest kosztowny, ale sklep detaliczny może lepiej reagować na wymagania klientów. Podobnie konfiguracja RAID 0 zwiększa szybkość transferu danych i pojemność, zapisując jednocześnie na wielu dyskach twardych. Zapisywanie danych na wielu dyskach nazywa się stripingiem. Zestaw dysków w paski jest szybki, ale nie zapewnia niezawodności. Jeśli jeden z dysków ulegnie awarii, dane na wszystkich dyskach zostaną utracone. Dane na innych dyskach są tracone, ponieważ części rozrzucone na dyskach stanowią połączony zestaw. Utrata 1/3 aplikacji czyni ją bezużyteczną. W przykładzie z wysyłką utrata jednego pudełka z zestawu trzech pudełek prawdopodobnie sprawiłaby, że produkt byłby bezwartościowy.

RAID 1

Istnieje możliwość wykorzystania dodatkowego magazynu, aby uzyskać niezawodne składowanie. Dodanie magazynu zapasowego do magazynu podstawowego zapewnia niezawodność. Jeśli magazyn podstawowy spłonie, z magazynu zapasowego można pobrać zduplikowane zapasy. Minusem jest to, że zakup magazynu zapasowego jest bardzo kosztowny. To samo dotyczy kopii zapasowych dysków twardych. Dysk kopii zapasowej 1 zawiera dokładną kopię wszystkich plików na Dysku 1. W konfiguracji RAID 1 system operacyjny klienta zapisuje dane jednocześnie na podstawowym dysku twardym i zapasowym dysku twardym. Nie stosuje się pasków, więc szybkość przesyłania danych pozostaje w przybliżeniu taka sama. Pojemność pamięci pozostaje taka sama, ponieważ dodatkowy dysk jest tylko lustrem dysku podstawowego. Jeśli podstawowy dysk twardy ulegnie awarii, można go wyjąć i zastąpić dyskiem zapasowym. Utrata danych praktycznie nie występuje, a czas przestoju wymagany do odzyskania danych po awarii jest minimalny. Konfiguracja RAID 1 skraca docelowy czas odzyskiwania

firmy (RTO) lub czas potrzebny na odzyskanie sprawności po awarii i przywrócenie normalnych operacji. Dublowanie skraca również cel punktu odzyskiwania (RPO), czyli punkt w czasie przed katastrofą, do którego wszystkie wcześniejsze dane muszą być możliwe do odzyskania. Innymi słowy, wszystkie dane przed RPO będą możliwe do odzyskania, ale dane między RPO a katastrofą zostaną utracone. Na przykład, jeśli ostatnia kopia zapasowa była na tydzień przed awarią, to RPO wynosi jeden tydzień. Twoja akceptowalna utrata danych to jeden tydzień danych. Korporacje wymagają krótkich RPO i RTO. W niektórych systemach utrata danych o kilka minut rocznie to za dużo. Dublowanie skraca zarówno czas utraty danych, jak i czas odzyskiwania. Jednak tworzenie kopii lustrzanych dużych ilości danych może być bardzo kosztowne. To sprawia, że RAID 1 jest mniej atrakcyjny.

RAID 5

Typowym sposobem na uzyskanie zarówno niezawodności, jak i dużych prędkości przesyłania danych jest użycie konfiguracji RAID 5. W analogii z wysyłką dodawanych jest więcej magazynów, aby zwiększyć szybkość, z jaką paczki wchodzą i wychodzą z magazynów. Zwiększa to ogólną wydajność. Niezawodność wynika z przechowywania części zamiennych w jednym magazynie, które odpowiadają pudełkom w pozostałych magazynach. W nieuszkodzonych magazynach jest wystarczająco dużo części, aby odtworzyć inwentarz, jeśli jeden magazyn spłonie. Nie ma wystarczającej liczby części, aby zrekonstruować inwentarz, jeśli spłonie więcej niż jeden magazyn. Podobnie konfiguracja RAID 5 rozkłada dane na wielu dyskach, aby zwiększyć prędkość przesyłania danych. Niezawodność zapewniają bity parzystości, które umożliwiają rekonstrukcję danych przechowywanych na innych dyskach. Konfiguracja RAID 5 może zostać odzyskana po awarii jednego dysku, ale nie awarii wielu dysków.

TEST

a. W jaki sposób macierze dyskowe mogą zapewnić niezawodność i dostępność danych?

b. Wyjaśnij RAID 0.

c. Wyjaśnij RAID 1.

d. Wyjaśnij RAID 5.

Powrót do zdrowia.

Załóżmy, że w przykładzie z wysyłką wybuchł pożar w Magazynie 3. Pole 4, Pole 6 oraz Części 1 i 2 zostaną zniszczone. Dobrą wiadomością jest jednak to, że w pozostałych magazynach jest wystarczająco dużo zapasów, aby zrekonstruować zniszczone pudła. Zapasy z magazynu 1 (pudełko 1, pudełko 3 oraz części 5 i 6), wraz z zapasami z magazynu 2 (pudło 2, pudełko 5 oraz części 3 i 4) mogą być wykorzystane do odtworzenia utraconych skrzyń (pudełko 4, pudełko 6 oraz części 1 i 2). Żaden inwentarz nie zostanie utracony. To samo odzyskanie byłoby możliwe, gdyby dysk 3 został utracony. Dane z Dysku 1 (Część 1, Część 3 i Parzystość 5 i 6), razem z danymi z Dysku 2 (Część 2, Część 5 i Parzystość 3 i 4) mogą być użyte do ponownego obliczenia utraconych danych na Dysku 3 (Część 4, Część 6 oraz parzystość 1 i 2). Żadne dane nie zostaną utracone. Po wykonaniu wszystkich obliczeń dane na nowym Dysku 3 będą identyczne z danymi przed pożarem. Konfiguracja dysków RAID 5 zapewnia dużą szybkość przesyłania danych poprzez rozłożenie danych na wielu dyskach i zapewnia niezawodność poprzez dystrybucję bitów parzystości na wszystkich dyskach. Przechowywanie bitów parzystości powoduje utratę niewielkiej ilości pamięci, ale znacznie mniej niż byłoby, gdyby cała tablica była zdublowana.

TEST

a Jakie są zalety RAID 5 nad RAID 1?

b. Który poziom RAID omówiony w tym rozdziale ma największą szybkość odczytu i zapisu?

c. Czy RAID 5 jest odpowiedni dla użytkowników domowych? Dlaczego lub dlaczego nie?

ZASADY PRZECHOWYWANIA DANYCH

Najlepsza technologia jest bezwartościowa bez dobrego zarządzania, a zasady są niezbędne do dobrego zarządzania.

ZASADY TWORZENIA KOPII ZAPASOWYCH

Jak wszystko inne w bezpieczeństwie, dobre zarządzanie ma kluczowe znaczenie dla powodzenia tworzenia kopii zapasowych. Zarządzanie zaczyna się od zrozumienia obecnego systemu i przyszłych potrzeb. Następnie tworzy polityki dla różnych typów danych i różnych typów komputerów. Zasady powinny określać, jakie dane powinny być archiwizowane, jak często powinny być archiwizowane, jak często należy testować przywracanie i tak dalej.

POLITYKA RENOWACJI

Scenariusz koszmaru to porażka, próba przywrócenia, a następnie odkrycie, że restauracja nie zadziała. Zasady tworzenia kopii zapasowych powinny narzucać częste testy przywracania, a audyty powinny obejmować przywracanie próbek.

ZASADY LOKALIZACJI PRZECHOWYWANIA MEDIÓW

Zarządzanie kopiami zapasowymi wymaga pewnych wyrafinowanych zasad dotyczących lokalizacji przechowywania nośników. Pierwszy to miejsce przechowywania nośnika kopii zapasowej. Najważniejszą rzeczą jest wymaganie przeniesienia nośnika kopii zapasowej do innej lokalizacji. W ten sposób w przypadku kradzieży komputera, pożaru lub zalania w głównej lokalizacji, kopie zapasowe będą nadal bezpieczne. Przeniesienie nośnika kopii zapasowej poza witrynę zajmuje zwykle kilka godzin lub nawet dzień. Zasady powinny nakazywać przechowywanie nośników kopii zapasowych w ognioodpornym i wodoodpornym sejfie do czasu ich wysłania z witryny.

POLITYKI SZYFROWANIA

Gdy nośniki są przenoszone z lokalizacji ich tworzenia do lokalizacji ich przechowywania, utrata i kradzież mogą spowodować uwolnienie krytycznych danych. W związku z tym zasady powinny nakazywać szyfrowanie wszystkich nośników kopii zapasowych. Wydłuży to czas tworzenia kopii zapasowych, ale było wiele przypadków utraty danych kopii zapasowych, które wymagały od firm powiadamiania klientów i innych osób dotkniętych problemem, że poufne dane osobowe na ich temat mogą być dostępne dla złodziei tożsamości.

ZASADY KONTROLI DOSTĘPU

Inną zasadą przechowywania powinno być ograniczenie osób, które mogą uzyskać dostęp do nośników kopii zapasowych w pamięci. Dane na taśmie są zazwyczaj bardzo wrażliwe. Ponadto, jeśli nośnik kopii zapasowej zostanie skradziony, firma nie będzie miała ochrony przed utratą danych. Zdarzały się również przypadki, że administratorzy systemów kradli taśmy z kopiami zapasowymi, kasowali je, a następnie usuwali dane z oryginalnego dysku twardego. To uniemożliwia przywrócenie. W związku z tym każda kasa powinna wymagać pisemnej zgody kierownika osoby chcącej uzyskać dostęp do taśm. Uprawnienie to powinno określać konkretne media do pobrania oraz powód ich pobierania. Pobieranie jest rzadkie, więc kasa powinna być podejrzana. Oczywiście, jeśli oryginalny system ulegnie awarii,

szybkie odzyskanie jest niezbędne. Mimo to, biorąc pod uwagę niebezpieczeństwa związane z kasą, kontrola musi być utrzymana nawet w sytuacjach awaryjnych.

ZASADY PRZECHOWYWANIA

Dane kopii zapasowej nie będą przechowywane na zawsze. Firmy potrzebują silnych i jasnych zasad dotyczących czasu przechowywania danych. Decyzje dotyczące retencji nie mogą być podejmowane po prostu na podstawie ilości miejsca do przechowywania w firmie. Istnieje wiele wymagań biznesowych i prawnych dotyczących zatrzymywania niektórych rodzajów danych, dlatego jednostki biznesowe i dział prawny muszą aktywnie tworzyć zasady przechowywania.

AUDYT ZGODNOŚCI Z POLITYKĄ BACKUP

Oczywiście posiadanie polityki to jedno. Zapewnienie ich realizacji to kolejna rzecz. Powinny być przeprowadzane okresowe audyty zgodności, w tym śledzenie, co się stało z próbkami danych, które powinny zostać objęte kopią zapasową.

TEST

a. Co powinny określać zasady tworzenia kopii zapasowych?

b. Dlaczego potrzebne są testy przywracania?

c. Gdzie należy przechowywać nośniki kopii zapasowych na dłuższą metę?

d. Co należy zrobić z nośnikami kopii zapasowych, dopóki nie zostaną przeniesione?

e. Dlaczego szyfrowanie nośników kopii zapasowych ma kluczowe znaczenie?

f. Jakie trzy zagrożenia wymagają kontroli dostępu do materiałów zapasowych?

g. Jeśli osoba A chce sprawdzić nośniki kopii zapasowych, kto powinien to zatwierdzić?

h. Dlaczego pobieranie nośników kopii zapasowych jest podejrzane?

i. Dlaczego jednostki biznesowe i dział prawny powinny być zaangażowane w tworzenie polityk retencji?

j. Co powinny obejmować audyty kopii zapasowych?

Przechowywanie e-maili

Wiele serwerów pocztowych przechowuje wiadomości na swoich dyskach przez pewien czas, a następnie archiwizuje je na taśmie. Skoordynowane wykorzystanie pamięci masowej online i przechowywania kopii zapasowych wiadomości jest określane jako przechowywanie.

KORZYŚCI Z RETENCJI

Z drugiej strony retencja pozwala użytkownikom przeglądać starą pocztę w poszukiwaniu informacji. W plikach i archiwach poczty elektronicznej przechowywana jest duża część „pamięci organizacyjnej" korporacji oraz informacji roboczych poszczególnych pracowników. Chociaż większość pobieranych wiadomości to niedawne wiadomości, projekty korporacyjne mogą trwać długo, a niektóre operacje pobierania muszą sięgać miesięcy, a czasem nawet lat.

NIEBEZPIECZEŃSTWA PRZECHOWYWANIA

Z drugiej strony, prawnicy mogą wykorzystać proces legalizacji w procesach sądowych, aby wydobyć wiadomości, w których pracownik powiedział coś zawstydzającego lub nawet oczywiście nielegalnego. Na przykład w federalnym procesie antymonopolowym Microsoftu wiadomości e-mail od Billa Gatesa i innych starszych menedżerów odnalezione podczas procesu wykrywania były żywe i szkodliwe dla Microsoftu. W niektórych przypadkach odzyskanie wiadomości e-mail będzie bardzo trudne, co spowoduje zamienienie plików kopii zapasowej w „pamięć tylko do zapisu". Jednak sądy konsekwentnie orzekają, że jeśli takie archiwa istnieją, firmy, które otrzymały nakazy odkrywania, muszą używać własnych pieniędzy do tworzenia programów do sortowania archiwów.

PRZYPADKOWE PRZECHOWYWANIE

Niektóre firmy odpowiedziały na widmo odkryć, odmawiając w ogóle archiwizacji poczty e-mail lub przechowując pocztę tylko przez 30 dni lub przez inny krótki okres czasu. Kopie zapasowe serwerów pocztowych są jednak rutynowo tworzone przy użyciu taśmy magnetycznej, a informacje mogą pozostawać na tych taśmach przez długi czas. Oliver North, główna postać w aferze Iran Contras za rządów Reagana, usunął swoje wiadomości e-mail, ale prokuratura była w stanie znaleźć je na rutynowych taśmach zapasowych. Ponadto, nawet jeśli poczta zostanie usunięta z serwerów i taśm z kopiami zapasowymi, pracownicy mogą zachować wiadomości na swoich komputerach klienckich. Jeśli wykrywanie obejmuje wiadomości e-mail na komputerach klienckich, może to oznaczać zawstydzające informacje, które mogły zostać legalnie odrzucone, a to z pewnością będzie kosztowne.

PRZECHOWYWANIE WIADOMOŚCI E-MAIL OSÓB TRZECICH

Pracownicy mogą korzystać z zewnętrznego dostawcy poczty e-mail, takiego jak Gmail®, Hotmail® lub Yahoo! Mail® do komunikacji korporacyjnej bez uwzględniania konsekwencji. Zewnętrzni dostawcy poczty e-mail mogą przechowywać dane użytkownika przez czas nieokreślony. Kiedy użytkownik zakłada konto e-mail, często zgadza się, aby dostawca zachował kopie jego wiadomości e-mail nawet po usunięciu. Wszystkie te e-maile mogą zostać wykryte. Na przykład polityka prywatności Google stwierdza: „Ze względu na sposób, w jaki utrzymujemy niektóre usługi, po usunięciu przez Ciebie informacji pozostałe kopie mogą potrwać pewien czas, zanim zostaną usunięte z naszych aktywnych serwerów i mogą pozostać w naszych systemach kopii zapasowych". Nie jest jasne, jak długo informacje o użytkowniku pozostaną w systemach kopii zapasowych Google.

PRAWNE WYMOGI DOTYCZĄCE ARCHIWIZACJI

Ponadto w branży usług finansowych firmy są zobowiązane do archiwizowania swojej komunikacji, w tym poczty elektronicznej. W 2002 roku amerykańska Komisja Papierów Wartościowych i Giełd nałożyła grzywny na sześć firm świadczących usługi finansowe w łącznej wysokości 10 milionów dolarów za nieutrzymywanie dobrych archiwów poczty elektronicznej. Wiele agencji rządowych jest również zobowiązanych do przechowywania wiadomości e-mail jako dokumentów publicznych, chociaż komunikacja krótkotrwała zwykle jest zwolniona z tej zasady. W rzeczywistości wszystkie branże są prawnie zobowiązane do zachowania pewnych form komunikacji, czy to za pośrednictwem poczty elektronicznej, czy na papierze. W takich przypadkach usunięcie wiadomości nie uchroni firmy przed karą. Przykłady obejmują niedobrowolne zwolnienia, publiczne informacje o ofertach pracy oraz skargi dotyczące pewnych problemów medycznych, które mogą być spowodowane przez toksyczne chemikalia. Wymogi te wynikają z różnych przepisów, a przepisy te wymagają różnych okresów przechowywania dla różnych typów wiadomości e-mail. Niezachowanie wymaganej poczty e-mail może być bardzo kosztowne. W jednym ze spraw sądowych Sprint został ukarany grzywną w pozwie patentowym za nieutrzymywanie dobrej dokumentacji e-mailowej dotyczącej patentu. Sądy mogą nawet wydać wyrok uproszczony w procesie cywilnym, jeśli pozwany nie zachował poczty elektronicznej.

FEDERALNE REGUŁY POSTĘPOWANIA CYWILNEGO STANÓW ZJEDNOCZONYCH

W federalnym systemie sądowym Stanów Zjednoczonych Federalne Zasady Postępowania Cywilnego określają procesy, które mają zastosowanie do prawników i sędziów w sprawach cywilnych. Najnowsza wersja, która weszła w życie w 2006 r., miała kilka implikacji dla obsługi informacji przechowywanych elektronicznie, w tym zarówno tradycyjnych baz danych, jak i nowszych form informacji, takich jak poczta elektroniczna i komunikatory. Jedna z najważniejszych zmian w regulaminie dotyczy wstępnych spotkań wyjaśniających pomiędzy powodem a pozwanym. Podczas tych spotkań pozwany musi być w stanie określić, jakie informacje są dostępne w ramach procesu prawnego ujawnienia. Te wstępne spotkania muszą odbyć się wkrótce po rozpoczęciu procesu, tak aby po rozpoczęciu procesu było już za późno na rozpoczęcie przygotowań do procesu. Firmy muszą jasno zrozumieć wszystkie swoje możliwe do znalezienia informacje i muszą mieć jasne plany dotyczące sposobów dostarczania informacji, jeśli to konieczne.

Jedna zasada wymaga od firm podjęcia kilku działań, jeśli proces sądowy się rozpoczął lub nawet jeśli można przewidzieć, że proces sądowy wkrótce się rozpocznie. Najważniejszym działaniem jest wstrzymanie wszelkiego niszczenia potencjalnie istotnych informacji. Jeśli firma nie posiada kompleksowych zasad i procedur dotyczących blokowania wszystkich informacji przechowywanych elektronicznie, naruszy tę zasadę.

UWIERZYTELNIANIE WIADOMOŚCI

Żenująco łatwo jest sfabrykować wiadomość tak, aby wyglądała, jakby pochodziła od kogoś innego. Poczta elektroniczna w sieci miała mniej niż cztery lata, gdy ktoś wysłał pierwszą sfałszowaną wiadomość przez ARPANET. Ta wiadomość, twierdząca, że pochodzi od urzędnika DARPA, zapowiadała niepopularną politykę. Był szeroko transmitowany do użytkowników ARPANET. Fałszywe wiadomości mogą być wykorzystywane do wrabiania innych pracowników i samej firmy, więc dobry system archiwizacji – i rzeczywiście każdy dobry system poczty e-mail – musi mieć wbudowane zabezpieczenia uwierzytelniania.

ROZWÓJ POLITYKI I PROCESÓW

Ogólnie rzecz biorąc, korporacje muszą opracować zasady i procesy archiwizacji dotyczące archiwizacji wiadomości e-mail, a plany te muszą odzwierciedlać ich środowisko prawne. Przy tworzeniu takich archiwów ważna jest współpraca z działem prawnym firmy.

TEST

a. Dlaczego przechowywanie poczty e-mail przez długi czas jest przydatne?

b. Dlaczego jest to niebezpieczne?

c. Czym jest odkrycie prawne?

d. Co może się stać, jeśli firma nie zachowa wymaganej poczty e-mail?

e. Co to jest przypadkowe zatrzymanie?

f. Jak długo zewnętrzni dostawcy poczty e-mail mogą przechowywać wiadomości e-mail?

g. Czy istnieje konkretna ustawa, która określa, jakie informacje należy przechowywać do celów prawnych?

h. Jakie dwa wymagania w amerykańskich przepisach postępowania cywilnego mogą spowodować problemy dla firm, które nie mają dobrego procesu archiwizacji?

i. Dlaczego uwierzytelnianie wiadomości jest ważne w systemie archiwizacji?

j. Skomentuj politykę firmy dotyczącą usuwania wszystkich wiadomości e-mail po 30 dniach.

Trening użytkownika

Chociaż technologia może pomóc firmom, kluczem do uniknięcia problemów w procesie wykrywania jest nauczenie użytkowników, czego nie należy umieszczać w wiadomościach e-mail. Użytkownicy mają tendencję do myślenia o wiadomościach e-mail jako osobistych. Jednak prawo nie postrzega ich w ten sposób. Odkrycie może je wydobyć, mogą zostać przypadkowo wysłane do niewłaściwej strony i mogą zostać przekazane niezamierzonym stronom. Ponadto pracodawcy mają generalnie prawo do sprawdzania wiadomości e-mail i ograniczania wiadomości do działalności firmy. Pracowników należy uczyć, aby nigdy nie umieszczali w wiadomościach niczego, czego nie chcieliby widzieć w sądzie, drukować w gazetach lub czytać przez szefa.

Pracowników należy uczyć, aby nigdy nie umieszczali w wiadomościach niczego, czego nie chcieliby widzieć w sądzie, drukować w gazetach lub czytać przez szefa.

Użytkowników należy również nauczyć, aby nie przekazywać wiadomości, o ile nie są do tego specjalnie upoważnieni. Po przesłaniu wiadomości traci się całą kontrolę. Nawet lista oryginalnych odbiorców może być szkodliwa dla informacji.

TEST

a. Czy wiadomości e-mail wysyłane przez pracowników są prywatne?

b. Co należy przeszkolić pracowników, aby nie umieszczali w wiadomościach e-mail?

