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?