Arkusze kalkulacyjne

W przeszłości specjaliści ds. bezpieczeństwa IT (tak jak ogólnie informatycy) ignorowali arkusze kalkulacyjne. Jednak nie jest to już możliwa do utrzymania pozycja. Arkusze kalkulacyjne znajdują się w centrum uwagi wielu systemów zgodności, zwłaszcza ustawy Sarbanes-Oxley z 2002 r. i zasad 21 CFR Part 11 dla firm farmaceutycznych przeprowadzających testy produktów. Ogólnie rzecz biorąc, firmy są zaniepokojone błędami w arkuszach kalkulacyjnych, oszustwami w arkuszach kalkulacyjnych i tradycyjnymi atakami na bezpieczeństwo, których celem są informacje prywatne, informacje zastrzeżone i inne informacje w arkuszach kalkulacyjnych. Aby zmniejszyć zagrożenia związane z arkuszami kalkulacyjnymi, potrzebne są dwa zestawy kontroli. Pierwszym z nich jest obszerne testowanie zarówno wskaźników błędów, jak i nadużyć. Drugi to wykorzystanie serwerów skarbca arkuszy kalkulacyjnych. Rysunek 9-21 ilustruje zabezpieczenia oferowane przez serwery skarbca.

KONTROLA DOSTĘPU DO SERWERA

Serwer repozytorium zapewnia silną kontrolę dostępu, w tym uwierzytelnianie o odpowiedniej sile, autoryzacje i audyt (AAA). Uprawnienia wykraczają poza to, co dana osoba może zrobić z plikiem. Ograniczają również to, co użytkownik może zobaczyć w arkuszu kalkulacyjnym. Na przykład firma może odmówić użytkownikom wprowadzania danych dostępu do formuł, które stanowią rozległą własność intelektualną. Z kolei użytkownicy raportów mogą być ograniczeni do przeglądania raportów i nie mogą mieć dostępu do części logicznych lub wprowadzania danych w arkuszu kalkulacyjnym.

Może to być najłatwiejsze do zaimplementowania za pomocą interfejsu internetowego odczytywanego przez przeglądarkę. W ten sposób informacje, do których użytkownik nie powinien mieć dostępu, w ogóle nie są do niego wysyłane. Audyt rozpoczyna się od wyewidencjonowania/zameldowania, ale jest kontynuowany do poziomu zmian w poszczególnych komórkach. Pobrane arkusze kalkulacyjne są

dostarczane z modułem audytu do rejestrowania wszystkich zmian w komórkach. Później firma może wykorzystać te dzienniki zmian komórek w analizach kryminalistycznych. Powinny istnieć aktywne narzędzia do wykrywania, które wyszukują naruszenia zasad i umożliwiają administratorowi sprawne i efektywne odczytywanie plików dziennika.

INNE ZABEZPIECZENIA SERWERA

Serwer repozytorium zapewni również, że użytkownik będzie mógł pracować tylko z najnowszą wersją pliku. Serwer repozytorium bezpiecznie zarchiwizuje starsze wersje pliku, tak aby pasowały do zasad dowodowych. Oczywiście serwer skarbca będzie chronił kryptograficznie wszystkie transmisje między użytkownikiem komputera PC a serwerem skarbca na odpowiednim poziomie siły. I wreszcie, powinny istnieć silne narzędzia zarządzania, które pozwolą menedżerom określać polityki i automatycznie je wdrażać.

TEST

a. Dlaczego bezpieczeństwo arkusza kalkulacyjnego jest problemem bezpieczeństwa IT?

b. Jakie dwa zabezpieczenia należy zastosować do arkuszy kalkulacyjnych?

c. Krótko wymień funkcje serwera repozytorium.

d. Skomentuj autoryzacje serwera repozytorium.

e. Opisz audyt serwera repozytorium.

BEZPIECZEŃSTWO BAZY DANYCH

Na początku tego rozdziału zwróciliśmy uwagę na znaczenie bezpiecznego przechowywania, przesyłania i przetwarzania danych. Bazy danych to zintegrowane zbiory danych i metadanych, przechowywane na komputerach. W tej sekcji przyjrzymy się sposobom ochrony przed zagrożeniami, których celem są konkretnie bazy danych. Korporacyjne bazy danych wymagają zabezpieczeń oprócz tych omówionych we wcześniejszych rozdziałach. Zabezpieczenia omówione we wcześniejszych rozdziałach odgrywają kluczową rolę w ochronie podstawowych danych korporacyjnych. Wdrożone razem zapewniają głęboką obronę. Poniżej znajdują się przykłady z poprzednich rozdziałów, w jaki sposób stosowane są zabezpieczenia do ochrony danych:

• Ochrona danych musi być oparta na polityce. Wymagania prawne i standardy akredytacji (np. PCI-DSS, HIPAA, CobiT) często kształtują politykę w zależności od rodzaju przechowywanych danych.

• Dane przechowywane w bazie danych muszą być chronione kryptograficznie .

• Bezpieczne sieci muszą pomagać w kontroli dostępu do wewnętrznych serwerów baz danych .

• Fizyczny i elektroniczny dostęp do magazynów danych musi być kontrolowany.

• Prawidłowo skonfigurowana zapora powstrzyma ataki skoncentrowane na degradacji poufności, integralności i dostępności danych firmowych.

• Serwery obsługujące bazy danych muszą być wzmocnione, aby zapobiec nieautoryzowanemu dostępowi za pośrednictwem systemu operacyjnego. Obejmuje to łatanie, posiadanie silnych haseł, regularne skanowanie antywirusowe i tak dalej.

• Aplikacje uzyskujące dostęp do baz danych muszą być zabezpieczone. Niezabezpieczone aplikacje mogą służyć do wyodrębniania lub usuwania danych za pomocą wstrzykiwania SQL .

Przyjrzymy się teraz kilku unikalnym zabezpieczeniom, które można wdrożyć na poziomie bazy danych w celu ochrony danych.

Relacyjne bazy danych

Większość baz danych to bazy relacyjne. Przechowują swoje dane w relacjach, potocznie zwanych tabelami. Bazy danych mogą mieć dziesiątki relacji. Każda relacja przechowuje informacje o jednostce. Encje to typy obiektów, które reprezentują osoby, miejsca, rzeczy lub zdarzenia. Encje to rzeczy (rzeczowniki), o których chcesz przechowywać informacje. Przykłady podmiotów obejmują:

• Osoby - pracownicy, klienci, dostawcy, studenci i profesorowie.

• Miejsca-oddziały, lokalizacje, sklepy, miasta i stany.

• Inwentarz rzeczy, komputery, samochody, szkoły i sale lekcyjne.

• Wydarzenia-sprzedaż, zakupy, zamówienia, semestry i zajęcia.

Relacja Pracownik będzie zawierała dane o wszystkich pracownikach. Wiersz, czasami nazywany krotką lub rekordem, reprezentuje określone wystąpienie encji. W tym przykładzie wiersz reprezentuje konkretnego pracownika. Atrybuty, kolumny w tabeli, to cechy (przymiotniki) dotyczące encji, którą chcesz zebrać. W tym przykładzie atrybuty obejmują imię, nazwisko, dział i wynagrodzenie. Każda tabela będzie miała również klucz składający się z co najmniej jednego atrybutu, który jednoznacznie identyfikuje każdy wiersz. W tym przykładzie kolumna Employee_ID jest kluczem używanym do jednoznacznej identyfikacji każdego pracownika.

OGRANICZENIE WIDOKU DANYCH

Nie każdy pracownik powinien mieć dostęp do wszystkich informacji w bazie danych. Pracownicy powinni mieć dostęp tylko do tych danych, których potrzebują do wykonywania swojej pracy. Zasada najmniejszych uprawnień dotyczy zarówno dostępu do danych, jak i dostępu fizycznego. Ograniczenie dostępu pracowników do danych powinno być traktowane jako ochrona, a nie kara. Ograniczanie dostępu do tabel.Dostęp do całych tabel może być ograniczony. Na przykład księgowy w szpitalu nie musiałby widzieć tabel zawierających dokumentację medyczną pacjenta. Mimo że księgowy może być uczciwym i pracowitym pracownikiem, jego praca nie wymaga dostępu do tabel zawierających dokumentację medyczną pacjenta. I odwrotnie, lekarz medycyny nie potrzebowałby dostępu do tabel zawierających dane finansowe. Ograniczanie dostępu do kolumn. Dostęp do kolumn można ograniczyć, więc dostępne są tylko niektóre kolumny z tabel. Na przykład tylko kilku pracowników może mieć możliwość pobierania informacji z kolumny wynagrodzeń. Inni pracownicy mogli odczytać inne atrybuty w tabeli Employee, ale nie pensje. Należy zachować szczególną ostrożność, aby zablokować dostęp do kolumn zawierających dane wrażliwe, które mogą być wykorzystywane w bazach danych poza korporacją. Na przykład numery ubezpieczenia społecznego mogą służyć do identyfikacji osób w wewnętrznych i zewnętrznych bazach danych. W przypadku kradzieży konsekwencje mogą być poważne.

Ograniczanie dostępu do wierszy. Dostęp do rzędów można również ograniczyć. Na przykład dostęp do danych pracowników można ograniczyć do wierszy dla każdego działu. Każdy dział może przeglądać własne rekordy pracowników, ale nie rekordy innych działów.

Granularność. Ponadto, gdy baza danych jest używana do analizy trendów i innych funkcji, może być pożądane zmniejszenie szczegółowości (poziomu szczegółowości) zapytań. Na przykład podczas analizowania danych dotyczących personelu obawy dotyczące prywatności mogą ograniczać wyszukiwanie do nie bardziej szczegółowych niż sumy i średnie na poziomie departamentu.

Ograniczanie informacji strukturalnych. Informacje o ogólnej strukturze bazy danych muszą być starannie strzeżone. Nazwy jednostek, atrybuty i struktura relacji między jednostkami, znana jako model danych, muszą być traktowane jako poufne. Wiedza o istnieniu tabeli i towarzyszących jej nazw atrybutów może umożliwić osobie atakującej wyodrębnienie wszystkich danych za pomocą wstrzyknięcia SQL. Nie znając struktury bazy danych, napastnicy zmuszeni są próbować mapować bazę danych metodą prób i błędów. Różne komunikaty o błędach umożliwiają atakującemu pośrednie mapowanie bazy danych. Jednak wielokrotne „zgadywanie" struktury bazy danych powoduje powstanie dużej liczby wpisów w dziennikach błędów bazy danych. Zaalarmowałoby to administratora bazy danych o ataku. Dostosowane ogólne komunikaty o błędach mogą być wykorzystywane do zapobiegania wyciekom informacji strukturalnych za pośrednictwem komunikatów o błędach.

TEST

a. Co to jest relacyjna baza danych? Wyjaśniać.

b. Dlaczego administrator bazy danych miałby ograniczać dostęp do niektórych tabel?

c. Dlaczego administrator bazy danych miałby chcieć ograniczyć dostęp do niektórych kolumn?

d. Dlaczego administrator bazy danych miałby chcieć ograniczyć dostęp do niektórych wierszy?

e. W jaki sposób ograniczenie granulacji danych chroniłoby bazową bazę danych?

f. Co to jest model danych?

Kontrola dostępu do bazy danych

Dostęp do sieci, hostów i aplikacji może być ograniczony do uwierzytelnionych i autoryzowanych użytkowników. Podobnie dostęp do baz danych musi być ograniczony. Użytkownicy, grupy i procesy mogą uzyskać dostęp do bazy danych po ich uwierzytelnieniu. Popularne systemy zarządzania bazami danych (DBMS), takie jak Microsoft SQL Server, MySQL, IBM DB2 i Oracle, mogą zarządzać strukturami baz danych i ograniczać dostęp do poszczególnych baz danych. Użytkownicy mogą być uwierzytelniani lokalnie na serwerze bazy danych lub za pośrednictwem centralnych serwerów uwierzytelniania, takich jak Kerberos lub Microsoft Active Directory. Rysunek 9-25 przedstawia opcje uwierzytelniania i polityki haseł dostępne podczas tworzenia nowego loginu dla Microsoft SQL Server. Niezależnie od tego, czy używasz lokalnego uwierzytelniania SQL Server, czy centralnego uwierzytelniania systemu Windows, ważne jest, aby wymusić złożoność hasła i wymagania dotyczące historii.

KONTA BAZ DANYCH

Te same zasady zalecane przy zarządzaniu kontami serwerów dotyczą zarządzania kontami bazy danych. Konto administratora bazy danych powinno zostać zmienione i zabezpieczone szczególnie silnym hasłem. Konta gości i publiczne powinny być wyłączone, ponieważ nie zapewniają indywidualnej odpowiedzialności. Są również głównymi celami atakujących. Usługom uzyskującym dostęp do bazy danych należy nadać możliwie najniższe niezbędne uprawnienia. Ograniczy to szkody, które mogą wystąpić w przypadku zhakowanej usługi.

ATAKI WTRYSKU SQL

Przyjrzeliśmy się, jak źle zakodowane aplikacje mogą umożliwiać przekazywanie nieoczekiwanych danych w ramach ataku typu SQL injection. Korzystając z wstrzyknięcia SQL, osoby atakujące mogą wyodrębnić dane, usunąć dane, ominąć uwierzytelnianie lub zamknąć bazy danych. W bazach danych można również zaimplementować zabezpieczenia, aby powstrzymać ataki typu SQL injection. Deweloperzy baz danych mogą sprawdzać przychodzące dane i zapytania, upewniając się, że mają one

oczekiwany typ danych (np. tekst, liczba całkowita lub binarna), rozmiar (np. 32 bity, 10 znaków lub mniej niż 5 KB) lub format (np. DD/MM/RR lub (555)555-5555). Przychodzące dane można również oczyścić w celu usunięcia niedopuszczalnych znaków, które mogłyby zostać użyte do manipulowania instrukcją SQL. Procedury składowane. Administratorzy baz danych mogą używać istniejących podprogramów, zwanych procedurami składowanymi, do oczyszczania i sprawdzania poprawności przychodzących danych. Procedury składowane mogą służyć do zapobiegania niektórym atakom typu SQL Injection, ale nie mogą one zapobiegać wszystkim atakom typu SQL Injection.

TEST

a. Co to jest DBMS?

b. Czy DBMS może zarządzać wieloma bazami danych? Czemu?

c. W jaki sposób walidacja może chronić przed atakiem typu SQL injection?

d. W jaki sposób warunki sanitarne mogą chronić przed atakiem typu SQL injection?

Audyt bazy danych

Ważną częścią zarządzania bezpieczną bazą danych jest audyt. Administratorzy baz danych używają inspekcji do zbierania informacji o interakcjach użytkowników z bazami danych. Inspekcja zapewnia administratorom środki wykrywania niezgodności z ustalonymi zasadami bezpieczeństwa. Audyt musi być procesem opartym na polityce, który odzwierciedla zobowiązania prawne i regulacyjne firmy.

CO DO AUDYTU

Podejmowanie decyzji o tym, co należy poddać audytowi, będzie się znacznie różnić w zależności od rodzaju danych, ilości danych i wymogów prawnych. Nawet wielkość i struktura organizacji wpłynie na wymagania dotyczące audytu. Poniżej przedstawiono tylko kilka typowych zdarzeń bazy danych, które są regularnie kontrolowane.

Logowania. Pomyślne i nieudane logowania muszą być rejestrowane. Informacje kontrolne obejmowałyby, kto zażądał dostępu, jego lokalizację (adres IP), datę i godzinę żądania dostępu oraz wykonane polecenia. Administratorzy powinni zwrócić uwagę na powtarzające się nieudane logowania, dostęp w dziwnych godzinach, dostęp z nieznanych zdalnych adresów IP oraz dostęp użytkowników, którzy przypuszczalnie są na wakacjach lub zostali niedawno zwolnieni.

Zmiany. Należy monitorować zmiany w procedurach składowanych, funkcjach, wyzwalaczach (omówionych poniżej), strukturze bazy danych, kontach i uprawnieniach użytkowników, harmonogramach tworzenia kopii zapasowych oraz zabezpieczeniach kryptograficznych. Administratorzy muszą być świadomi szkód, jakie niezadowolony pracownik może wyrządzić bazie danych w krótkim czasie. Pozornie drobne zmiany mogą spowodować rozległe szkody. Ostrzeżenia. Wszystkie ostrzeżenia muszą być rejestrowane. Ostrzeżenia mogą służyć jako wskaźniki, że organizacja jest atakowana. Na przykład ostrzeżenia o błędnie sformułowanych instrukcjach SQL przesyłanych do bazy danych mogą ostrzec administratora bazy danych o możliwym ataku typu SQL injection.

Wyjątki. Dzienniki kontroli mogą szybko rosnąć i stać się nieporęczne. Często są zaśmiecone wpisami z legalnych wydarzeń. Uzasadnione zdarzenia mogą powodować zbyt duży „szum” w dziennikach kontrolnych. Z punktu widzenia bezpieczeństwa interesują nas przede wszystkim naruszenia polityki bezpieczeństwa. Wyjątki mogą zmniejszyć ilość szumu w dziennikach inspekcji poprzez usunięcie uzasadnionych zdarzeń. Jednak wyjątki od zasad audytu muszą być uzasadnione i starannie rejestrowane.

Dostęp specjalny. Wreszcie korporacja może mieć pewne dane, które są tak wrażliwe, że wymagają wpisów w dzienniku przy każdym dostępie. Dane te mogą obejmować własność intelektualną, nowe plany projektów badawczo-rozwojowych, dokumentację medyczną lub klucze kryptograficzne.

WYZWALACZE

Czasami zmiany wprowadzone w bazie danych wymagają natychmiastowej odpowiedzi. Wyzwalacze to fragmenty kodu SQL, które są automatycznie uruchamiane po wprowadzeniu zmian w bazie danych. Firmy często używają wyzwalaczy do automatyzacji procesów biznesowych.

Przykład wykorzystania wyzwalaczy do automatyzacji procesu biznesowego można zobaczyć w zakupach online. Po sfinalizowaniu zakupu można użyć wyzwalacza, aby automatycznie wysłać klientowi potwierdzenie zamówienia e-mailem. Wyzwalacze mogą być również używane do wdrażania zasad audytu i wykrywania niezgodności z zasadami bezpieczeństwa.

Wyzwalacze języka definicji danych (DDL) mogą być używane do generowania automatycznych odpowiedzi, jeśli struktura bazy danych została zmieniona. Na przykład wyzwalacze DDL mogą być używane do powiadamiania administratora bazy danych, jeśli użytkownik lub osoba atakująca próbuje utworzyć nowe tabele, usunąć istniejące tabele lub zmienić właściwości istniejącej tabeli.

Wyzwalacze języka manipulacji danymi (DML) mogą być używane do generowania automatycznych odpowiedzi w przypadku zmiany danych. Na przykład wyzwalacz DML może służyć do powiadamiania administratora bazy danych o wstawieniu, zaktualizowaniu lub usunięciu określonych danych.

TEST

a. Jakie typy zdarzeń w bazie danych powinny być kontrolowane?

b. Jak można wykorzystać wyzwalacze SQL do zabezpieczenia bazy danych?

c. Co to jest wyzwalacz DDL?

d. Co to jest wyzwalacz DML?

e. Jaki rodzaj danych wrażliwych istnieje w Twojej organizacji?

Umiejscowienie i konfiguracja bazy danych

Bezpieczeństwo bazy danych można poprawić, wprowadzając zmiany architektoniczne w lokalizacji fizycznej bazy danych. Architektura trójwarstwowa oddziela funkcje prezentacji (serwer WWW), przetwarzania aplikacji (serwer oprogramowania pośredniczącego) i zarządzania bazą danych (serwer bazy danych). Architektura warstwowa zapewnia wyższy poziom ochrony bazy danych, ponieważ luki w zabezpieczeniach lub ataki na jedną warstwę niekoniecznie wpływają na inne warstwy. Na przykład atak DoS na serwer WWW nie przeciąży serwera bazy danych i nie zamknie bazy danych. Podobnie luka w aplikacji na serwerze oprogramowania pośredniczącego niekoniecznie naruszy bazę danych. W architekturze wielowarstwowej serwer bazy danych powinien być skonfigurowany do akceptowania tylko bezpiecznych połączeń z oprogramowania pośredniego lub serwera WWW. Połączenia z innych zewnętrznych lub wewnętrznych hostów powinny być blokowane.

ZMIEŃ PORT DOMYŚLNY

Prostym, ale skutecznym sposobem na zniechęcenie atakujących do dostępu do bazy danych jest zmiana domyślnego portu nasłuchiwania. Atakujący używają automatycznych skanerów portów do wyszukiwania baz danych działających na znanych portach domyślnych. Domyślny port dla Microsoft SQL Server to 1433, a domyślny port dla MySQL to 3306. Zmiana domyślnego portu nie zatrzyma

całkowicie atakujących, ale utrudni im rozpoznanie usługi bazy danych. Jeśli zmienisz domyślny port nasłuchiwania, ważne jest, aby pamiętać o dostosowaniu reguł zapory.

TEST

a. Czym jest architektura wielopoziomowa? Dlaczego to jest ważne?

b. Jak wielowarstwowa architektura może zatrzymać lub złagodzić skutki ataku?

c. Dlaczego zmiana domyślnego portu nasłuchiwania bazy danych jest ważna?

Szyfrowanie danych

W Części 3 zobaczyliśmy, że szyfrowanie zapewniające poufność sprawia, że informacje są nieczytelne dla atakujących, ale mogą być odczytane przez upoważnione osoby, które posiadają klucz, którego należy użyć do ich odszyfrowania. Szyfrowanie zyskuje na znaczeniu. Ujawnienie poufnych tajemnic handlowych lub prywatnych informacji może spowodować ogromne szkody. Brak szyfrowania poufnych danych jest dziś prawie nie do usprawiedliwienia. Z drugiej strony szyfrowanie danych może uniknąć koszmaru PR, jeśli zaszyfrowane dane zostaną zgubione lub skradzione. Prawa, które rządzą zgłoszeniem zagubionych lub skradzionych poufnych informacji często nie wymaga powiadomienia, ponieważ znalazca lub złodziej prawdopodobnie nie może odczytać zaszyfrowanych danych.

KLUCZ ESCROW

Jeśli zapomnisz hasła, jest to zwykła niedogodność. Personel pomocy technicznej po prostu resetuje hasło i podaje je do resetowania. Utrata klucza w szyfrowaniu jest znacznie poważniejsza. Jeśli szyfrowanie odbywa się w taki sposób, że atakujący nie mogą uzyskać informacji bez klucza, osoby o uzasadnionych potrzebach dostępu również zostaną zablokowane w przypadku zgubienia klucza. Jeśli szyfrowanie jest wykonane dobrze, to odpowiedź na pytanie „Jak mogę znaleźć mój klucz?" będzie „Nie możesz". Jeśli uda ci się odzyskać klucz, napastnik też. W rzeczywistości niektóre organizacje w większości przypadków zabraniają szyfrowania, obawiając się, że ryzyko utraty klucza jest znacznie poważniejsze niż ryzyko odczytania przez atakujących niezaszyfrowanych informacji. mogą być przechowywane poza komputerem. Jeśli wystąpi problem, zdeponowany klucz można odzyskać i użyć do odszyfrowania informacji. Deponowany klucz powinien być bezpiecznie zamknięty, a dostęp do klucza powinien być ograniczony. Depozyt kluczy nigdy nie powinien być pozostawiony indywidualnym użytkownikom. Po pierwsze, indywidualni użytkownicy prawdopodobnie nie będą przestrzegać kluczowych zasad dotyczących depozytów. Po drugie, jeśli tylko poszczególni użytkownicy znają swoje klucze szyfrowania, mogą szantażować firmę, odmawiając odszyfrowania krytycznych danych. Lepsze jest wykorzystanie automatycznego centralnego serwera depozytowego kluczy do zarządzania kluczami szyfrowania. W większym środowisku korporacyjnym może być konieczne zakupienie oddzielnego urządzenia sprzętowego zwanego sprzętowym modułem zabezpieczeń (HSM), które może tworzyć i przechowywać klucze kryptograficzne. Mogą mieć postać dysku USB, wewnętrznej karty PCI, a nawet urządzenia sieciowego. Oprócz zarządzania kluczami moduły HSM mogą zapewniać dodatkowe funkcje, takie jak szyfrowanie, odszyfrowywanie, mieszanie i tworzenie podpisów cyfrowych. Są one często używane w celu zmniejszenia obciążenia przetwarzania w firmach korzystających z wielu równoczesnych połączeń SSL, takich jak banki lub podmioty przetwarzające karty kredytowe. Urzędy certyfikacji używają również modułów HSM do bezpiecznego zarządzania parami kluczy kryptograficznych.

SZYFROWANIE PLIKU/KATALOGU A SZYFROWANIE CAŁEGO DYSKU

Podczas szyfrowania informacji na dysku istnieją dwie ogólne opcje — szyfrowanie plików/katalogów i szyfrowanie całego dysku. Nazwy nie wymagają wyjaśnień. Szyfrowanie plików/katalogów szyfruje tylko określone pliki i katalogi, które każesz zaszyfrować, podczas gdy szyfrowanie całego dysku szyfruje cały dysk. Jeśli użytkownik zna katalogi zawierające poufne dane, może bez obaw korzystać z szyfrowania plików/katalogów. Jednak szyfrowanie całego dysku zapewnia ochronę poufnych danych, nawet jeśli użytkownik przeoczy ważny katalog.

ZABEZPIECZENIE DOSTĘPU DO KOMPUTERA

Szyfrowanie jest zwykle w pełni niewidoczne dla użytkownika komputera. Dopóki znasz hasło do swojego komputera, możesz pracować z zaszyfrowanymi katalogami i plikami dokładnie tak samo, jak z niezaszyfrowanymi katalogami i plikami. W rzeczywistości zwykle nawet nie wiesz, czy informacje są zaszyfrowane. Oczywiście każdy, kto zna hasło do Twojego komputera, ma tak samo łatwy dostęp. W związku z tym szyfrowanie zwykle jest tak silne, jak hasło logowania, a praktyki dotyczące hasła logowania są zwykle kiepskie.

TRUDNOŚCI W UDOSTĘPNIANIA PLIKÓW

Chociaż szyfrowanie jest bardzo pożądane, utrudnia udostępnianie. Pliki zwykle muszą zostać odszyfrowane, jeśli zostaną przeniesione na inny komputer. Korzystanie z oprogramowania szyfrującego innej firmy (takiego jak AxCrypt lub TrueCrypt) do szyfrowania plików jest bardziej pracochłonne, ale znacznie ułatwia wysyłanie i udostępnianie zaszyfrowanych plików.

TEST

a. Dlaczego szyfrowanie danych wrażliwych jest zazwyczaj atrakcyjne z prawnego punktu widzenia?

b. Jak długo musi być dzisiaj klucz szyfrowania, aby był uważany za silny?

c. Co się stanie, jeśli klucz szyfrowania zostanie zgubiony?

d. Jak firmy radzą sobie z tym ryzykiem?

e. Dlaczego powierzanie użytkownikom depozytu kluczy jest ryzykowne?

f. W jakim sensie szyfrowanie jest zwykle niewidoczne dla użytkownika?

g. Dlaczego to jest atrakcyjne?

h. Dlaczego to niebezpieczne?

i. Co muszą zrobić użytkownicy, aby zaradzić temu niebezpieczeństwu?

j. W jaki sposób szyfrowanie utrudnia udostępnianie plików?

ZAPOBIEGANIE UTRACIE DANYCH

Utrata danych jest zarówno szkodliwa, jak i krępująca. W przypadku korporacji utrata danych może prowadzić do procesów sądowych, zmniejszenia bazy klientów, utraty własności intelektualnej i bezpośredniej utraty przychodów. Z tych powodów korporacje niechętnie przyznają, że utraciły dane. Często bagatelizują znaczenie danych lub po prostu zaprzeczają, że zostały utracone. Utrata danych może być zamierzona (kradzież) lub niezamierzona (nieostrożność). Zarówno pracownicy wewnętrzni, jak i zewnętrzni atakujący mogą ujawnić poufne dane. Zapobieganie utracie danych (DLP) to zestaw zasad, procedur i systemów zaprojektowanych w celu zapobiegania udostępnieniu poufnych danych osobom nieupoważnionym. Planowanie dla DLP odbywa się w ramach ogólnego procesu planowania strategicznego firmy.

Zbieranie danych

Większość korporacji gromadzi więcej danych, niż jest w stanie odpowiednio chronić. Osoby zarządzające i marketingowe są zainteresowane zebraniem jak największej ilości danych. Wierzą, że pomoże im to podejmować lepsze decyzje. Czasami tak. Jednak gromadzenie pewnych rodzajów danych lub zbyt dużej ilości danych może w rzeczywistości zaszkodzić korporacji. Na przykład dealer samochodowy może poprosić Cię o podanie numeru ubezpieczenia społecznego (SSN) podczas ubiegania się o pożyczkę samochodową. Używają Twojego numeru SSN, aby poprawnie zidentyfikować Twoją historię kredytową. Jest to rozsądne wykorzystanie numeru SSN. Powstaje zatem pytanie: Czy dealer samochodowy powinien przechowywać Twój numer SSN? Niezależnie od tego, czy dane są przechowywane w formie elektronicznej, czy na papierze, dealer samochodowy może zostać pociągnięty do odpowiedzialności w przypadku utraty danych. Czy przechowywane dane SSN przyniosą większe korzyści finansowe? A może utrata danych doprowadzi do zirytowania klientów, utraty reputacji i kosztownej bitwy prawnej? Menedżerowie muszą dokładnie rozważyć koszty i korzyści związane z gromadzeniem określonych rodzajów danych.

DANE OSOBOWE

Jednym z rodzajów danych, który zasługuje na szczególną uwagę, są informacje umożliwiające identyfikację osoby (PII). Może to obejmować prywatne informacje o pracownikach i prywatne informacje o klientach, które można wykorzystać do jednoznacznej identyfikacji osoby. W opiece zdrowotnej dane osobowe muszą być chronione prawem. Ogólnie rzecz biorąc, utrata PII może prowadzić do kradzieży karty kredytowej i kradzieży tożsamości. W rezultacie korporacje z „głębokimi kieszeniami" są celem procesów sądowych. Narodowy Instytut Standardów i Technologii (NIST) wymienia następujące dane jako PII

• Imię i nazwisko, takie jak imię i nazwisko, nazwisko panieńskie, nazwisko panieńskie matki lub pseudonim.

• Osobisty numer identyfikacyjny, taki jak numer ubezpieczenia społecznego (SSN), numer paszportu, numer prawa jazdy, numer identyfikacyjny podatnika lub numer rachunku finansowego lub karty kredytowej.

• Informacje adresowe, takie jak ulica lub adres e-mail.

• Cechy osobowe, w tym wizerunek fotograficzny (zwłaszcza twarzy lub innej cechy identyfikującej), odciski palców, pismo ręczne lub inne dane biometryczne (np. skan siatkówki, podpis głosowy lub geometria twarzy).

• Łączenie informacji, informacji o osobie, która jest powiązana lub powiązana z jednym z powyższych (np. data urodzenia, miejsce urodzenia, rasa, religia, waga, aktywność, wskaźniki geograficzne, informacje o zatrudnieniu, informacje medyczne, informacje o wykształceniu lub Informacje finansowe).

MASKOWANIE DANYCH

Jeśli to możliwe, lepiej w ogóle nie zbierać PII. Lepiej jest przypisywać klientom unikalne identyfikatory klienta, zamiast identyfikować ich za pomocą numeru SSN lub innych informacji umożliwiających identyfikację. Jeśli konieczne jest przechowywanie PII, istnieją alternatywne sposoby przechowywania PII. Maskowanie danych zaciemnia dane tak, że nie można zidentyfikować konkretnej osoby, ale pozostaje praktycznie przydatne.

TEST

a. Co to jest zapobieganie utracie danych (DLP)?

b. Czy istnieją rodzaje danych, których gromadzenie jest zbyt ryzykowne?

c. Czy Twoim zdaniem większość organizacji odpowiednio chroni swoje dane? Czemu?

d. Co to są informacje umożliwiające identyfikację osób? Proszę podać kilka przykładów PII.

e. Co to jest maskowanie danych?

Triangulacja informacji

Niektóre z wymienionych powyżej kategorii PII mogą wydawać się nieszkodliwe. Może być trudno zrozumieć, w jaki sposób znajomość kodu pocztowego klienta może być szkodliwa. Rysunek 9-29 pokazuje, w jaki sposób można połączyć dwa różne zbiory danych, aby zebrać więcej informacji o osobie. Profesor Latanya Sweeney z Carnegie Mellon University połączyła dane z publicznej listy wyborców z pozornie anonimowymi danymi medycznymi.16 Odkryła, że możliwe jest prawidłowe ponowne zidentyfikowanie 87 procent osób przy użyciu kodu pocztowego, daty urodzenia i płci. Innymi słowy, nazwisko osoby z publicznej listy wyborców może być powiązane z danymi medycznymi poprzez łączenie atrybutów. Łączenie dwóch części informacji, a następnie dokładne wywnioskowanie wartości trzeciej to prawdopodobnie coś, co robiłeś już wcześniej na zajęciach z geometrii. Rysunek 9-30 pokazuje, że trzeci kąt (X°) w trójkącie można wywnioskować z pozostałych dwóch kątów (60°), a także nazwy trójkąta. Podobnie dane z wielu źródeł można łączyć w celu identyfikacji osób w formie triangulacji informacji. Połączenie dwóch zgodnych „anonimowych" zbiorów danych można wykorzystać do stworzenia trzeciego zbioru danych, który jest niezgodny i prawdopodobnie niezgodny z prawem.

Nawet jeśli nie ma bezpośrednich atrybutów łączących między zbiorami danych, możliwe jest zastosowanie profilowania w celu identyfikacji osób. Profilowanie wykorzystuje metody statystyczne, algorytmy i matematykę w celu znalezienia wzorców w zbiorze danych, które jednoznacznie identyfikują daną osobę.

KUP LUB SPRZEDAJ DANE

Korporacje często kupują i sprzedają informacje o klientach. Dane o sprzedaży stanowią dodatkowe źródło dochodu, które może zwiększyć marże zysku. Kupowanie informacji może identyfikować nowe rynki, udoskonalać kampanie reklamowe, a nawet ulepszać istniejący produkt lub usługę informacyjną. Kupowanie informacji może również zmniejszyć rotację, identyfikując potencjalnych pracowników z historią kryminalną, nawykowymi problemami finansowymi i kiepską historią jazdy. Korporacja może zdecydować się na sprzedaż danych klientów. Zanim dane opuszczą firmę, należy podjąć szczególne środki ostrożności, aby zapewnić ich odpowiednie zniekształcenie i zamaskowanie. Sprzedawane dane muszą chronić prywatność klientów i strategiczną przewagę firmy. Najlepiej założyć, że sprzedawane dane mogą trafić w ręce konkurencji. Przepisy nadrabiają zaległości w zakresie ochrony indywidualnej prywatności. W 2011 roku Sąd Najwyższy stanu Kalifornia orzekł, że sprzedawcy detaliczni nie mogą zebrać kodu pocztowego klienta, ponieważ może on służyć do identyfikacji osoby.17

TEST

a. W jaki sposób atrybuty łączenia są używane do łączenia różnych baz danych?

b. Wyjaśnić triangulację informacji?

c. Jakie są szanse na prawidłową identyfikację osoby na podstawie jej kodu pocztowego, daty urodzenia i płci? Czemu?

d. Co to jest profilowanie?

Ograniczenia dotyczące dokumentów

Ostatni zestaw zabezpieczeń jest w tej chwili w powijakach. Ograniczenia dotyczące dokumentów próbują ograniczyć to, co użytkownicy mogą zrobić z dokumentami, aby zmniejszyć zagrożenia bezpieczeństwa.

ZARZĄDZANIE PRAWAMI CYFROWYMI

Pierwszym z tych zabezpieczeń jest zarządzanie prawami cyfrowymi (DRM), które ogranicza to, co ludzie mogą robić z danymi. W rzeczywistości lepszym terminem może być zarządzanie ograniczeniami cyfrowymi. W przypadku korporacji DRM jest pożądany w celu ochrony tajemnic handlowych i wrażliwych danych osobowych.

Zarządzanie prawami cyfrowymi (DRM) ogranicza to, co ludzie mogą robić z danymi. W przeszłości DRM był używany głównie przez wydawców muzyki i filmów, aby uniemożliwić ludziom piractwo materiałów chronionych prawem autorskim. Oczywiście uniemożliwiło to również użytkownikom przenoszenie plików między swoimi urządzeniami. Jedyną dobrą rzeczą, która pochodzi od wydawcy DRM, było uświadomienie sobie, że prawie wszystkie techniczne zabezpieczenia DRM mogą zostać pokonane przez atakujących. Wśród wydawców rośnie tendencja do udostępniania wersji niechronionych po nieco wyższej cenie. W biznesie DRM zwykle ogranicza to, co ludzie mogą zrobić, do dokumentów różnego rodzaju. Na przykład dana osoba może być w stanie pobrać plik arkusza kalkulacyjnego lub dokument edytora tekstu, ale może nie być w stanie zapisać go lokalnie, wydrukować, zmienić lub podjąć innych działań. Wiele z tych ograniczeń można ominąć, wykonując zrzuty ekranu tego, co pojawia się na monitorze. Inne ograniczenia są bardziej skuteczne. Na przykład osoba przeglądająca plik arkusza kalkulacyjnego prawdopodobnie nie będzie mogła przeglądać ukrytych informacji, a nawet widocznych części arkusza kalkulacyjnego.

ZARZĄDZANIE EKSTRUZJĄ DANYCH

Inną ochroną dokumentów jest zarządzanie wypychaniem danych, które ma na celu zapobieganie opuszczeniu firmy przez zastrzeżone pliki danych bez pozwolenia. Podczas gdy DRM wbudowuje ograniczenia w pliki dokumentów, zarządzanie wyciąganiem danych stosuje filtrowanie za każdym razem, gdy podjęta zostanie próba wysłania pliku poza firmę.

ZAPOBIEGANIE WYCISKANIU

Można również przeprowadzić filtrowanie, aby uniemożliwić pracownikom wysyłanie własności intelektualnej poza korporację. Filtrowanie zapobiegające wyciskaniu zaczyna się od prostego przeszukiwania dokumentów w poszukiwaniu słów takich jak „poufne”. W praktyce wykracza to daleko poza to.

Systemy zapobiegania utracie danych

Specjalne systemy zwane systemami zapobiegania utracie danych (DLP) są przeznaczone do zarządzania wyciąganiem danych, filtrowaniem zapobiegania wyciąganiu i zasadami DLP. Na poziomie przedsiębiorstwa systemy DLP to zazwyczaj urządzenia sprzętowe. Rysunek 9-32 pokazuje, że klienci DLP mogą być ładowani na wielu urządzeniach, a następnie zarządzani z jednego serwera. Rzeczywiste umiejscowienie menedżera DLP (serwera) będzie się różnić w zależności od wybranego dostawcy. Rysunek 9-32 ilustruje wspólne funkcje występujące w większości systemów DLP bez promowania konkretnego dostawcy. Systemy DLP są podobne do systemów antywirusowych. Skanują zarówno dane przychodzące do organizacji, jak i dane o każdym kliencie. Jednak zamiast skanowania w

poszukiwaniu wirusów, systemy DLP skanują w poszukiwaniu wskazanej zawartości (tj. typów plików, wzorców danych).

DLP PRZY BRAMIE

Systemy DLP mogą filtrować całą zawartość przychodzącą i wychodzącą, w tym wiadomości e-mail, komunikatory, transfery FTP, niezatwierdzoną pocztę internetową i tak dalej. Ponieważ serwer DLP jest oddzielnym urządzeniem sprzętowym, brama może kierować ruch przez serwer DLP.

DLP DLA KLIENTÓW

Systemy DLP mogą być ładowane na poszczególnych klientach. Zawartość można zeskanować przed wysłaniem danych. Uniemożliwiłoby to przesyłanie nielegalnych treści przez sieć lokalną. Uniemożliwiłoby to również kopiowanie danych z lokalnego klienta na urządzenie USB lub między dwoma dyskami. Pojedynczy system DLP obserwujący przychodzące i wychodzące strumienie danych przegapiłby te lokalne transfery. Ładowanie klientów DLP na każdym komputerze wymaga więcej czasu i wysiłku. Jednak dodatkowy wysiłek ułatwia egzekwowanie zasad dotyczących danych. Zapewnia również kontrolę nad danymi na każdym hoście, które zostałyby pominięte przez DLP na bramie.

DLP DO PRZECHOWYWANIA DANYCH

Systemy DLP mogą aktywnie wyszukiwać, oznaczać i monitorować wrażliwe dane w dowolnym miejscu firmy. Mogą również monitorować dostęp do wrażliwych danych. Systemy DLP mogą powiadamiać administratora, jeśli poufne dane są przechowywane niewłaściwie, takie jak numery SSN na serwerze FTP.

MENEDŻER DLP

Menedżer DLP może tworzyć zasady dotyczące danych w celu ochrony danych wrażliwych. Następnie może rozesłać te zasady do każdego klienta. Centralnie zarządzana funkcja DLP znacznie obniża koszty pracy w dużych korporacjach.

ZNAKI WODNE

Jednym ze sposobów ograniczenia przesyłania plików jest użycie znaku wodnego, który jest niewidoczną informacją przechowywaną w plikach. Pliki mogą być opatrzone znakiem wodnym tylko do użytku wewnętrznego, a pliki te można odfiltrować, jeśli podejmowane są próby wysłania ich poza firmę za pośrednictwem załączników e-mail, FTP lub innych środków.

Dodatkowo każdej kopii pliku można nadać inny znak wodny. Jeśli plik zostanie wyciągnięty do świata zewnętrznego, a następnie znaleziony ponownie, plik można prześledzić z powrotem do pierwszego odbiorcy za pomocą określonego znaku wodnego pliku. Innym podejściem jest analiza ruchu, która mierzy natężenie ruchu określonego typu od jednej strony do drugiej. Celem jest sygnalizowanie sytuacji, gdy ktoś pobiera niezwykle dużą liczbę poufnych dokumentów lub wysyła niezwykle dużą liczbę dokumentów poza firmę.

WYMIENNE ELEMENTY STERUJĄCE NOŚNIKIEM

Ostatnią strategią ograniczenia transmisji dokumentów jest zakazanie korzystania z nośników wymiennych, takich jak dyski optyczne, zewnętrzne dyski twarde, karty pamięci i napędy USB. Taka polityka może się powieść tylko wtedy, gdy na poszczególne komputery zostaną nałożone ograniczenia technologiczne. Poleganie wyłącznie na zachowaniu użytkownika jest receptą na niepowodzenie. Dyski USB są szczególnie niebezpieczne, ponieważ system Windows domyślnie implementuje automatyczne uruchamianie na tych dyskach. Oznacza to, że jeśli włożysz dysk USB do komputera i jeśli USB ma

złośliwe oprogramowanie ustawione na automatyczne uruchamianie, złośliwe oprogramowanie zostanie uruchomione natychmiast po włożeniu dysku. Czasami istnieje uzasadniona potrzeba biznesowa danych wymiennych. W takich przypadkach wszystkie dyski powinny być zaszyfrowane. Dostępne są dyski szyfrowane programowo i sprzętowo. Rysunek 9-33 przedstawia popularny szyfrowany dysk USB (IronKey). Ten dysk ulegnie samozniszczeniu, jeśli błędne hasło zostanie wprowadzone zbyt wiele razy.

PERSPEKTYWICZNY

Jak dotąd próby ograniczenia nieautoryzowanych transferów danych okazały się trudne do wyegzekwowania. Ponadto zazwyczaj w niewygodny sposób ograniczają funkcjonalność. Większość firm waha się przed egzekwowaniem ścisłych zasad zarządzania danymi.

TEST

a. Co to jest DRM? Podaj przykład działania DRM.

b. Dlaczego pożądany jest DRM?

c. Podaj kilka przykładów ograniczeń użytkowania, które firma może chcieć nałożyć na dokument.

d. Jak można obejść wiele zabezpieczeń DRM przed nieautoryzowanym drukowaniem?

e. Jaki jest cel zarządzania ekstruzją danych?

f. W jaki sposób systemy DLP mogą być skuteczne, gdy są umieszczone w bramie, na klientach i na serwerze bazy danych?

g. Co to jest znak wodny?

h. Na jakie dwa sposoby można wykorzystać znak wodny w zarządzaniu ekstruzją danych?

i. Dlaczego pożądane jest uniemożliwienie pracy komputera z nośnikami wymiennymi?

j. Dlaczego ograniczenia dotyczące nośników wymiennych powinny być egzekwowane technologicznie?

k. Dlaczego ochrona dokumentów nie jest intensywnie wykorzystywana w organizacjach?

Szkolenie pracowników

Jednym z najczęściej pomijanych mechanizmów wykorzystywanych do ograniczania utraty danych jest szkolenie pracowników. Bez względu na to, czy robią to złośliwie, czy nieumyślnie, pracownicy prawdopodobnie nadal będą istotnym źródłem utraty danych. Poniżej znajduje się kilka przykładów tego, jak pracownicy mogą nieumyślnie utracić dane.

SIEĆ SPOŁECZNOŚCIOWA

Pracowników należy przeszkolić, aby nie omawiali pracy na swoich osobistych blogach lub portalach społecznościowych. Może to być naruszenie umowy o zachowaniu poufności, którą podpisali, gdy zostali zatrudnieni. Mogą mówić o nowym projekcie, który rozpoczynają, krytykować wcześniejszy produkt jako „śmieci”, mówić o nowym patencie, który zamierzają zgłosić, lub komentować tajną kampanię marketingową. Pracownicy muszą być świadomi informacji, które zamieszczają w profesjonalnych serwisach sieciowych. Profesjonalne witryny sieciowe mogą udostępniać listy pracowników, doświadczenie zawodowe, zestawy umiejętności technicznych i komentarze dotyczące bieżących projektów. Konkurencja może wykorzystać te informacje do zatrudnienia kluczowych

pracowników i rozpoczęcia podobnego projektu. Jest za wcześnie, aby wiedzieć, jak serwisy społecznościowe wpłyną na bezpieczeństwo firmy.

TEST

a. Dlaczego pracownicy muszą być przeszkoleni w zakresie bezpieczeństwa danych?

b. Czy znasz kogoś, kto opublikował informacje o pracy na swoim blogu lub w serwisie społecznościowym? Czy było to pozytywne czy negatywne?

c. Z punktu widzenia bezpieczeństwa, czy uważasz, że serwisy społecznościowe uczyniły korporacje bardziej czy mniej bezpiecznymi?

Niszczenie danych

W pewnym momencie konieczne staje się zniszczenie danych. Po pierwsze, firmy muszą bezpiecznie niszczyć nośniki kopii zapasowych, które nie są już potrzebne. Po drugie, zniszczenie danych jest konieczne, gdy komputer zostanie wyrzucony lub przekazany innemu użytkownikowi. Istnieje wiele przerażających historii o ludziach kupujących komputery w serwisie eBay lub na pchlich targach, które zawierają wrażliwe dane osobowe, korporacyjne, a nawet dotyczące bezpieczeństwa narodowego.

Praktycznie rzecz biorąc, istnieją cztery rodzaje lub poziomy usuwania. Wybór jednej metody usunięcia zależy od przyczyny usunięcia danych. Jeden niekoniecznie jest lepszy od drugiego. W rzeczywistości większość tego rozdziału koncentrowała się na zachowaniu danych, a nie na ich niszczeniu. Jak zobaczysz, prawidłowe zniszczenie danych może wymagać tyle samo wysiłku, ile wymagało ich zachowanie.

USUNIĘCIE NOMINALNE

Najpopularniejszą formą usuwania w systemach Windows jest usuwanie nominalne (rysunek 9-35). Usunięcie nominalne ma miejsce po wybraniu pliku, a następnie naciśnięciu klawisza usuwania. Plik nie jest w ogóle usuwany. Został po prostu przeniesiony do Kosza. Kosz istnieje z tego samego powodu, dla którego w ołówkach pojawiają się gumki – każdy popełnia błędy. Pliki można odzyskać z Kosza za pomocą kilku kliknięć. Nie jest potrzebne żadne dodatkowe oprogramowanie do odzyskiwania plików.

PODSTAWOWE USUWANIE PLIKÓW

W systemach opartych na systemie Windows podstawowe usuwanie plików ma miejsce po opróżnieniu Kosza. Wskaźniki odnoszące się do niektórych sektorów są usuwane, ale dane w tych sektorach pozostają. Usunięto jedynie odniesienie do sektorów. Plik został usunięty logicznie, ale nie fizycznie. Podstawowe usuwanie plików jest podobne do usuwania części spisu treści książki. Odniesienie do rozdziału może zostać usunięte ze spisu treści, ale materiał rozdziału pozostaje nienaruszony. Dane można przywrócić za pomocą specjalnego oprogramowania do odzyskiwania danych, o ile nie zostały nadpisane. Nawet ponowne formatowanie lub partycjonowanie może nie spowodować bezpiecznego usunięcia danych. Dysk twardy pozostaje sprawny i można go ponownie wykorzystać. Wielu użytkowników popełnia błąd polegający na użyciu tylko podstawowego usuwania plików przed ponownym użyciem dysku, oddaniem go komuś innemu lub wyrzuceniem. Większość plików będzie można odzyskać, ponieważ nie zostały one bezpiecznie usunięte. Warto zauważyć, że osoby atakujące mogą użyć podstawowego usuwania plików, aby wydostać się z organizacji. Muszą tylko umieścić dane na dysku USB lub zewnętrznym, a następnie usunąć je za pomocą podstawowego usuwania plików. Nawet jeśli firma zeskanowała USB, czego zwykle nie robią, wszystko, co zobaczy, to puste miejsce. Atakujący może wrócić do domu i odzyskać wszystkie wcześniej usunięte pliki. Jedynym

sposobem zapobiegania tego typu atakom byłoby obowiązkowe wyczyszczenie całego wolnego miejsca na nośnikach pamięci przed opuszczeniem organizacji.

CZYSZCZENIE/CZYSZCZENIE

Bezpieczne usuwanie plików, zwane wymazywaniem lub czyszczeniem, polega na logicznym i fizycznym usuwaniu danych, dzięki czemu nie można ich odzyskać. Nawet oprogramowanie do odzyskiwania nie może przywrócić plików, jeśli zostały one bezpiecznie usunięte. Dysk twardy nadal nadaje się do użytku, ale wcześniejszych danych nie można odzyskać. Wszystkie dyski muszą zostać całkowicie wyczyszczone, zanim zostaną zmienione, opuszczą organizację lub zostaną zniszczone. Oprogramowanie do czyszczenia dysku zazwyczaj zastępuje wszystkie pliki, w tym wolne miejsce, jednym lub kilkoma przebiegami danych pseudolosowych. Nie wystarczy bezpiecznie usunąć istniejące pliki. Miejsce na dysku twardym oznaczone jako wolne miejsce może zawierać pliki, które zostały usunięte logicznie, ale nie zostały usunięte fizycznie. Dlatego cały dysk musi zostać wyczyszczony. Darik's Boot and Nuke (DBAN) to popularny program do czyszczenia dysków o otwartym kodzie źródłowym, używany przez administratorów od lat. Na koniec argumentowano, że szyfrowanie całego dysku jest alternatywną metodą wymazywania dysku. Dysk jest czyszczony po zaszyfrowaniu całego dysku, a następnie zniszczeniu kluczy szyfrowania. Odkażanie. W przeszłości można było odzyskać pliki nawet po wyczyszczeniu dysku. Do odzyskania danych potrzebny był specjalny sprzęt laboratoryjny. Termin odkażanie oznacza, że nośniki pamięci muszą być czyszczone, aby nawet specjalne metody laboratoryjne nie mogły odzyskać usuniętych danych. Jednak wraz ze zmianą nośników pamięci (gęstość ścieżek) odzyskanie danych stało się praktycznie niemożliwe nawet przy użyciu sprzętu laboratoryjnego. Ponieważ specjalne metody laboratoryjne przestały być skuteczne, termin ten stracił swoje wyróżnienie. Odkażanie i wycieranie oznaczały to samo. Jednak ostatnie badania z wykorzystaniem nowszych dysków półprzewodnikowych (SSD) wykazały, że bezpieczne usuwanie za pomocą czyszczenia może nie wystarczyć. Może zaistnieć potrzeba nowej sanityzacji proces dla dysków SSD, który uniemożliwi odzyskanie danych metodami laboratoryjnymi. Do tego czasu zniszczenie może być jedynym sposobem na uniemożliwienie odzyskania danych na dyskach SSD.

ZNISZCZENIE

W przypadku mediów najlepszym rozwiązaniem wydaje się fizyczne niszczenie. Wiele niszczarek biurowych może teraz niszczyć zarówno dyski optyczne, jak i papier. Firmy powinny mieć zasadę, że zanim jakikolwiek dysk optyczny zostanie wyrzucony, musi zostać zniszczony.

W przypadku dysków twardych czasami zaleca się fizyczne zniszczenie, ale każdy, kto próbował to zrobić, ma wielki szacunek dla wytrzymałości dysków twardych. Narodowy Instytut Standardów i Technologii (NIST) zaleca niszczenie wszystkich nośników, które były używane do przechowywania materiałów niejawnych. Fizyczne zniszczenie gwarantuje, że dane będą nie do odzyskania i bezużyteczne. Nośniki pamięci nie mogą być zmieniane, dlatego należy wziąć pod uwagę koszt dysków zastępczych. Mogą również wystąpić koszty związane z niszczeniem nośników. Mogą one obejmować opłatę za rozdrobnienie, stopienie lub rozmagnesowanie (rozmagnesowanie) nośników pamięci.

TEST

a. Dlaczego ważne jest, aby zniszczyć dane na nośnikach kopii zapasowych i komputerach przed ich wyrzuceniem lub przekazaniem komuś innemu?

b. Jaka jest różnica między podstawowym usuwaniem plików a czyszczeniem?

c. Czy bezpieczne jest wyczyszczenie dysku twardego, a następnie przekazanie go komuś innemu? Dlaczego lub dlaczego nie?

d. Co robi rozmagnesowanie?

e. Wymień kilka skutecznych metod niszczenia danych?

f. Jak można zniszczyć dyski optyczne?

WNIOSEK

Przyjrzano się roli danych w biznesie i znaczeniu ich bezpiecznego przechowywania. Zaczęliśmy od backupu, który jest pierwszą linią obrony firmy przed niszczycielskimi atakami. Przyjrzeliśmy się różnicy między tworzeniem kopii zapasowych plików/katalogów, tworzeniem kopii zapasowych obrazu i cieniowaniem. Przyjrzeliśmy się pełnej i przyrostowej kopii zapasowej kopii zapasowych plików/katalogów. Porównaliśmy także backup lokalny (na jednym komputerze) z systemami backupu sieciowego, w tym backupem scentralizowanym, ciągłą ochroną danych (CDP) dla serwerów, usługi tworzenia kopii zapasowych przez Internet dla klientów i tworzenie kopii zapasowych typu mesh dla klientów.

W następnej sekcji przyjrzeliśmy się nośnikom pamięci masowej i sposobom wykorzystania wielodyskowych macierzy RAID w celu zwiększenia niezawodności, wydajności odczytu i zapisu, szybkości tworzenia kopii zapasowych i skrócenia czasu odzyskiwania. Porównaliśmy poziomy RAID 0, 1 i 5. Zobaczyliśmy, jak połączenie parzystości i stripingu może zwiększyć prędkość dostępu do dysku i zapewnić nadmiarowość. Następnie przyjrzeliśmy się zasadom zarządzania kopiami zapasowymi, w tym określaniu, które dane muszą być zarchiwizowane według określonego harmonogramu, wymaganiem testów przywracania, ograniczaniem miejsca na nośniki, określaniem przechowywania i audytem wdrażania wszystkich zasad. Dyskusja na temat bezpieczeństwa baz danych koncentrowała się na ograniczaniu widoków według tabeli, kolumny, wierszy lub poziomu szczegółowości danych (ziarnistości). Następnie przyjrzeliśmy się kontrolom dostępu do bazy danych, audytom, wyzwalaczom i rozmieszczeniu baz danych w architekturze wielowarstwowej. W przypadku danych przyjrzeliśmy się również szyfrowaniu, w tym depozytowi kluczy i rozróżnieniu między szyfrowaniem plików/katalogów a szyfrowaniem całego dysku. W następnej sekcji skupiono się na tym, jak zapobiegać utracie danych. Mówiąc dokładniej, widzieliśmy, jak pewne dane osobowe mogą być wykorzystywane do łączenia odmiennych zbiorów danych w celu utworzenia nowego zbioru danych, który narusza prywatność danej osoby. Przyjrzeliśmy się, jak triangulację informacji można wykorzystać do wnioskowania lub obliczenia nieznanych danych. Zauważyliśmy, że systemy DRM, DLP i szkolenia pracowników to powszechne sposoby zapobiegania opuszczaniu organizacji wrażliwych danych. Zakończyło się dyskusją na temat metod bezpiecznego usuwania i niszczenia danych

Pytania do przemyślenia

1. Czy w Twojej organizacji są dane, które powinny być szyfrowane, ale nie są? Czemu?

2. Czy możesz uzyskać z Internetu wystarczającą ilość informacji, aby zaciągnąć pożyczkę na cudze nazwisko?

3. Ile danych byś stracił, gdyby dysk twardy twojego komputera uległ awariom? Czy możesz zmniejszyć ilość danych, które zostałyby utracone? Jak?

4. Jak Twoim zdaniem przetwarzanie w chmurze będzie miało wpływ na bezpieczeństwo danych?

5. Jak myślisz, jaki wpływ będą miały sieci społecznościowe na bezpieczeństwo danych? Podaj swoje uzasadnienie.

6. Dlaczego tak wiele kradzieży danych pochodzi spoza kraju przyjmującego ofiarę (wskazówka: ekstradycja)?

REAKCJA NA INCYDENTY I KATASTROFY

WPROWADZENIE

Walmart i huragan Katrina

W 2005 roku huragan Katrina uderzył w Luizjanę i Missisipi, Nowy Orlean i wiele innych miast na wybrzeżu Zatoki Meksykańskiej. Niedługo potem, czwarty pod względem intensywności huragan atlantycki w historii Rita ogromnie przyczynił się do zniszczenia. Federalna Agencja Zarządzania Kryzysowego (FEMA) stała się znana z radzenia sobie z kryzysem, reagując z opóźnieniem i działając nieudolnie, gdy zareagowała. Wiele firm upadło, ponieważ były słabo przygotowane na huragany. Jedną z firm, która zareagowała skutecznie, był Walmart. W swoim centrum dystrybucyjnym Brookhaven w stanie Mississippi firma miała 45 ciężarówek załadowanych i gotowych do dostawy jeszcze przed lądowaniem Katriny. Wkrótce firma dostarczyła 20 milionów dolarów darowizn w gotówce, 100 000 darmowych posiłków i 1900 ciężarówek pełnych pieluch, szczoteczek do zębów i innych artykułów ratunkowych dla ośrodków pomocy. Firma dostarczała również latarki, baterie, amunicję, sprzęt ochronny oraz posiłki dla policji i pracowników pomocy humanitarnej.

Chociaż akcja pomocy była imponująca, była to tylko widoczna końcówka programu odzyskiwania po awarii Walmart. Dwa dni przed uderzeniem Katriny Walmart uruchomił swoje centrum ciągłości biznesowej. Wkrótce ciężko pracowało 50 menedżerów i ekspertów w konkretnych obszarach, takich jak transport samochodowy. Tuż przed burzą, która zniszczyła firmową sieć komputerową, centrum nakazało centrum dystrybucji w Mississippi wysłanie do swoich sklepów produktów służących do odzyskiwania, takich jak wybielacze i mopy. Firma wysłała również do swoich sklepów 40 generatorów, aby sklepy, które utraciły energię, mogły otworzyć się, aby służyć swoim klientom. Wysłała również wielu pracowników ochrony do ochrony sklepów. Po awarii sieci komputerowych firma korzystała z telefonu, aby kontaktować się ze swoimi sklepami i innymi kluczowymi okręgami. Większość sklepów wróciła natychmiast, a prawie wszystkie sklepy były w stanie obsłużyć swoich klientów w ciągu kilku dni. Kolejki klientów były długie, a Walmart zaangażował lokalne organy ścigania do pomocy w utrzymaniu porządku. Walmart odniósł sukces dzięki intensywnym przygotowaniom. Firma posiada pełnoetatowego dyrektora ds. ciągłości działania. Posiada również szczegółowe plany ciągłości działania i jasne linie odpowiedzialności. W rzeczywistości, podczas gdy firma nadal reagowała na Katrinę i Ritę, monitorowała huragan u wybrzeży Japonii, przygotowując się do podjęcia tam działań Jeśli to konieczne.

TEST

a. Dlaczego Walmart był w stanie szybko zareagować?

b. Wymień co najmniej trzy działania podjęte przez Walmart, o których mogłeś nie pomyśleć.

Zdarzają się incydenty

Poprzednie części obejmowały fazy planowania i ochrony cyklu plan-ochrona-reakcja. Dobrze wykonane planowanie i ochrona mogą znacznie zmniejszyć liczbę udanych ataków, ale ochrona nigdy nie jest doskonała. Według Federalnego Biura Śledczego (FBI) około 1 procent skoncentrowanych ataków kończy się sukcesem. W związku z tym nawet firmy z dobrymi zabezpieczeniami muszą być przygotowane do obsługi udanych ataków (znanych również jako incydenty bezpieczeństwa, naruszenia lub kompromitacje). W tym rozdziale przyjrzymy się różnym poziomom ważności incydentów związanych z bezpieczeństwem i odpowiednim reakcjom korporacyjnym.

TEST

a. Czy dobre planowanie i ochrona mogą wyeliminować incydenty bezpieczeństwa?

b. Jakie trzy rzeczy są powszechnie nazywane skutecznymi atakami?

Ciężkość incydentu

Nie wszystkie incydenty są równie poważne. Incydenty wahają się od sytuacji na tyle łagodnych, że można je zignorować, aż po zagrożenia dla samej ciągłości biznesu. W tym rozdziale użyjemy skali zagrożeń z czterema kategoriami ważności incydentów: fałszywe alarmy, drobne incydenty, poważne incydenty i katastrofy.

FAŁSZYWE ALARMY

Fałszywe alarmy to sytuacje, które wydają się incydentami (lub przynajmniej potencjalnymi), ale okazują się niewinnymi działaniami. Działania podejmowane często przez atakujących są podobne do tych, które pracownicy, administratorzy systemów lub menedżerowie sieci rutynowo wykonują w swojej pracy. Systemy wykrywania włamań (IDS) prawdopodobnie oznaczą wiele legalnych działań jako podejrzanych. W rzeczywistości, w prawie wszystkich systemach IDS, większość podejrzanych działań okazuje się fałszywymi alarmami, czyli fałszywymi alarmami. Fałszywe alarmy, którymi zajmuje się personel dyżurny, marnują dużo czasu na ochronę. Bardziej subtelnie, jeśli jest zbyt wiele fałszywych alarmów, może to osłabić gotowość do zbadania każdego potencjalnego incydentu. Dzięki temu prawdziwe incydenty mogą pozostać niezauważone.

MNIEJSZE INCYDENTY

Przesuwając się w górę skali dotkliwości, drobne incydenty są prawdziwymi naruszeniami, z którymi może sobie poradzić personel dyżurny i które nie mają szerszych implikacji dla firmy. Przykładem drobnego incydentu jest infekcja wirusowa obejmująca kilkanaście komputerów. Metody reagowania na drobne incydenty są zwykle specyficzne dla naruszeń i dlatego trudno o nich mówić ogólnie. W tym rozdziale nie będziemy przyglądać się drobnym incydentom. Firmy muszą sobie z nimi radzić, ale nie poruszają one poważnych kwestii związanych z zarządzaniem lub polityką.

Drobne incydenty to naruszenia, z którymi dyżurny personel może sobie poradzić i które nie mają szerszych konsekwencji dla firmy.

GŁÓWNE INCYDENTY

W przeciwieństwie do tego, poważne incydenty mają zbyt duży wpływ na dyżurny personel IT. W przypadku poważnych incydentów wiele firm tworzy zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Oprócz specjalistów ds. IT i bezpieczeństwa IT zespoły CSIRT zazwyczaj mają członków z działu prawnego, public relations i wyższej kadry kierowniczej.

Poważne incydenty mają zbyt duży wpływ, aby mógł być obsłużony przez dyżurny personel IT i wymagają działania ze strony pracowników firmy spoza działu IT.

Poważne incydenty mogą stanowić poważne zagrożenie zysku. Firmy muszą radzić sobie z tymi incydentami szybko, sprawnie i skutecznie, aby ograniczyć straty. W tym rozdziale skupimy się na reagowaniu na poważne incydenty ze względu na wagę i złożoność tego typu reakcji na incydenty.

KATASTROFY

Pożary, powodzie i inne katastrofy wykraczają poza możliwości zespołów CSIRT. Klęski żywiołowe często zagrażają ciągłości biznesowej, czyli utrzymaniu bieżącej, przynoszącej dochody działalności firmy. Planowanie ciągłości biznesowej ma na celu jak najszybsze utrzymanie działalności lub

przywrócenie jej do działania. Firmy potrzebują silnych planów ciągłości działania i dobrze przećwiczonych zespołów ciągłości działania, kierowanych przez kierownika wyższego szczebla.

TEST

a. Jakie są cztery poziomy ważności incydentów?

b. Jaki jest cel zespołu CSIRT?

c. Z jakich części firmy pochodzą jej członkowie?

d. Co to jest ciągłość biznesowa?

e. Kto powinien kierować zespołem ciągłości działania?

Szybkość i dokładność

PRĘDKOŚĆ JEST ISTOTNA

Poważne naruszenia bezpieczeństwa i zagrożenia dla ciągłości biznesowej zawsze powodują poważną presję czasu. Atakujący będą nadal zadawać obrażenia, dopóki nie zostaną zatrzymani. Atakujący będą również nadal podejmować kroki, aby ich działania były trudniejsze do wykrycia i analizy. Nawet po tym, jak firma zatrzyma atakującego, potrzeba szybkości nadal trwa. W wielu przypadkach ważne systemy korporacyjne ulegną awarii, a ich awaria może kosztować firmę wiele pieniędzy w każdej godzinie ich awarii. Szybki powrót do zdrowia ma kluczowe znaczenie dla zmniejszenia obrażeń.

TAK JEST DOKŁADNOŚĆ

Dokładność jest równie ważna jak szybkość. Częstym błędem popełnianym przez ludzi pod presją jest pośpieszna reakcja, zanim dokładnie zrozumieją problem. Pospieszna reakcja może przesłonić ludziom prawdziwą pierwotną przyczynę problemu, która pozostaje niewidoczna i pozwala atakującemu na dalsze wyrządzanie szkód, podczas gdy osoba rozwiązująca problem próbuje rozwiązać niewłaściwy problem.

PLANOWANIE

Sposobem na szybką i poprawną reakcję jest przygotowanie się z wyprzedzeniem. Paradoksalnie działania podjęte przed incydentem są zwykle bardziej krytyczne niż działania podjęte po wystąpieniu incydentu. Organizacje muszą szczegółowo zaplanować, jak będą reagować na poważne incydenty i katastrofy. Być może najlepszą definicją reagowania na incydenty jest reagowanie na incydenty zgodnie z planem. Kryzys to nie czas na myślenie o tym, jak zareagować. Żaden plan nie będzie dokładnie pasował do incydentu, a sztywne trzymanie się planu może być szkodliwe. Jednak improwizacja w ramach planu jest o wiele bardziej efektywna niż praca bez planu.

Reagowanie na incydenty to reagowanie na incydenty zgodnie z planem.

PRÓBA

Oprócz planowania, kolejnym kluczem do szybkiej i prawidłowej reakcji na incydenty są próby. Kiedy drużyna piłkarska uczy się gry, ćwiczy ją wielokrotnie, aż jej wykonanie będzie skuteczne i płynne. Drobne incydenty są na tyle częste, że szybkość i dokładność są normalne. Jednak w przypadku rzadkich poważnych incydentów i katastrof próby są krytyczne i firmy muszą je często wykonywać. Najprostszym rodzajem próby jest instruktaż, w którym menedżerowie i inni kluczowi pracownicy spotykają się i omawiają krok po kroku, co każdy z nich zrobi podczas incydentu. W przypadku złożonych incydentów te instruktaże (nazywane również ćwiczeniami planszowymi) są dużymi

przedsięwzięciami, ponieważ angażują osoby z wielu działów. W przewodnikach często wykorzystuje się ćwiczenie scenariuszowe, w którym istnieje wstępny scenariusz opisujący incydent lub katastrofę. Często kierownik scenariusza dorzuca komplikacje podczas wykonywania ćwiczenia, aby sytuacja była jak najbardziej realistyczna. Okazjonalne testy na żywo dla krytycznych systemów sprawiają, że zespół faktycznie podejmuje działania zamiast opisywać, co by zrobił. Testy na żywo ujawniają subtelne wady, których nie są w stanie wykonać animacje. Na przykład jeden test na żywo wykazał, że krytyczne hasło wymagane w miejscu tworzenia kopii zapasowej znajdowało się w sejfie w uszkodzonej witrynie. Skażenie chemiczne spowodowane pożarem uniemożliwiło dostęp do tego sejfu. Testy na żywo są również lepsze w przypadku szkolenia ludzi. Oczywiście testy na żywo są drogie, więc firmy zwykle wykonują je rzadziej niż ćwiczenia przy stole.

TEST

a. Dlaczego szybkość reakcji jest ważna?

b. Dlaczego dokładność odpowiedzi jest ważna?

c. Zdefiniuj reakcję na incydent pod kątem planowania.

d. Dlaczego próby są ważne?

e. Co to jest samouczek lub ćwiczenie na stole?

f. Dlaczego test na żywo jest lepszy?

g. Na czym polega problem z testami na żywo?

PROCES REAGOWANIA NA WŁAMANIE W PRZYPADKU WAŻNYCH INCYDENCJI

Reakcja na incydent odpowiada zgodnie z planem. Zazwyczaj plan określa procesy, które firma powinna stosować w przypadku różnych rodzajów incydentów. Przyjrzymy się typowemu procesowi naruszenia pojedynczego serwera, który zawiera poufne informacje o kliencie. Jest to poważny incydent, ponieważ serwer zawiera poufne informacje o klientach, więc ma szersze znaczenie dla firmy.

Wykrywanie, analiza i eskalacja

Na początku incydentu są trzy priorytety.

• Pierwszym z nich jest szybkie nauczenie się, że doszło do incydentu. To jest wykrycie.

• Drugim jest zrozumienie incydentu, aby mieć pewność, że jest to prawdziwe wydarzenie, aby określić jego potencjalne szkody oraz zebrać informacje potrzebne do rozpoczęcia planowania zabezpieczenia i odzyskania. To jest analiza.

• Trzecim jest zajęcie się incydentem z personelem dyżurnym lub eskalacja obsługi do zespołu CSIRT lub zespołu ciągłości działania.

WYKRYCIE

Istnieje wiele sposobów na wykrycie ataku. IDS może ostrzec firmę o ataku lub analityk bezpieczeństwa może znaleźć podejrzane wzorce zdarzeń podczas analizy pliku dziennika IDS. Mówiąc prościej, ważny system może zawieść. Chociaż technologia może być w stanie wykryć wiele incydentów, firma nigdy nie powinna lekceważyć swoich zasobów ludzkich. Często pracownik nietechniczny jest pierwszą osobą, która zauważy, że system uległ awarii lub wydaje się działać nieprawidłowo. W związku z tym każdy, kto odkryje incydent, musi wiedzieć, jak go zgłosić. Każdy telefon powinien mieć np. naklejkę z numerem działu bezpieczeństwa IT, a szkolenie pracowników powinno zachęcać wszystkich

pracowników do dzwonienia nawet w razie wątpliwości. Z kolei pracownicy ochrony IT muszą być przeszkoleni, aby z szacunkiem odpowiadać na telefony.

ANALIZA

Po rozpoczęciu reakcji na włamanie, analityk bezpieczeństwa musi zrozumieć sytuację, zanim będzie można podjąć skuteczne działanie. Początkowo analityk bezpieczeństwa nie będzie nawet pewien, czy incydent jest problemem bezpieczeństwa, problemem sprzętowym, usterką oprogramowania, a nawet normalną pracą. Często większość fazy analizy włamań odbywa się poprzez odczytywanie plików dziennika z okresu, w którym incydent prawdopodobnie się rozpoczął. Celem jest dowiedzenie się, jak doszło do ataku, kto go doprowadził i co się wydarzyło od początku incydentu. Uzbrojona w te informacje, firma może działać skutecznie.

ESKALACJA

Poważne incydenty należy eskalować (przekazywać) do zespołu CSIRT lub zespołu ds. ciągłości działania.

TEST

a. Rozróżnij wykrywanie i analizę.

b. Dlaczego dobra analiza jest ważna na późniejszych etapach obsługi ataku?

c. Co to jest eskalacja?

Powstrzymywanie

Kolejny krok to powstrzymywanie - zatrzymanie obrażeń.

ODŁĄCZENIE

Radykalnym sposobem na opanowanie sytuacji jest odłączenie serwera od sieci lokalnej lub nawet odłączenie połączenia internetowego witryny. Chociaż rozłączenie powstrzymuje włamania, uniemożliwia również serwerowi obsługę uprawnionych użytkowników. W efekcie rozłączenie pomaga atakującemu, czyniąc serwer całkowicie niedostępnym. Wpływ na biznes może być poważny, jeśli serwer jest ważny.

CZARNE DZIUROWANIE NAPRACOWNIKA

Innym podejściem do powstrzymywania jest odcięcie atakującego, powiedzmy przez czarne dziurkowanie adresu IP atakującego, co oznacza, że firma odrzuci wszystkie przyszłe pakiety z tego adresu IP. Jednak osoby atakujące często mogą szybko przełączyć się na inny adres IP. Ponadto czarna dziura zdecydowanie powiadamia hakerów, że zostali wykryci. Jeśli atakujący wrócą ponownie, ich następne podejście może być bardziej skryte i trudniejsze do wykrycia.

KONTYNUACJA ZBIERANIA DANYCH

Jeśli uszkodzenie nie jest zbyt poważne, firma może zezwolić hakerom na dalszą pracę na serwerze. W tym czasie firma może obserwować, co robi napastnik. Informacje te mogą pomóc w analizie i mogą być potrzebne do zebrania dowodów do oskarżenia. Jednak nie blokowanie atakujących tak szybko, jak to możliwe, jest ryzykowne. Im dłużej atakujący znajdują się w systemie, tym bardziej stają się niewidoczni dzięki usunięciu dzienników IDS i tym więcej tylnych drzwi i innych szkód mogą stworzyć atakujący. To, czy zatrzymać atak, czy pozwolić mu kontynuować, to decyzja biznesowa, a nie tylko decyzja IT czy decyzja dotycząca bezpieczeństwa IT. Odłączenie systemu o znaczeniu krytycznym dla

firmy jest również decyzją biznesową. Zawsze powinien być dostępny kierownik wyższego szczebla, który podejmie krytyczne decyzje biznesowe związane z bezpieczeństwem. Ten wykonawca powinien posiadać możliwie największą wiedzę poprzez omówienie scenariuszy z wyprzedzeniem.

TEST

a. Co to jest powstrzymywanie?

b. Dlaczego odłączenie jest niepożądane?

c. Co to jest czarna dziura?

d. Dlaczego może to być tylko tymczasowe rozwiązanie zabezpieczające?

e. Dlaczego firma może pozwolić atakującemu na kontynuowanie pracy w systemie przez krótki czas?

f. Dlaczego to niebezpieczne?

g. Kto powinien podejmować decyzje o kontynuowaniu ataku lub odłączeniu ważnego systemu?

Powrót do zdrowia

Po powstrzymaniu ataku rozpoczyna się etap odzyskiwania. Atak niewątpliwie pozostawił serwer zaśmiecony backdoorami i innymi problemami. Personel musi przywrócić system do działania. W rzeczywistości system musi być lepszy niż przed atakiem, aby atakujący nie mógł wrócić. Gdy atakujący złamie system, często zaprasza innych atakujących, aby udowodnili swoje umiejętności. Jeśli atak zostanie zatrzymany, inni napastnicy będą próbowali włamać się, aby pokazać swoją wyższość.

NAPRAWA PODCZAS CIĄGŁEJ PRACY SERWERA

Idealnie, personel może naprawić serwer podczas pracy komputera. Na przykład, jeśli twój program antywirusowy wykryje wirusa, zwykle może naprawić zainfekowane pliki podczas kontynuowania pracy. Wykonanie tego na serwerze z funkcją krytyczną zapewnia dostępność tych usług dla użytkowników. Oznacza to również, że żadne dane nie zostaną utracone, ponieważ nie ma potrzeby uciekania się do taśm kopii zapasowych, które zawierają tylko informacje od ostatniej kopii zapasowej. Niestety bardzo trudno jest wykorzenić wszystkie konie trojańskie, wpisy w rejestrze, rootkity i inne nieprzyjemne niespodzianki zasiane przez atakującego. W przypadku ataku wirusa lub robaka czasami istnieją programy, które usuwają określone artefakty utworzone przez określony atak. Jednak w przypadku ręcznych włamań nie ma ogólnego programu do wykrywania i zawsze istnieje poważna obawa, że „mogliśmy przeoczyć jedno".

PRZYWRACANIE Z TAŚM ZAPASOWYCH

Jeśli atak miał miejsce w określonym czasie, personel może przywrócić pliki programu i danych z ostatniej zaufanej taśmy kopii zapasowej. Jednak dane zebrane od ostatniej kopii zapasowej zostaną utracone. Co gorsza, jeśli atakujący rozpocznie atak wcześniej, niż sądził, „zaufana" taśma zapasowa może przywrócić konie trojańskie i inne artefakty atakujących.

CAŁKOWITA PONOWNA INSTALACJA OPROGRAMOWANIA

O ile firmy nie mają pewności, że mogą znaleźć wszystkie rootkity i inne złośliwe oprogramowanie, zazwyczaj dokonują całkowitej ponownej instalacji systemu operacyjnego i programów. Jest to skomplikowany proces i nie rozwiązuje problemu utraty danych. Aby to osiągnąć, firma musi ponadto zachować i mieć gotowe oryginalne nośniki instalacyjne i klucze produktów. Ważne jest również udokumentowanie opcji konfiguracyjnych oprogramowania przed incydentem, aby firma mogła

przywrócić konfigurację po ponownej instalacji. Aby zmniejszyć problemy, firmy mogą okresowo wykonywać obrazy całego dysku i po prostu przywracać ten obraz dysku w razie potrzeby.

TEST

a. Jakie są trzy główne opcje odzyskiwania?

b. Z jakich dwóch powodów naprawa podczas ciągłej eksploatacji jest dobra?

c. Dlaczego to może nie działać?

d. Dlaczego przywracanie plików danych z taśm kopii zapasowych jest niepożądane?

e. Jakie są potencjalne problemy z całkowitą ponowną instalacją oprogramowania?

f. W jaki sposób posiadanie obrazu dysku zmniejsza problemy związane z całkowitą ponowną instalacją oprogramowania?

Przeprosiny

Jeśli atak wyrządził szkodę klientom lub pracownikom, ważne jest szybkie i szczere przeprosiny. Niestety, po wyciekach danych osobowych i innych szkodliwych incydentach większość przeprosin jest wypełniona hedgingiem i waflowaniem. Pomijanie powagi incydentu może wywołać jeszcze więcej gniewu i frustracji.

• Po pierwsze, uznaj odpowiedzialność i krzywdę. Przeprosiny, które obwiniają hakera lub przepraszają warunkowo, mówiąc coś w stylu „jeśli ktoś był niedogodny", co zrozumiałe, wywołują gniew, gdy są czytane. Przeproś, że firma pozwoliła na powodzenie ataku i przeproś po prostu za niedogodności lub inne szkody, które incydent spowodował adresata.

• Po drugie, wyjaśnij, co się stało. Szczegóły techniczne nie są konieczne. Należy jednak szczegółowo wyjaśnić potencjalne niedogodności i szkody. Autor przeprosin powinien zastanowić się, co chciałby wiedzieć, gdyby był ofiarą.

• Po trzecie, wyjaśnij, jakie działania zostaną podjęte w celu zrekompensowania tej osobie, jeśli w ogóle. Oczywiście różne incydenty wymagają różnych przeprosin. Niektóre w ogóle nie wymagają przeprosin, ale bardziej zasługują na przeprosiny niż je. Wyjaśnienia i działania, które należy podjąć, mogą, ale nie muszą być konieczne.

TEST

a. Jakie są trzy zasady przeprosin?

Kara

Niektóre firmy skupiają się wyłącznie na odzyskiwaniu, ignorując możliwość ukarania intruza. Jednak w pewnych okolicznościach niektóre firmy zdecydują się ukarać intruzów.

KARANIE PRACOWNIKÓW

Ściganie napastnika z zewnątrz jest bardzo złożone. Znacznie łatwiej jest ukarać pracownika, który atakuje wewnętrznie lub z domu. Chociaż sądy wymagają mocnych dowodów do oskarżenia, uzasadnienie nagany lub zwolnienia pracownika zwykle może być znacznie słabsze. W związku z tym większość firm jest znacznie bardziej skłonna ukarać pracownika niż próbować ścigać zewnętrznego hakera. Dział kadr i dział prawny będą jednak musiały podjąć decyzję o ukaraniu pracownika w oparciu o takie czynniki, jak przepisy związkowe i lokalne przepisy prawa pracy.

DECYZJA O WSZCZĘCIU PROCESU

Ściganie napastnika jest pożądane z wielu powodów, ale wiele firm niechętnie to robi.

Koszt i wysiłek. Jedną z par powodów, dla których nie należy ścigać napastników, są koszty i wysiłek, które byłyby potrzebne, aby znaleźć i ścigać przeciwnika. To nigdy nie są trywialne.

Prawdopodobieństwo sukcesu. W wielu przypadkach okaże się, że intruz mieszka w innym kraju lub nastolatek, który dostałby się do aresztu tylko przez kilka miesięcy. W takich przypadkach ściganie rzadko jest warte wysiłku.

Utrata reputacji. Ściganie jest procesem publicznym. Firma przyzna publicznie, że nie była w stanie zapobiec włamaniom. Może to zaszkodzić reputacji firmy, a utrata reputacji może kosztować firmę niektórych jej klientów. Przynajmniej niektórzy klienci mentalnie postawią firmę na okres próbny.

ZBIERANIE I ZARZĄDZANIE DOWODAMI

Sądy mają rygorystyczne zasady dotyczące zbierania i postępowania z dowodami kryminalistycznymi (dowodami, które są dopuszczalne w postępowaniu sądowym) po ich zebraniu.

Dowody kryminalistyczne to dowody, które można zaakceptować w postępowaniu sądowym.

Policja i FBI. Przed każdym atakiem personel ds. bezpieczeństwa IT powinien zapoznać się z lokalną jednostką policyjną ds. cyberprzestępczości oraz lokalną jednostką ds. cyberprzestępczości FBI. Funkcjonariusze organów ścigania mówią pracownikom ochrony, do kogo zadzwonić i co muszą zrobić pracownicy ochrony, dopóki nie przyjadą funkcjonariusze organów ścigania. FBI zbada sprawy handlu międzystanowego i kilka innych ataków. Policja zbada przypadki naruszenia prawa lokalnego i stanowego. Podczas incydentu jednak pracownicy ochrony powinni wezwać zarówno lokalną policję, jak i FBI, ponieważ nie zawsze jest pewne, która agencja sprawuje jurysdykcję nad konkretnym przestępstwem.

Ekspert medycyny sądowej. Policja i FBI mają własnych ekspertów z zakresu kryminalistyki komputerowej, ale w przypadku czynów niedozwolonych (pozwów cywilnych) firma musi korzystać z usług certyfikowanego eksperta z zakresu medycyny sądowej, który zbiera dane i interpretuje je w sądzie. Jeśli próbuje samodzielnie zebrać dowody, dowody prawdopodobnie nie będzie dopuszczalne w sądzie.

Zachowanie dowodów. Chociaż firma powinna jak najszybciej wezwać urzędy, pracownicy IT muszą rozumieć podstawowe zasady postępowania z dowodami. Na przykład bardzo ważne jest zachowanie dowodów. Zawartość dysku komputera szybko się zmienia. Jeśli to możliwe, pracownicy powinni wyciągnąć wtyczkę (dosłownie) na serwerze, którego dotyczy problem. Rysunek 10-8 przedstawia torbę dowodową Wireless StrongHold firmy Paraben dla urządzeń bezprzewodowych. Ta specjalnie zaprojektowana torba na dowody zapobiega przedostawaniu się lub wychodzeniu sygnałów bezprzewodowych z zajętego urządzenia bezprzewodowego.

Dokumentowanie łańcucha dostaw. Kolejną ważną zasadą jest dokumentowanie tego, co dzieje się z materiałem dowodowym po zebraniu. Łańcuch dowodowy to historia wszystkich transferów dowodów między ludźmi oraz wszystkich działań podejmowanych w celu ochrony dowodów znajdujących się w posiadaniu każdej osoby. Łańcuch dowodowy musi być jasny i dobrze udokumentowany. W przeciwnym razie sędzia prawdopodobnie całkowicie odrzuci dowody. Nawet jeśli dowód zostanie przyjęty, ława przysięgłych może nie zaakceptować dowodów, jeśli zostaną wykryte poważne problemy z pieczą.

TEST

a. Czy łatwiej jest karać pracowników lub ścigać napastników z zewnątrz?

b. Dlaczego firmy często nie ścigają napastników?

c. Czym są dowody kryminalistyczne? Porównaj, jakie cyberprzestępstwa badają FBI i lokalna policja.

d. Dlaczego oba mają być wezwane?

e. Na jakich warunkach będziesz musiał zatrudnić eksperta medycyny sądowej?

f. Dlaczego powinieneś zatrudnić eksperta medycyny sądowej, zamiast prowadzić własne śledztwo?

g. Czym jest łańcuch dowodowy i dlaczego jego dokumentacja jest ważna?

Ocena pośmiertna

W trakcie odpowiedzi niektóre rzeczy nieuchronnie nie potoczą się dobrze. Ważne jest, aby przeprowadzić pośmiertną ocenę tego, co po ataku poszło dobrze, a co nie, i wdrożyć wszelkie ulepszenia potrzebne w procesie reagowania. Niestety ten dość prosty, ale ważny krok jest często pomijany, ponieważ firma musi nadrobić zaległości, które zostały przełożone podczas ataku.

TEST

a. Dlaczego firmy powinny przeprowadzać ocenę pośmiertną po ataku?

Organizacja zespołu CSIRT

Większość z tego, co do tej pory opisaliśmy, to działania podejmowane przez personel IT i bezpieczeństwa IT. Jednak, jak wspomniano wcześniej w tym rozdziale, większość firm korzysta z zespołów CSIRT (zespołów reagowania na incydenty związane z bezpieczeństwem komputerów) do zarządzania poważnymi incydentami. Zespoły CSIRT mają szerszy udział, w tym:

• Kierownikowi wyższego szczebla powinien przewodniczyć zespół CSIRT. Wszystkie decyzje dotyczące bezpieczeństwa podczas poważnego incydentu są decyzjami biznesowymi. Tylko menedżerowie wyższego szczebla mogą zdecydować, czy wyłączyć serwer e-commerce. Chociaż kierownik zespołu CSIRT jest prawdopodobnie pracownikiem bezpieczeństwa IT, jego rola musi być podporządkowana prezesowi biznesowemu.

• Zespół CSIRT powinien mieć członków z zainteresowanych organizacji liniowych. Na przykład w przypadku incydentu związanego z handlem elektronicznym w podejmowaniu decyzji powinien uczestniczyć ktoś z działu handlu elektronicznego, chociaż może on nie być stałym członkiem zespołu CSIRT.

• Dyrektor ds. public relations firmy powinien być członkiem zespołu CSIRT. Dyrektor PR musi być jedynym głosem, który przemawia w imieniu korporacji do świata zewnętrznego podczas incydentu. Pracownicy IT i pracownicy ochrony IT nigdy nie powinni rozmawiać bezpośrednio z prasą lub innymi podmiotami zewnętrznymi. Nawet w firmie dyrektor ds. public relations powinien zajmować się komunikacją.

• Radca prawny firmy powinien być członkiem zespołu, aby umieścić wszystko w odpowiednich ramach prawnych. Radca prawny może doradzać w zakresie konsekwencji prawnych różnych działań, w tym sensu próby wniesienia oskarżenia.

• Dział zasobów ludzkich firmy powinien być członkiem, który oferuje wskazówki w kwestiach pracowniczych. Dodatkowo, jeśli sprawcą jest pracownik, dział kadr wdroży sankcje.

TEST

a. Dlaczego kierownik wyższego szczebla powinien kierować zespołem CSIRT?

b. Dlaczego członkowie odpowiednich działów liniowych powinni być w zespole CSIRT?

c. Kto jest jedyną osobą, która powinna wypowiadać się w imieniu firmy?

d. Dlaczego radca prawny firmy powinien być w CSIRT?

e. Dlaczego dział zasobów ludzkich firmy powinien znajdować się w zespole CSIRT?

Rozważania prawne

Jeśli firma decyduje się na ściganie, potrzebuje silnego zrozumienia prawa. Chociaż prawnicy wykonują ciężką pracę prawną, osoby zajmujące się bezpieczeństwem IT potrzebują ogólnego zrozumienia procesów prawnych, jeśli mają nadzieję uniknąć błędów, które unieważniają ich sprawy. Również firma może znaleźć się na krześle pozwanego. Może nie zapewnić ochrony danych klientów, pracownik może zaatakować komputery w innej firmie lub skompromitowany komputer może zaatakować inną firmę. Również w tych przypadkach bezpieczeństwo IT wymaga rozsądnego zrozumienia procesów prawnych.

Prawo karne a prawo cywilne

Być może najbardziej podstawowym rozróżnieniem w prawie jest rozróżnienie między prawem karnym a prawem cywilnym. Rysunek 10-9 pokazuje, że to rozróżnienie ma kilka czynników.

• Co najważniejsze, prawo karne zajmuje się naruszeniami ustaw karnych, które określają zachowania zabronione. Natomiast prawo cywilne zajmuje się interpretacjami praw i obowiązków, jakie mają względem siebie firmy lub osoby fizyczne.

• Jeśli chodzi o kary, sprawy karne mogą wiązać się z karą więzienia i grzywnami, podczas gdy sprawy cywilne skutkują jedynie karami pieniężnymi lub nakazami podjęcia lub niepodjęcia przez oskarżonego określonych działań.

• Najwidoczniej sprawy karne wytacza prokurator przeciwko pozwanemu, natomiast w sprawach cywilnych powód (strona wnosząca czyn niedozwolony) wszczyna sprawę przeciwko pozwanemu. Zazwyczaj strona pozwana wnosi pozew przeciwko stronie pozywającej. W takich przypadkach obie strony są powodami i obie są pozwanymi.

• W sprawach karnych prokurator ma obowiązek udowodnić winę oskarżonego ponad wszelką wątpliwość. W sprawie cywilnej powód zwykle musi jedynie wykazać przewagę dowodów (ponad 50%), że pozwany ponosi odpowiedzialność odszkodowawczą. Przewaga dowodów jest znacznie niższym standardem dowodowym.

• W sprawach karnych prokurator zwykle musi udowodnić, że oskarżony znajdował się w określonym stanie psychicznym, takim jak zamiar popełnienia czynu. Stan psychiczny to złożony temat, a wymagania dotyczące udowodnienia konkretnego stanu psychicznego są bardzo zróżnicowane w zależności od rodzaju przestępstwa. Na przykład w federalnych sprawach hakerskich w USA prokurator musi udowodnić, że oskarżony celowo uzyskał dostęp do zasobów bez upoważnienia lub z przekroczeniem upoważnienia. Prokurator nie ma jednak obowiązku udowadniania, że pozwany zamierzał wyrządzić szkodę, gdyby szkoda wystąpiła. Natomiast sprawy cywilne zwykle nie wymagają od powoda wykazania określonego stanu psychicznego pozwanego.

Specjaliści ds. bezpieczeństwa IT muszą rozumieć zarówno sprawy karne, jak i cywilne. Jeśli na przykład firma utraci dane osobowe swoich klientów, prawdopodobnie stanie się przedmiotem sprawy cywilnej. Jeśli jednak firma chce ukarać przestępcę komputerowego, będzie musiała przekonać prokuratora do wszczęcia procesu karnego. Czasami to samo zachowanie może naruszać zarówno prawo karne, jak i cywilne. Oskarżony, którego działania naruszają zarówno przepisy karne, jak i cywilne, może być ścigany karnie przez państwo, a następnie pozwany przez poszkodowanego o odszkodowanie pieniężne. Na przykład w 1995 roku O. J. Simpson został oskarżony o zabójstwo i uniewinniony. W całkowicie oddzielnej sprawie Simpson został również pozwany cywilnie za „niesłuszną śmierć" przez rodziny ofiar. Pod koniec sprawy cywilnej, w 1997 roku, Simpson został uznany za „odpowiedzialnego" za śmierć ofiar i nakazano mu zapłacić miliony dolarów odszkodowania.

TEST

a. Jakimi rodzajami działań zajmuje się prawo karne i cywilne?

b. Czym różnią się kary w prawie cywilnym i karnym?

c. Kto wnosi pozwy w sprawach cywilnych i karnych?

d. Jaki jest normalny standard rozstrzygania sprawy w procesach cywilnych i karnych?

e. Co to jest skóra męska?

f. W jakim rodzaju próbach mężczyźni są ważni?

g. Czy dana osoba może być sądzona oddzielnie w procesie karnym, a później w procesie cywilnym?

Jurysdykcje

Różne organy rządowe mają różne jurysdykcje – obszary odpowiedzialności, w których mogą tworzyć i egzekwować prawa, ale poza którymi nie mogą. Te jurysdykcje mają zastosowanie do prawa cybernetycznego, czyli dowolnego prawa dotyczącego technologii informatycznych.

Cyberprawo to każde prawo dotyczące technologii informatycznych.

Prawo międzynarodowe

Na arenie międzynarodowej przepisy dotyczące cyberprzestępczości również są bardzo zróżnicowane. W przypadku praw karnych i cywilnych dotyczących komputerów różnice między krajami często są duże i szybko się zmieniają (w większości przypadków stają się coraz większe). Prawo międzynarodowe jest ważne dla firm międzynarodowych a nawet dla firm, które mają do czynienia tylko z klientami lub dostawcami w innych krajach. Prawo międzynarodowe jest również ważne, ponieważ napastnicy często mieszkają w innym kraju niż ofiara. Podpisano szereg traktatów promujących współpracę międzynarodową w zakresie harmonizacji prawa i ścigania transgranicznego, ale ogólny stan współpracy międzynarodowej na tym etapie jest niedojrzały.

TEST

a. Czym jest orzecznictwo?

b. Jakie są jurysdykcje?

c. Czym jest cyberprawo?

d. Jakie są trzy poziomy sądów federalnych w USA?

e. Jakie poziomy mogą tworzyć precedensy?

f. Czy jurysdykcja federalna zazwyczaj obejmuje przestępstwa komputerowe, które są popełniane w całości na terenie danego stanu i które nie mają wpływu na handel międzystanowy?

g. Kto może zbadać cyberprzestępczość, która ma miejsce w mieście?

h. Czy międzynarodowe przepisy dotyczące cyberprzestępczości są dość jednolite?

i. Dlaczego firmy, które prowadzą działalność tylko w danym kraju, powinny martwić się międzynarodowym prawem cybernetycznym?

Dowody i informatyka śledcza

W sądach obowiązują surowe zasady określające, jakie dowody będą dopuszczane (dopuszczalne) w sądzie. Celem jest ochrona ławy przysięgłych przed przesłuchaniem niewiarygodnych dowodów. Po prostu nie można ufać przysięgłym, że będą w stanie ocenić wiarygodność dowodów. Na przykład prawo zwyczajowe od dawna jest podejrzliwe wobec dowodów ze słyszenia, które polegają na podsłuchiwaniu tego, co ktoś powiedział bez przysięgi. Tylko w bardzo nielicznych przypadkach dowody ze słyszenia są dopuszczalne. W federalnym systemie sądowym Stanów Zjednoczonych zasady dopuszczalności dowodów są skodyfikowane w federalnych zasadach dowodowych. Są aktualizowane co kilka lat i mają teraz silne zasady oceny dopuszczalności dowodów elektronicznych. Biorąc pod uwagę surowość federalnych zasad dowodowych, a także surowość zasad dowodowych w innych systemach sądowych, informacje mogą być dopuszczalne tylko wtedy, gdy są gromadzone przez osobę przeszkoloną zarówno w zakresie zasad dowodowych, jak i właściwych metod gromadzenia danych komputerowych.

Ekspert informatyki śledczej to profesjonalista przeszkolony w zakresie zbierania i oceny dowodów komputerowych w sposób, który może być dopuszczony w sądzie. Eksperci od informatyki śledczej dysponują na przykład specjalnym sprzętem do kopiowania zawartości dysków twardych w sposób technicznie uniemożliwiający wprowadzanie jakichkolwiek zmian w oryginalnym dysku twardym. Błędy w gromadzeniu danych komputerowych zazwyczaj unieważniają dowody, a sądy w ogóle nie pozwolą na przedstawienie dowodów ławie przysięgłych.

Ekspert informatyki śledczej to profesjonalista przeszkolony w zakresie zbierania i oceny dowodów komputerowych w sposób, który może być dopuszczony w sądzie.

Forensic Toolkit (FTK) firmy AccessData może wykonywać różnorodne zadania, w tym łamanie haseł, deszyfrowanie, obrazowanie i zdalne pozyskiwanie danych. Może również generować raporty na podstawie analizy danych znalezionych w pamięci RAM, dyskach twardych i rejestrach. W zeznaniach sądowych zwykli świadkowie mogą jedynie zeznawać na temat faktów i nie mogą próbować interpretować faktów dla ławy przysięgłych. W przeciwieństwie do tego, biegli świadkowie mogą interpretować fakty, aby dowody były zrozumiałe dla ławy przysięgłych w sytuacjach, w których ławnicy mogą mieć trudności z oceną samych dowodów. Biegli sądowi są certyfikowani biegli sądowi. Biorąc pod uwagę znaczenie dopuszczalności, firmy powinny korzystać z pomocy ekspertów medycyny sądowej, gdy przewiduje się ściganie. Biorąc pod uwagę znaczenie linii czasu, powinni oni wcześniej porozmawiać z wybranymi ekspertami medycyny sądowej, aby zrozumieć, co może być wymagane. Ponadto pierwszym krokiem w każdym dochodzeniu powinno być skontaktowanie się z ekspertem medycyny sądowej w celu uzyskania porady. Zwykle, na przykład, dowody komputerowe są najlepiej zachowane przez odłączenie komputera, ale nie zawsze tak jest. Zazwyczaj eksperci informatyki śledczej mogą zbierać dane z systemu, którego dotyczy problem, i przywracać jego działanie do dalszego użytku.

TEST

a. Dlaczego sądy nie uznają niewiarygodnych dowodów?

b. Kim jest ekspert informatyki śledczej?

c. Jaki świadek może interpretować fakty dla ławy przysięgłych?

d. Dlaczego firmy powinny współpracować z ekspertami kryminalistyki, zanim będą ich potrzebować?

SYSTEMY WYKRYWANIA WŁAMAŃ

Ataki często przebiegają niewidocznie z punktu widzenia ludzi - po prostu zmieniające się wzorce magnetyczne na dyskach lub wzorce elektroniczne w pamięci. Jak widzieliśmy w rozdziale 6, system wykrywania włamań (IDS) to oprogramowanie i sprzęt, który przechwytuje podejrzane dane o aktywności sieci i hosta w dziennikach zdarzeń i zapewnia automatyczne narzędzia do generowania alarmów, a także zapytania i narzędzia do raportowania, które pomagają administratorom w interaktywnej analizie danych w trakcie i po incydencie.

System wykrywania włamań (IDS) to oprogramowanie i sprzęt, który przechwytuje podejrzane dane o aktywności sieci i hosta w dziennikach zdarzeń i zapewnia automatyczne narzędzia do generowania alarmów oraz narzędzia do tworzenia zapytań i raportowania, które pomagają administratorom w interaktywnej analizie danych podczas i po incydencie.

IDS jest jak kamera bezpieczeństwa w budynku. Kamera bezpieczeństwa może zapewnić wykrywanie włamań w czasie rzeczywistym, jeśli ktoś monitoruje kamerę, i zapewnia taśmy, które można sprawdzić po incydencie, ale kamery bezpieczeństwa w budynkach nie zastępują zamków drzwi ani sejfów. Podobnie IDS jest tylko elementem architektury bezpieczeństwa. Nie powstrzymuje włamań; tylko je wykrywa. Używając innej terminologii, jest to kontrola detektywistyczna, a nie kontrola prewencyjna. Jak zauważono w rozdziale 6, głównym problemem związanym z IDS są fałszywe alarmy, czyli fałszywe alarmy. Podobnie jak chłopiec, który zbyt często krzyczał „wilk", IDS są zwykle ignorowane, jeśli generują wiele fałszywych alarmów, podobnie jak większość ludzi ignoruje alarmy samochodowe.

TEST

a. Co to jest IDS?

b. Czy IDS jest środkiem zapobiegawczym, detektywistycznym czy naprawczym?

c Co to są fałszywe alarmy?

d. Dlaczego problemy z fałszywymi alarmami są związane z IDS?

Funkcje IDS

IDS ma cztery główne funkcje: rejestrowanie, automatyczna analiza przez IDS, działania administratora i zarządzanie.

REJESTRACJA (GROMADZENIE DANYCH)

Funkcja rejestrowania rejestruje dyskretne działania, takie jak nadejście pakietu lub próba zalogowania. Każde działanie jest oznaczane znacznikiem czasu i przechowywane w pliku sekwencyjnym posortowanym według czasu. Ten plik zawiera surowe dane, które administratorzy IDS muszą przeanalizować, aby odpowiedzieć prawidłowo.

ZAUTOMATYZOWANA ANALIZA PRZEZ IDS

Systemy IDS wykonują wiele zautomatyzowanych analiz w ciągu dnia. Administratorzy zwykle nie wiedzą o tej analizie, chyba że system IDS wyśle ostrzeżenie na podstawie tego, co znajdzie podczas automatycznej analizy.

Sygnatury ataków. Dla systemu IDS dostępnych jest kilka ogólnych metod wyszukiwania wzorców w dużej ilości danych w plikach dziennika. Najprostszą analizą IDS jest wykorzystanie sygnatur ataków. Identyfikują one znane wzorce ataków. Działa to przez większość czasu, ale nie wykrywa ataków, które nie mają sygnatur w bazie sygnatur. Wykrywanie anomalii. Najbardziej wyrafinowane techniki obejmują wykrywanie anomalii, w ramach których system IDS szuka odchyleń od historycznych wzorców ruchu. Wykrywanie anomalii może wykrywać nowe zagrożenia, które nie mają jeszcze sygnatur ataków, ale jest mniej precyzyjne niż sygnatury ataków.

DZIAŁANIA

Wreszcie są działania podejmowane przez IDS i osoby z niego korzystające. Alarmy. Samo zbieranie i analizowanie danych nic nie daje. IDS muszą wykorzystywać wyniki analizy do interakcji z ludźmi. Najwyraźniej generują alarmy, jeśli analiza wskazuje na niebezpieczny stan. System IDS powinien generować alarmy tylko w przypadku stanów wysokiego zagrożenia. Gdyby system IDS wysyłał alarmy o wszystkich zagrożeniach, administratorzy bezpieczeństwa zostaliby zalani alertami. (Pomyśl o alarmach samochodowych uruchamianych włosowo.) Niektóre firmy stwierdzają, że nawet alarmy o wysokim zagrożeniu są zbyt liczne (i zbyt często nieprawidłowe) i wyrzucają swoje IDS. Alarmy nie powinny być uogólnionymi wskaźnikami, że coś jest nie tak.

• Alarmy powinny być jak najbardziej szczegółowe, dając użytkownikowi opis problemu.

• Powinien istnieć sposób na przetestowanie dokładności alarmu oraz

• Alarm powinien informować o tym, co powinien zrobić administrator bezpieczeństwa.

RAPORTY PODSUMOWANIA DZIENNIKA

Systemy IDS wysyłają alarmy tylko w przypadku zagrożeń wysokiego ryzyka. Rejestrują jedynie inne zagrożenia. Jednak administratorzy bezpieczeństwa muszą również rozumieć te mniejsze zagrożenia. Systemy IDS zazwyczaj generują raporty podsumowujące dzienniki, które wymieniają różne typy podejrzanej aktywności. Wskazują również priorytet zagrożenia według typu zagrożenia lub poprzez analizę statystyczną wskazującą na wysoką częstotliwość. Administratorzy IDS muszą analizować te raporty przynajmniej raz dziennie.

WSPARCIE DLA INTERAKTYWNEJ RĘCZNEJ ANALIZY LOGÓW

Ponadto systemy IDS pomagają ludziom zrozumieć gromadzone dane, zapewniając interaktywne narzędzia ręcznej analizy dzienników do przeglądania plików dzienników. Umożliwia to administratorom bezpieczeństwa „przeszukiwanie" plików dziennika, aby lepiej zrozumieć trwający lub zakończony atak i odfiltrować nieistotne wpisy. Na przykład analityk ds. bezpieczeństwa może przyjrzeć się wszystkim atakom na serwery poczty e-mail w ciągu ostatnich trzech godzin.

Kierownictwo. Ostatnią funkcją jest zarządzanie. IDS nie są jak tostery. Nie można ich po prostu podłączyć i oczekiwać, że same zapewnią bezpieczeństwo. Jak zobaczymy później, firma musi robić wiele rzeczy, aby zarządzać systemem IDS. Słabe zarządzanie spowoduje nadmierną pracę i może sprawić, że IDS będzie bezużyteczny.

TEST

a. Jakie są cztery funkcje IDS?

b. Jakie są dwa rodzaje analiz, które zwykle wykonują IDS?

c. O jakich rodzajach działań wspomniano w tej sekcji?

d. Jakie informacje powinny zawierać alarmy?

e. Jaki jest cel raportów podsumowujących dzienniki?

f. Opisz interaktywną analizę pliku dziennika.

Rozproszone IDS

W prostym IDS wszystkie cztery funkcje istnieją w jednym urządzeniu. Chociaż istnieją samodzielne systemy IDS, mają one ograniczone zastosowanie. Aby zrozumieć incydent związany z bezpieczeństwem, zwykle konieczne jest zobaczenie szerszego obrazu tego, które pakiety przepływają przez sieć i co dzieje się na wielu hostach. Ponowne uruchomienie jednego hosta jest normalne. Jeśli jednak kilka hostów uruchomi się ponownie w ciągu kilku minut, powinno to być poważne przebudzenie. Rysunek 10-18 przedstawia rozproszony IDS, który może zbierać dane z wielu urządzeń na centralnej konsoli menedżera (klient PC lub stacja robocza z systemem Unix).

AGENCI

Każde urządzenie monitorujące ma agenta oprogramowania, który zbiera dane o zdarzeniach i przechowuje je w plikach dziennika na urządzeniach monitorujących. Czasami agenci dokonują również analizy i zgłaszania alarmów.

MENEDŻER I ZINTEGROWANY PLIK LOGÓW

Program zarządzający jest odpowiedzialny za integrację informacji z wielu agentów działających na wielu urządzeniach monitorujących. W tym celu kierownik musi zebrać pliki dziennika z różnych urządzeń i zintegrować je w jeden zintegrowany plik dziennika (lub co najwyżej kilka plików dziennika). Menedżer musi analizować dane z pliku dziennika, generować alarmy i umożliwiać ludziom wykonywanie interaktywnych zapytań o dane.

PARTIA A PRZESYŁ DANYCH W CZASIE RZECZYWISTYM

Agent może przesyłać pliki dziennika do menedżera na dwa sposoby. Najtańszy jest transfer wsadowy, w którym agent czeka, aż ma kilka minut lub kilka godzin danych, a następnie wysyła do menedżera blok danych z pliku dziennika. Transfery w trybie wsadowym powodują najmniejsze obciążenie sieci, ponieważ wysyłanie dużych bloków danych zamiast wysyłania każdej transakcji jest wydajne. Minimalizuje również liczbę zakłóceń menedżera. (Każda przerwa na hoście wymaga znacznej aktywności procesora). W przeciwieństwie do tego, w transferach w czasie rzeczywistym dane każdego zdarzenia trafiają natychmiast do menedżera. Jest to atrakcyjne, ponieważ jedną z pierwszych rzeczy, które wielu hakerów robi po przejęciu urządzenia, jest usunięcie lub przynajmniej wyłączenie rejestrowania zdarzeń. Jeśli atakującemu się to uda, a ostatni transfer w trybie wsadowym został wykonany jakiś czas przed włamaniem się do systemu, dane dotyczące wszystkich jego działań zostaną utracone. W przypadku transferów w czasie rzeczywistym utracone zostaną tylko działania po usunięciu lub wyłączeniu rejestrowania zdarzeń.

BEZPIECZNA KOMUNIKACJA MENEDŻER-AGENT

Komunikacja między agentami a menedżerem powinna być bezpieczna, z uwierzytelnianiem, sprawdzaniem integralności, poufnością i ochroną przed powtórkami. Jeśli atakujący zdoła włamać się do komputera i sfałszować agenta lub menedżera, rezultatem będzie chaos.

KOMUNIKACJA Z DOSTAWCAMI

Dostawca również odgrywa rolę w tym procesie. Dostawcy okresowo tworzą nowe reguły filtrowania. Firmy muszą je pobrać i zainstalować na wszystkich IDS, zwykle za pośrednictwem menedżera. Komunikacja między dostawcą a menedżerem również musi być bezpieczna, z uwierzytelnianiem, sprawdzaniem integralności, poufnością i ochroną przed powtórkami.

TEST

a. Jaka jest zaleta rozproszonego IDS?

b. Nazwij elementy w rozproszonym IDS.

c. Rozróżnij kierownika i agentów.

d. Rozróżnij transfery wsadowe i w czasie rzeczywistym dla danych zdarzeń.

e. Jaka jest zaleta każdego typu?

f. Jakie dwa rodzaje komunikacji muszą być bezpieczne?

Identyfikatory sieciowe

Do tej pory mówiliśmy niejasno o „agentach". Teraz przyjrzymy się dwóm konkretnym typom agentów, z których korzystają firmy. Jak pokazuje Rysunek 10-18, istnieją dwa typy agentów — sieciowe IDS i hosta IDS. Zaczniemy od sieciowych IDS (NIDS), które przechwytują pakiety w trakcie ich podróży przez sieć.

SAMODZIELNE NIDS

Samodzielne NIDS to skrzynki zlokalizowane w różnych punktach sieci. Odczytują i analizują wszystkie ramki sieciowe, które przez nie przechodzą. Zasadniczo są to sniffery należący do korporacji.

NIDS PRZEŁĄCZNIKA I ROUTERA

Natomiast przełączniki NIDS i routery NIDS to przełączniki i routery z oprogramowaniem IDS. Zazwyczaj przechwytują one dane na wszystkich portach.

MOCNE STRONY NIDS

Siłą NIDS jest to, że widzą wszystkie pakiety przechodzące przez niektóre lokalizacje w sieci. Często te pakiety są wysoce diagnostyczne pod kątem ataków.

SŁABE STRONY NIDS

Jednak NIDS mają szereg słabości, które powodują problemy, o ile nie zostaną uzupełnione przez niesieciowe systemy IDS. Po pierwsze, chociaż NIDS przełączników i routerów oferują możliwość wewnętrznego gromadzenia danych, żadna firma nie może sobie pozwolić na obsługę agentów na wszystkich wewnętrznych przełącznikach i routerach. W konsekwencji wszystkie firmy mają martwe punkty, w których NIDS nie widzą pakietów. Jeśli w rzeczywistości wykorzystywane są tylko graniczne NIDS, to cała sieć wewnętrzna stanowi jeden duży martwy punkt. Po drugie, podobnie jak zapory sieciowe, NIDS nie mogą skanować zaszyfrowanych danych. Chociaż NIDS mogą skanować niezaszyfrowane części zaszyfrowanego pakietu (zazwyczaj dodany nagłówek IP), dostarcza to ograniczonych informacji. Wraz ze wzrostem popularności szyfrowania skuteczność NIDS będzie się proporcjonalnie zmniejszać.

TEST

a. Na jakie informacje zwracają uwagę NIDS?

b. Rozróżnij autonomiczne NIDS i NIDS oparte na przełączniku lub routerze.

c. Jakie są mocne strony NIDS?

d. Jakie są dwie słabości NIDS?

ID HOSTA

Firma ma wiele komputerów-hostów. Najbardziej krytycznymi hostami są serwery firmy. Systemy IDS hosta (HIDS) działają na danych zebranych na komputerze hosta.

ATRAKCJA HIDS

Główną atrakcją HIDS jest to, że dostarczają bardzo szczegółowych informacji o tym, co wydarzyło się na konkretnym hoście. Jest to ważne przy diagnozowaniu problemu.

SŁABE STRONY IDS HOSTA

Ograniczony punkt widzenia. IDS hosta mają dwie główne słabości. Po pierwsze, IDS hosta ma ograniczony widok na to, co dzieje się w sieci. To samo krótkowzroczne skupienie, które pozwala im być konkretnymi, oznacza również, że nie widzą szerszego obrazu. Powodem do niepokoju są powtarzające się błędy logowania na jednym hoście. Powtarzające się niepowodzenia logowania na wielu hostach w krótkim czasie są znacznie większym powodem do niepokoju. IDS hosta może zostać naruszony. Ponadto IDS hosta jest przedmiotem ataku. Jak wspomniano wcześniej, atakujący może usunąć lub zmienić pliki dziennika, skutecznie czyniąc atakującego niewidocznym dla HIDS.

ID HOSTA: MONITORY SYSTEMU OPERACYJNEGO

Większość IDS hosta to monitory systemu operacyjnego, które koncentrują się na zdarzeniach systemu operacyjnego. Oto niektóre dane zwykle gromadzone przez identyfikatory IDS monitorów systemu operacyjnego.

• Wiele nieudanych logowań

• Tworzenie nowych kont

• Dodawanie nowych plików wykonywalnych (programów — mogą być programami atakującymi)

• Modyfikowanie plików wykonywalnych (do tego służy instalacja koni trojańskich)

• Dodawanie kluczy rejestru (zmienia sposób działania systemu)

• Zmienianie lub usuwanie dzienników systemowych i plików audytu

• Zmiana zasad audytu systemu

• Użytkownik uzyskujący dostęp do krytycznych plików systemowych

• Użytkownik uzyskujący dostęp do nietypowych plików

• Zmiana samego monitora systemu operacyjnego

TEST

a. Jaka jest główna atrakcja HIDS?

b. Jakie są dwie słabości systemów IDS hosta?

c. Wymień kilka rzeczy, na które wyglądają monitory systemu operacyjnego hosta.

Pliki dziennika

WYDARZENIA CZASOWE

Wszystkie pliki dziennika mają ten sam format podstawowy. Każdy z nich to płaski plik wpisów dziennika. Każdy wpis dziennika ma sygnaturę czasową i typ zdarzenia. Poza tym pliki dziennika mogą zawierać inne informacje pomocne w diagnozowaniu zdarzenia. Na przykład pliki dziennika NIDS mogą zawierać podstawowe wartości pól pakietów. Z kolei wpisy HIDS dotyczące podejrzanych operacji na plikach będą nazywać plik, czynność wykonaną na pliku oraz użytkownika lub program podejmujący akcję.

INDYWIDUALNE DZIENNIKI

Problem z plikami dziennika z poszczególnych NIDS lub IDS hosta polega na tym, że każdy plik dziennika reprezentuje tylko lokalny widok działań w danym momencie. Na przykład powolne skanowanie wielu hostów w sieci prawdopodobnie nie przyciągnie uwagi żadnego pojedynczego hosta lub agenta monitorowania sieci.

ZINTEGROWANE DZIENNIKI

Aby zapewnić lepszy widok zdarzeń, firmy zwykle importują dane z plików dziennika z wielu hostów IDS i NIDS. Oprócz przechowywania wszystkich plików dziennika na jednym komputerze, rozproszone systemy IDS próbują agregować wszystkie wpisy dziennika z wielu źródeł w jeden zintegrowany plik dziennika, który zawiera dane z wielu miejsc w sieci w dowolnym momencie. Rysunek 10-21 przedstawia jeden z tych zintegrowanych plików dziennika. Proces tworzenia zintegrowanych plików dziennika nazywa się agregacją. Trudne do stworzenia. Jeśli firma posiada NIDS i HIDS od wielu dostawców, każdy z nich prawdopodobnie użyje innego formatu wpisów w pliku dziennika. W takim przypadku stworzenie zintegrowanego dziennika będzie niezwykle trudne, a być może nawet niemożliwe. Jednak niewiele firm jest skłonnych do standaryzacji u jednego dostawcy tylko po to, aby móc tworzyć zintegrowane dzienniki. Ponadto niektórzy dostawcy zajmują się tylko rejestrowaniem hostów, rejestrowaniem w sieci autonomicznej lub rejestrowaniem przełączników/routerów.

Synchronizacja czasu. Jeśli czasy na różnych IDS są przesunięte nawet o kilka tysięcznych sekundy, niezwykle trudno będzie zobaczyć, co się dzieje w danym momencie – zwłaszcza jeśli atak jest zautomatyzowany i następuje szybko. Network Time Protocol (NTP) umożliwia ten rodzaj synchronizacji. Wszystkie urządzenia muszą być zsynchronizowane z jednym wewnętrznym serwerem NTP

Korelacja zdarzeń. Często pojedyncze zdarzenia są podejrzane. Jeśli aplikacja próbuje zmienić plik wykonywalny systemu, jest to wysoce sugerujące atak. W innych przypadkach poszczególne zdarzenia nie są podejrzane, ponieważ osoby atakujące mają tendencję do robienia wielu takich samych rzeczy, jak zwykli użytkownicy. W takich przypadkach tylko sekwencje kilku wydarzeń mogą sugerować ataki. Analiza wzorców wielozdarzeniowych nazywana jest korelacją zdarzeń.

Na przykład jeden z menedżerów zauważył z pewnym zainteresowaniem, że na serwerze występuje duża liczba niepowodzeń autoryzacji bloku komunikatów serwera (SMB), co wskazuje na nieudane próby uzyskania dostępu do plików na innym serwerze. Kiedy trzy inne serwery zaczęły mieć dużą liczbę nieudanych autoryzacji SMB, śledztwo zostało wszczęte na najwyższych obrotach. Problemem okazało się rozprzestrzenianie się wirusa Sircam, który częściowo rozprzestrzeniał się poprzez

infekowanie udziałów sieciowych na innych komputerach. To pozwoliło firmie zacząć działać, gdy wirus dopiero zaczynał się rozprzestrzeniać. W pytaniach do przemyślenia zostaniesz poproszony o opisanie wzorców działań, które są podejrzane i czy sugerują one atak, czy też definitywnie dowodzą ataku. Aby rozpocząć, pamiętaj, że osoba, która się logowała, miała wcześniej dwa nieudane logowania kolejne. Może to wskazywać na zgadywanie hasła. Jednak zwykli użytkownicy czasami błędnie wpisują lub zapominają swoje hasła, więc dwa nieudane logowania nie są łącznie ostateczne. Zwróć uwagę, że między próbami logowania jest wystarczająco dużo czasu, aby wskazać człowieka. Gdyby próby były oddalone od siebie tylko o setki sekund, sugerowałoby to zautomatyzowany atak i byłby ostatecznym dowodem, że atak ma miejsce.

ANALIZA RĘCZNA

Znajdowanie przydatnych wzorców w zintegrowanych plikach dziennika, takich jak pokazany na rysunku 10-21, nie jest dla osób o słabym sercu. Ponadto znacznie uprościliśmy zadanie, usuwając nieistotne wpisy z pliku dziennika. Analityk musi najpierw posortować plik dziennika w poszukiwaniu odpowiednich wpisów. Wymaga to wysokiego poziomu doświadczenia i zdolności analitycznych.

TEST

a. Dlaczego zintegrowane pliki dziennika są dobre?

b. Dlaczego są trudne do stworzenia?

c. Wyjaśnij problem z synchronizacją czasu dla zintegrowanych plików dziennika.

d. Jak firmy osiągają synchronizację czasu?

e. Co to jest korelacja zdarzeń?

f. Rozróżnij agregację i korelację zdarzeń.

g. Dlaczego analiza danych pliku dziennika jest trudna?

h. Na rysunku 10-21, jak długie jest opóźnienie między pierwszą próbą logowania a drugą?

i. Czy oznacza to, że atak jest atakiem człowieka czy atakiem automatycznym?

Zarządzanie IDS

Firmy nie mogą po prostu podłączyć IDS i oczekiwać wspaniałych wyników. Być może bardziej niż jakiekolwiek inne dzisiejsze technologie bezpieczeństwa, systemy IDS wymagają ciągłej uwagi. Firmy bez znacznej wiedzy na temat bezpieczeństwa i zaangażowania w ciągłe nakłady czasu i pieniędzy nie powinny kupować systemów IDS.

STROJENIE DLA PRECYZJI

Ważnym problemem w zarządzaniu jest precyzja, co oznacza, że system IDS powinien zgłaszać wszystkie zdarzenia ataków i jak najmniej fałszywych alarmów.

Fałszywe pozytywy. Jak wspomniano wcześniej , IDS mają tendencję do generowania wielu fałszywych alarmów, znanych technicznie jako fałszywe alarmy. W wielu przypadkach fałszywe alarmy przewyższają liczbę prawdziwych alarmów dziesięć do jednego lub nawet więcej. W rzeczywistości duża liczba fałszywych alarmów generowanych przez IDS jest obecnie głównym problemem z IDS, powodując, że wiele firm przestaje ich używać po okresie próbnym.

Fałszywe negatywy. Systemy IDS mają również wiele fałszywych wyników negatywnych, które nie zgłaszają prawdziwych działań ataku. Fałszywe negatywy są o wiele bardziej niebezpieczne niż fałszywie pozytywne, ponieważ pozwalają na kontynuowanie prawdziwych ataków niewykrytych. Ponieważ jednak wyniki fałszywie negatywne nie są nachalne i często pozostają niewykryte, ich znaczenie często nie jest doceniane.

Strojenie. Firma może radykalnie zmniejszyć liczbę fałszywych trafień, jeśli „dostroi" swój IDS. Dostrajanie polega na wyłączeniu niepotrzebnych reguł i zmniejszeniu poziomu istotności alarmów generowanych przez inne reguły. Po pierwsze, firma powinna porzucić zasady, które nie mają sensu w konkretnym środowisku. Na przykład, jeśli organizacja używa wszystkich serwerów Unix, dlaczego jej IDS ma testować i tworzyć alarm dla ataku, którego celem jest złamanie zabezpieczeń programu serwera sieciowego IIS (który działa tylko na serwerach Windows)? Nawet po dostrojeniu fałszywe alarmy będą dominować w alertach. Counterpane, zarządzana firma zajmująca się bezpieczeństwem, odkryła, że nawet po dostrojeniu tylko 14% to rzeczywiste ataki.

Aktualizacje. Firmy muszą często aktualizować swoje sygnatury ataków IDS. Często dostawcy aktualizują swoje podpisy co tydzień lub nawet częściej. Oczywiście, jeśli firma dostosuje swoje reguły IDS, musi również dostroić reguły w każdej aktualizacji.

Wydajność przetwarzania. Problemy z wydajnością mogą sprawić, że IDS będzie bezużyteczny. Po pierwsze, przetwarzanie każdego zdarzenia wymaga dużej liczby cykli procesora. Wraz ze wzrostem ruchu w sieci i wzrostem liczby sygnatur ataków, systemowi IDS może brakować wydajności obliczeniowej potrzebnej do przetwarzania pakietów przy dużym obciążeniu sieci. Jeśli tak się stanie, IDS pominie niektóre pakiety i może przegapić ataki. Niewystarczająca wydajność jest szczególnie zła podczas wielu rodzajów ataków, takich jak wirusy, robaki i ataki DoS, które znacznie zwiększają ruch w sieci. IDS, który działa dobrze tylko wtedy, gdy system nie jest atakowany, jest bezwartościowy.

Składowanie. Pliki dziennika szybko stają się bardzo duże, więc IDS ograniczają rozmiary plików dziennika. Gdy pamięć dyskowa zbliża się do pojemności, IDS przesyła plik dziennika do kopii zapasowej i uruchamia nowy plik dziennika. Ogranicza to czas zajmowany przez każdy plik dziennika. Zdarzenie, które obejmuje pliki dziennika, jest trudne do przeanalizowania. Dodanie miejsca na dysku dla plików dziennika może wydłużyć czas zajmowany przez każdy plik dziennika, ale problem pozostanie.

TEST

a. Czym jest precyzja w IDS?

b. Co to są fałszywe alarmy i dlaczego są złe?

c. Czym są fałszywe negatywy i dlaczego są złe?

d. Jak strojenie może zmniejszyć liczbę fałszywych alarmów?

e. Co robi IDS, jeśli nie może przetworzyć wszystkich otrzymanych pakietów?

f. Co może się stać, jeśli w systemie zabraknie miejsca na dane?

g. Dlaczego ograniczenie rozmiaru plików dziennika jest konieczne, ale niefortunne?

Honeypot

Jednym z typów IDS jest honeypot. Honeypot to fałszywy serwer lub cały segment sieci z wieloma klientami i serwerami. Uprawnieni użytkownicy nigdy nie powinni próbować sięgnąć do zasobów honeypota, więc każda próba dostępu do honeypota może być atakiem. Jeśli alarm jest wysyłany przy

każdej nieprzemijającej próbie dostępu, administrator bezpieczeństwa ma duże szanse na złapanie atakujących. W praktyce honeypoty są używane głównie przez naukowców badających zachowanie napastników, rejestrując wszystko, co robi lub próbuje zrobić odwiedzający. Niektórzy administratorzy bezpieczeństwa korporacyjnego również uważają je za przydatne. Honeypot otworzył ponad 1300 różnych „fałszywych" gniazd. Skaner portów wykrył: jeden aktywny host, nazwę hosta, jego nazwę NetBIOS, 118 otwartych portów TCP i 33 otwarte porty UDP. Wyświetlał również odpowiedzi na zapytania z niektórych portów otwartych przez honeypot. Co ciekawe, uzyskanie obrazu dla rysunku 10-23 okazało się trudne. Podczas gdy autor (Randy Boyle) próbował zrobić zrzut ekranu, pułapka odświeżała się z powodu nowych wpisów. Wiele zdalnych komputerów z Pekinu (Chiny) próbowało uzyskać dostęp do jednego z sfałszowanych przez pułapkę portów. Port był prawdopodobnie powiązany z trojanem zdalnego dostępu. Zdalne maszyny wytrwale podejmowały próby komunikacji. Żądania pojawiały się co 30 sekund, a pierwotny adres IP był przenoszony na pół tuzina komputerów w tym samym bloku IP zlokalizowanym w Pekinie. W pewnym momencie jeden ze zdalnych adresów IP stał się bardzo aktywny. Wielokrotnie skanowali komputer autora w poszukiwaniu kilkunastu portów, o których wiadomo, że są kojarzone z popularnymi robakami, botami i trojanami.

TEST

a. Co to jest honeypot?

b. Jak honeypoty mogą pomóc firmom w wykrywaniu napastników?

c. Czy honeypot może przyciągnąć niechcianą uwagę atakujących?

PLANOWANIE CIĄGŁOŚCI DZIAŁALNOŚCI

Klęski żywiołowe, takie jak powodzie i huragany, poważne pożary budynków i masowe incydenty związane z bezpieczeństwem, takie jak cyberterror czy cyberwojna, mogą zagrozić podstawowej działalności firmy, a nawet zagrozić jej przetrwaniu. Każda firma powinna mieć solidny plan ciągłości działania, który określa, w jaki sposób firma będzie utrzymywać lub przywracać podstawowe operacje biznesowe po katastrofach.

Plan ciągłości działania określa, w jaki sposób firma planuje utrzymać lub przywrócić podstawowe operacje biznesowe w przypadku wystąpienia awarii.

Plan opracowuje zespół ds. planowania ciągłości działania z szeroką reprezentacją działów firmy. Plan określa, jakie działania biznesowe zostaną podjęte, a nie tylko jakie działania technologiczne należy podjąć. W przeciwieństwie do działań związanych z ciągłością działania, odzyskiwanie po awarii IT, jak pokazuje Rysunek 10-25, przywraca funkcje IT po awarii. Odzyskiwanie po awarii IT może być częścią szerszych działań firmy w zakresie ciągłości biznesowej po awarii lub może istnieć samodzielnie, gdy w centrum danych wybuchnie pożar.

Odzyskiwanie po awarii IT to przywracanie funkcji IT po awarii.

TEST

a. Co określają plany ciągłości działania?

b. Rozróżnij plany ciągłości biznesowej i plany odzyskiwania po awarii IT.

Zasady Zarządzania Ciągłością Działalności

Zanim zagłębimy się w szczegóły planowania ciągłości działania, powinniśmy przyjrzeć się trzem podstawowym zasadom, które powinny leżeć u podstaw każdego myślenia o ciągłości działania.

NAJPIERW LUDZIE

Pierwszym zadaniem planowania i zarządzania wydarzeniami jest zapewnienie bezpieczeństwa ludzi.

• Powinny istnieć plany ewakuacji i ćwiczenia ewakuacyjne.

• Firma nigdy nie powinna pozwalać członkom personelu na przebywanie w niebezpiecznym środowisku ze słabościami konstrukcyjnymi lub toksycznymi chemikaliami.

• Firma powinna mieć systematyczny sposób natychmiastowego rozliczania wszystkich pracowników, aby można było podjąć działania w przypadku zaginięcia osób. Ponadto firma musi udostępniać bliskim informacje o statusie pracownika.

• Później będzie potrzebna porada.

ZMNIEJSZONA ZDOLNOŚĆ W PODEJMOWANIU DECYZJI

Inną podstawową zasadą jest to, że ludzie podczas kryzysów nie są najlepsi poznawczo. Osoby w stresie, w sytuacjach emocjonalnych i pod presją czasu zwykle nie myślą dobrze. W związku z tym ważne jest, aby zaplanować jak najwięcej z wyprzedzeniem i aby ludzie przećwiczyli to, co będą robić, czyniąc jak najwięcej działań tak automatycznymi, jak to tylko możliwe.

UNIKANIE SZTYWNOŚCI

Jednocześnie sztywne planowanie wstępne nie powinno prowadzić do utraty elastyczności reakcji. W sytuacji kryzysowej często zdarzają się nieoczekiwane sytuacje, komunikacja będzie niestabilna, a informacje nierzetelne. Jeśli struktura jest zbyt sztywna, decydenci nie będą w stanie zareagować na te niepewności. Osoby z największą wiedzą na pierwszej linii muszą być w stanie podejmować decyzje. Nie powinno to oznaczać, że staranne planowanie nie jest konieczne. Jak zauważono wcześniej w tym rozdziale, adaptacja w ramach silnego planu jest zwykle znacznie lepsza niż całkowita improwizacja.

KOMUNIKACJA, KOMUNIKACJA, KOMUNIKACJA

W sytuacjach kryzysowych komunikacja nieuchronnie się załamuje, ponieważ technologia nie może przetrwać uszkodzeń budynków lub długich okresów bez zasilania elektrycznego. Decydenci muszą radzić sobie z awariami łączności, mając awaryjne zapasowe systemy łączności. Obejmuje to takie rozwiązania low-tech, jak drzewka telefoniczne, w których każdy pracownik dzwoni do stałej liczby innych pracowników, aby przekazać ważne wiadomości.

TEST

a. Jakie cztery zabezpieczenia firmy mogą zapewnić ludziom w sytuacji zagrożenia?

b. Dlaczego rozliczanie całego personelu jest ważne? (Odpowiedzi nie ma w tekście.)

c. Dlaczego ludzkie poznanie w sytuacjach kryzysowych wymaga szeroko zakrojonego planowania wstępnego i prób?

d. Dlaczego konieczne jest, aby plany i procesy wyjścia z kryzysu nie były zbyt sztywne?

e. Dlaczego systemy komunikacji ulegają awariom podczas kryzysów?

Analiza procesów biznesowych

IDENTYFIKACJA PROCESÓW BIZNESOWYCH I ICH POWIĄZANIA

Pierwszym krokiem w tworzeniu planu ciągłości działania jest identyfikacja głównych procesów firmy i ocena ważności każdego z nich. Firma to sieć procesów biznesowych, takich jak księgowość, sprzedaż, produkcja i marketing. Te procesy są współzależne. Każdy musi być zidentyfikowany. Co ważniejsze, kluczowe interakcje między biznesem procesy muszą być określone i zrozumiane.

PRIORYTETYZACJA PROCESÓW BIZNESOWYCH

Następnym krokiem jest ustalenie priorytetów procesów biznesowych, tak aby firma mogła najpierw przywrócić najważniejsze procesy biznesowe. Kluczowym czynnikiem jest wrażliwość funkcji na przestoje. Firma musi szybko uruchomić systemy wprowadzania zamówień, w przeciwnym razie sprzedaż zostanie utracona. Naliczanie opłat może trwać nieco dłużej, zanim zacznie wpływać na działalność firmy. Aby skomplikować sprawy, niektóre procesy biznesowe o niskiej wartości muszą zostać uruchomione jako pierwsze, ponieważ wymaga ich jeden lub więcej procesów biznesowych o wyższej wartości.

OKREŚL POTRZEBY ZASOBOWE

Oprócz ustalania priorytetów dla każdego procesu, planowanie powinno określać, jakich zasobów potrzebuje każdy proces. Z powodu zakłóceń w trakcie i po katastrofie firma może być zmuszona do przeniesienia części pozostałych zasobów z procesów o niższym priorytecie na procesy o wyższym priorytecie.

OKREŚL AKCJE I SEKWENCJE

Studium przypadku Walmart na początku tego rozdziału wskazuje, że plan określał kilka bardzo precyzyjnych działań, w tym dostarczanie materiałów do sprzątania i personelu ochrony do poszczególnych sklepów.

TEST

a. Wymień cztery kroki w analizie procesów biznesowych?

b. Wyjaśnij, dlaczego każdy z nich jest ważny.

Testowanie i aktualizowanie planu

Po opracowaniu planu ciągłości działania przy użyciu danych pochodzących od wielu różnych działów i zewnętrznych partnerów biznesowych, firma musi przetestować plan. Jak wspomniano wcześniej w tym rozdziale, przydatne są zarówno instrukcje (ćwiczenia na stole), jak i testy na żywo. Testowanie jest trudniejsze w przypadku awarii ciągłości biznesowej niż w przypadku poważnych incydentów związanych z bezpieczeństwem, ponieważ katastrofy mają znacznie szerszy wpływ i angażują tak wiele osób. Firma musi często aktualizować plan, ponieważ warunki biznesowe stale się zmieniają, a firmy nieustannie się reorganizują. W czasie kryzysu to zły moment na zastanawianie się, kto musi przejąć obowiązki przypisane do działu, który już nie istnieje. To jeszcze gorszy czas, by odkryć, że Twój plan nie obejmuje nowych działań biznesowych. Numery telefonów i inne dane kontaktowe zmieniają się nawet szybciej niż inne czynniki i powinny być aktualizowane co miesiąc. Wszystkie te aktualizacje wymagają małego stałego personelu do zapewnienia ciągłości biznesowej. Personel będzie również pełnił funkcję kierownika operacyjnego podczas katastrofy.

TEST

a. Dlaczego plany ciągłości działania są trudniejsze do przetestowania niż plany reagowania na incydenty?

b. Dlaczego częste aktualizowanie planu jest ważne?

c. Dlaczego firmy muszą jeszcze częściej aktualizować dane kontaktowe?

d. Z jakich dwóch powodów niezbędny jest personel zapewniający ciągłość działania?

ODZYSKIWANIE PO KATASTROFIE IT

Planowanie ciągłości biznesowej określa ogólną strategię ponownego uruchomienia firmy. Z kolei odzyskiwanie po awarii IT skupia się w szczególności na technicznych aspektach tego, jak firma może przywrócić IT do działania. Odzyskiwanie po awarii IT może istnieć samoistnie, jak w przypadku pożaru centrum danych, lub może być częścią znacznie większego wysiłku ciągłości biznesowej w przypadku awarii. Odzyskiwanie po awarii skupia się w szczególności na technicznych aspektach, w jaki sposób firma może przywrócić działanie IT za pomocą narzędzi do tworzenia kopii zapasowych.

Planowanie odzyskiwania po awarii IT ma kluczowe znaczenie dla szybkiego i pomyślnego przywrócenia ciągłości biznesowej. Podczas ataku na World Trade Center dwie firmy prawnicze w pobliżu centrum zostały poważnie uszkodzone, gdy dwie wieże się zawaliły. Jeden miał dobry program odzyskiwania po awarii IT i wrócił do normalnej działalności biznesowej w ciągu dwóch dni. Drugi nie utracił i utracił wszystkie swoje skomputeryzowane dane. Rok później druga firma wciąż przeglądała zadrukowane papiery w magazynach w celu odtworzenia swojej ewidencji. Aby częściowo zreplikować swoje dane, musiał trafić do klientów, a nawet konkurencji.

Chociaż wiele osób postrzega odzyskiwanie po awarii IT jako „problem dla techników", najwyższe kierownictwo musi dobrze rozumieć realia odzyskiwania po awarii IT. Na przykład w jednej firmie ubezpieczeniowej dyrektorzy myśleli, że mogą wrócić do pełnej działalności w ciągu 48 godzin. Jednak dyrektor wykonawczy firmy zajmujący się odzyskiwaniem po awarii IT wiedział, że nawet plan wymagał sześciu dni odzyskiwania, a plan nigdy nie został nawet przeanalizowany w celu ustalenia, czy jest wykonalny. Ponadto, jak wspomniano wcześniej w tym rozdziale, każda decyzja informatyczna podjęta w odpowiedzi jest decyzją biznesową. Decyzje, które wydają się czysto techniczne, mogą mieć poważne implikacje dla biznesu, których specjaliści IT mogą nie zaakceptować i z pewnością nie powinni mieć do nich ostatecznego wezwania.

TEST

a. Co to jest odzyskiwanie po awarii IT?

b. Dlaczego jest to problem biznesowy?

Rodzaje urządzeń do tworzenia kopii zapasowych

Kiedy główny ośrodek komputerowy przestaje działać, praca musi zostać przeniesiona do ośrodka zapasowego, zwykle w innym miejscu. Istnieje kilka rodzajów urządzeń do tworzenia kopii zapasowych. Każdy typ ma mocne i słabe strony.

GORĄCE STRONY

Atrakcyjny obiekt zapasowy to gorący obiekt gotowy do działania w sytuacji awaryjnej. Gorąca lokalizacja to obiekt fizyczny z zasilaniem, HVAC (ogrzewanie, wentylacja i klimatyzacja), sprzętem, zainstalowanym oprogramowaniem i aktualnymi danymi. Gdy tylko ludzie będą mogli się wprowadzić, gorąca strona może przejąć pełną eksploatację uszkodzonego miejsca. Z załogą szkieletową podstawowa operacja może rozpocząć się jeszcze wcześniej. Gorące witryny są atrakcyjne, gdy procesy mają niewielką tolerancję na przestoje. Mogą szybko wrócić do działania i rzadko zdarzają się poważne opóźnienia, które mogą wystąpić, gdy oprogramowanie jest trudne do zainstalowania na komputerach

używanych w innych typach urządzeń do tworzenia kopii zapasowych. Jednak gorące witryny są również bardzo drogie, a zapewnienie, że oprogramowanie w witrynie kopii zapasowej jest skonfigurowane w taki sam sposób, jak oryginalne oprogramowanie, jest trudne.

ZIMNE STRONY

Z kolei chłodne miejsca oferują zaplecze fizyczne, energię elektryczną i HVAC, ale są to puste pomieszczenia z połączeniami ze światem zewnętrznym. Aby skorzystać z zimnej witryny, firma musi zaopatrzyć się w sprzęt, sprowadzić i skonfigurować; Zainstaluj oprogramowanie; i montuj dane. Zanim to wszystko się stanie, firma może zbankrutować. Witryny zimne są tanie niż witryny gorące, ale firmy muszą realistycznie ocenić, na ile byłyby przydatne w praktyce.

UDOSTĘPNIANIE WITRYNY Z CIĄGŁĄ OCHRONĄ DANYCH

Chociaż gorące strony są atrakcyjne, ich utrzymanie jest kosztowne i wymaga czasu, aby zacząć działać. Firmy, które mają wiele centrów danych, mogą przenieść najbardziej krytyczne prace uszkodzonego centrum do innego centrum w firmie. Jednak nigdy nie jest to automatyczne. Firma potrzebuje sposobu na instalowanie programów i plików danych na komputerach w innych witrynach. Jeśli udostępnianie witryn wykorzystuje zsynchronizowane oprogramowanie w obu lokalizacjach z ciągłą ochroną danych (CDP), odzyskiwanie może być natychmiastowe. Jednak witryna rzadko będzie w stanie przejąć pełne obowiązki obu witryn, więc plan reagowania musi określać priorytety aplikacji. Jako przykład udostępniania witryn w firmie, UAL Loyalty Services ma dwa centra danych, które udostępniają witryny w rejonie Chicago. Aby dane w dwóch lokalizacjach były synchronizowane w czasie rzeczywistym, firma korzysta z obszaru metropolitalnego gigabit na sekundę. Oprócz zapewnienia odzyskiwania danych po awarii ciągła ochrona danych zapewnia najwyższy poziom ogólnego tworzenia kopii zapasowych.

LOKALIZACJA WITRYN

Jednym z problemów związanych z udostępnianiem witryn jest to, jak daleko od siebie znajdują się witryny. Jeśli znajdują się w tym samym mieście, oba mogą zostać zlikwidowane przez tę samą katastrofę. Jeśli są zbyt daleko od siebie, przenoszenie personelu między lokalizacjami może być niemożliwe. Jeśli firma ma wiele lokalizacji, może rozwiązać oba problemy.

Na przykład, kiedy firma Hewlett-Packard skonsolidowała swoje 85 centrów danych w zaledwie 6, umieściła po 2 w każdym z trzech miast – Atlancie, Houston i Austin. Miasta są na tyle odległe od siebie, że katastrofa, która dotknie więcej niż jedno z tych miast, jest mało prawdopodobna. Oznacza to, że większość katastrof będzie kosztować HP tylko jedną trzecią pojemności serwera. Pary w każdym mieście znajdowałyby się w odległości 15 mil od siebie – wystarczająco blisko, aby przenieść personel, ale na tyle daleko, aby jedno miejsce w każdej parze mogło przetrwać wszystko poza regionalną katastrofą.

TEST

a. Jakie są główne alternatywy dla witryn kopii zapasowych?

b. Jaka jest siła każdego z nich?

c. Jaki problem lub problemy wywołuje każdy z nich?

d. Dlaczego CDP jest konieczne?

Komputery biurowe

Chociaż serwery mają kluczowe znaczenie, komputery biurowe prawdopodobnie przechowują większość informacji biznesowych i możliwości analitycznych firmy. Pożar może zniszczyć powierzchnię biurową lub kilka obszarów biurowych, tak jak zniszczy serwerownię.

BACKUP DANYCH

W przypadku katastrofy często nie ma sposobu, aby przenieść wiele komputerów stacjonarnych z bezpiecznej drogi. Na przykład, nawet jeśli firma używa tylko notebooków, które można łatwo przenosić, nie będzie to skuteczne w przypadku pożaru budynku w środku nocy. Jedynym realnym rozwiązaniem jest posiadanie scentralizowanej kopii zapasowej plików PC i wymuszanie bieżącej synchronizacji plików.

NOWE KOMPUTERY

Jeśli większość komputerów zostanie utracona, firma będzie potrzebować nowych komputerów i będzie ich potrzebować bardzo szybko. Wcześniejsze ustalenia z dostawcami sprzętu firmy mogą usprawnić ten proces. Nowy komputer to za mało. Musi mieć oprogramowanie aplikacyjne, dlatego ważne jest, aby firmy zachowały swoje nośniki instalacyjne lub, jeśli mają standardowe konfiguracje, aby obrazy dysków tych standardowych konfiguracji były dostępne po awarii.

ŚRODOWISKO PRACY

Kolejną kwestią jest znalezienie miejsca do pracy. Powszechną opcją jest zabezpieczenie pokoi w hotelu z dobrym dostępem do Internetu. Inną opcją jest praca w domu, która eliminuje interakcje międzyludzkie, które są szczególnie krytyczne w płynnym i niepewnym środowisku po katastrofie. Ludzie mogą również lepiej radzić sobie emocjonalnie w środowisku ze znajomymi współpracownikami.

TEST

Jakie trzy rzeczy powinna zrobić firma, jeśli chodzi o planowanie odzyskiwania po awarii dla komputerów biurowych?

Przywracanie danych i programów

Wcześniej przyjrzeliśmy się archiwizacji plików programów i danych. Firmy muszą przywrócić te pliki w witrynie komputera kopii zapasowej. Przywracanie z taśm kopii zapasowych to jeden ze sposobów przenoszenia plików do lokalizacji kopii zapasowej. Jeśli taki jest cel, miejsce wykonywania kopii zapasowej musi mieć odpowiedni sprzęt do wykonania przywracania. Ponadto firmy muszą szybko dostarczać taśmy z kopiami zapasowymi do miejsca tworzenia kopii zapasowych i bezpiecznie. Może to być trudne w przypadku klęsk żywiołowych lub jeśli lokalizacja kopii zapasowej znajduje się daleko od miejsca przechowywania taśm kopii zapasowych. Oczywiście, jeśli firma stosuje omówioną wcześniej ciągłą ochronę danych, to nie jest konieczne ich odzyskiwanie. System zapasowy jest natychmiast gotowy do przejęcia.

TEST

a. Co należy zrobić, aby przywrócić dane w lokalizacji kopii zapasowej za pomocą taśm?

b. Jak to się zmienia, jeśli firma stosuje ciągłą ochronę danych?

Testowanie planu odzyskiwania po awarii IT

Podobnie jak plany ciągłości biznesowej wymagają testowania, firmy muszą również testować plany odzyskiwania po awarii IT w możliwie najbardziej realistyczny sposób. Ponadto firmy muszą przetestować swoje procedury odzyskiwania po awarii IT, aby poprawić szybkość i dokładność reakcji.

WNIOSEK

Ta ostatnia część zamyka cykl, omawiając reakcje zarówno na tradycyjne incydenty bezpieczeństwa, jak i katastrofy. Rozpoczęła się przykładem wzorowej reakcji na katastrofę. To było postępowanie Walmart w przypadku katastrofy huraganu Katrina w 2005 roku. Walmart ma dedykowany dział reagowania na katastrofy, który przyciąga ekspertów z wielu dziedzin, gdy katastrofa ma się wydarzyć. Ekspertyzy Walmart dotyczące katastrof nie przyszły łatwo. Opracował swoją metodę reagowania przez długi czas, który obejmował szereg katastrof. Po sprawie Walmart omówiliśmy podstawową terminologię i koncepcje reagowania na incydenty i katastrofy. Skupiliśmy się na czterostopniowej skali ważności incydentów - fałszywych alarmów, drobnych incydentów, którymi może zająć się dyżurny personel IT, poważnych incydentów wymagających zwołania przez firmę CSIRT oraz katastrof, które wpływają wyłącznie na IT lub zagrażają ciągłości działania dla całej firmy. W przypadku wszystkich incydentów i katastrof szybkość i dokładność mają kluczowe znaczenie. Wymagają one rozległego planowania i prób. Następnie przyjrzeliśmy się reakcji na poważne incydenty związane z bezpieczeństwem. Omówiliśmy szereg etapów, w tym wykrywanie, analizę, eskalację, powstrzymywanie, odzyskiwanie, przeprosiny, karę i ocenę pośmiertną. Omówiliśmy również organizację zespołu CSIRT. W przypadku kary omówiliśmy trudność ścigania karnego w porównaniu z (względną) prostotą dyscyplinowania pracowników. Następnie odbyła się dyskusja o względach prawnych, która rozpoczęła się od różnicy między prawem karnym a cywilnym. Następnie omówiono jurysdykcje w Stanach Zjednoczonych na poziomie federalnym i stanowym oraz międzynarodowe prawo dotyczące cyberprzestępczości. Omówiono również zasady dowodowe i kryminalistykę komputerową. Ta sekcja zakończyła się omówieniem przepisów federalnych dotyczących hakowania, ataków typu „odmowa usługi", ataków złośliwego oprogramowania i przechwytywania wiadomości elektronicznych podczas przesyłania i przechowywania. Następna sekcja dotyczyła IDS. Przyjrzeliśmy się czterem funkcjom IDS. Przyjrzeliśmy się również rozproszonym systemom IDS wykorzystującym systemy HIDS i NIDS. Przyjrzeliśmy się zagregowanym plikom dziennika i trudnościom w korelacji zdarzeń. Omówiliśmy problemy z dostrajaniem i trudnościami w korelacji zdarzeń w wielu zapisanych plikach dziennika. Rozdział zakończył się omówieniem planowania ciągłości działania i reagowania na katastrofy IT. W celu reagowania na awarie IT ważne jest, aby przywrócić funkcjonalność serwera w innych lokacjach, najlepiej poprzez współdzielenie lokacji z CDP. Omówiono również korzyści płynące z korzystania z centrów danych. Reakcja ciągłości działania w przypadku katastrof zagrażających funkcjonowaniu firmy jest zadaniem o wiele bardziej złożonym. Aby osiągnąć sukces, potrzeba dużo planowania.

Pytania do przemyślenia

1. Doradzasz małej firmie. (a) Czy poleciłbyś użycie firewalla? Wyjaśniać. (b) Czy poleciłbyś korzystanie z programu antywirusowego?filtracja? Wyjaśniaj. (c) Czy poleciłbyś system wykrywania włamań? Wyjaśnij.

2. Gdy systemy IDS generują alerty, mogą wysyłać je do konsoli w centrum bezpieczeństwa, na telefon komórkowy lub za pośrednictwem poczty e-mail. Omów zalety i wady każdego z nich.

3. Sprawdź zintegrowany plik dziennika pokazany na rysunku

Entry	Time	Log Information
1	8:45:05:47	Packet from 1.15.3.6 to 60.3.4.5 (NIDS log entry)
2	8:45:07:49	Host 60.3.4.5. Failed login attempt for account Lee (Host 60.3.4.5 log entry)
3	8:45:07:50	Packet from 60.3.4.5 to 1.15.3.6 (NIDS)
4	8:45:50:15	Packet from 1.15.3.6 to 60.3.4.5 (NIDS)
5	8:45:50:18	Host 60.3.4.5. Failed login attempt for account Lee (HIDS)
6	8:45:50:19	Packet from 60.3.4.5 to 1.15.3.6 (NIDS)
7	8:49:07:44	Packet from 1.15.3.6 to 60.3.4.5 (NIDS)
8	8:49:07:47	Host 60.3.4.5. Successful login attempt for account Lee (HIDS)
9	8:49:07:48	Packet from 60.3.4.5 to 1.15.3.6 (NIDS)
10	8:56:12:30	Packet from 60.3.4.5 to 123.28.5.210. TFTP request (NIDS)
11	8:56:28:07	Series of packets from 123.28.5.210 and 60.3.4.5. TFTP response (NIDS)
13	9:03:17:33	Series of packets between 60.3.4.5 and 1.17.8.40. SMTP (NIDS)
14	9:05:55:89	Series of packets between 60.3.4.5 and 1.17.8.40. SMTP (NIDS)
15	9:11:22:22	Series of packets between 60.3.4.5 and 1.17.8.40. SMTP (NIDS)
16	9:15:17:47	Series of packets between 60.3.4.5 and 1.17.8.40. SMTP (NIDS)
17	9:20:12:05	Packet from 60.3.4.5 to 60.0.1.1. TCP SYN=1, Destination Port 80 (NIDS)
18	9:20:12:07	Packet from 60.0.1.1 to 60.3.4.5. TCP RST=1, Source Port 80 (NIDS)
19	9:20:12:08	Packet from 60.3.4.5 to 60.0.1.2. TCP SYN=1, Destination Port 80 (NIDS)
20	9:20:12:11	Packet from 60.3.4.5 to 60.0.1.3. TCP SYN=1, Destination Port 80 (NIDS)
21	9:20:12:12	Packet from 60.0.1.3 to 60.3.4.5. TCP SYN=1; ACK=1, Source Port 80 (NIDS)

(a) Zidentyfikuj etapy tego pozornego ataku. (b) Dla każdego etapu opisz, co wydaje się robić napastnik. (c) Zdecyduj, czy działania na tym etapie działają z ludzką szybkością, czy z większą szybkością, co wskazuje na zautomatyzowany atak. (d) Zdecyduj, czy dowody na każdym etapie sugerują atak, czy też rozstrzygające dowody. (e) Ogólnie, czy masz rozstrzygające dowody ataku? (f) Czy masz rozstrzygające dowód, kto popełnił atak?

4. Firma stara się zdecydować, czy umieścić swoje centrum zapasowe w tym samym mieście, czy w odległym mieście. Wymień zalety i wady każdego wyboru.

5. Aby wyjść z egzaminów, uczniowie czasami dzwonią z groźbami bombowymi tuż przed egzaminem. Stwórz plan radzenia sobie z takimi atakami. Powinno to zająć jedną stronę z pojedynczym odstępem. Powinien być napisany przez ciebie (doradcę politycznego), aby twój dziekan mógł go zatwierdzić i opublikować w twojej uczelni.

6. Po przywróceniu plików po incydencie użytkownicy skarżą się, że brakuje niektórych plików danych. Co mogło się stać?