ZABEZPIECZENIA E-COMMERCE I SERWERÓW WWW

WPROWADZENIE.

Dziś handel elektroniczny obejmuje całe przedsiębiorstwo. Najbardziej oczywiste aplikacje e-commerce obejmują transakcje biznesowe z klientami zewnętrznymi na urządzeniach mobilnych i w sieci WWW (WWW lub WWW), ale są one jedynie przysłowiowym wierzchołkiem góry lodowej. Obecność handlu elektronicznego stała się znacznie bardziej wszechobecna, często obejmując całe logistyczne i finansowe łańcuchy dostaw, które są podstawą współczesnego handlu. Nawet najmniejsze organizacje teraz polegają na Internecie, aby uzyskać dostęp do usług i informacji. Gwałtowny rozwój aplikacji mobilnych w ciągu ostatnich kilku lat spowodował głęboką integrację transakcji elektronicznych z minutą na minutę życia codziennego. Spacerując ulicą w dowolnym obszarze miejskim, urządzenia mobilne stały się wszechobecne. Narody, którym brakowało infrastruktury przewodowej, opuściły pokolenie technologiczne i przeszły bezpośrednio na infrastrukturę telekomunikacyjną opartą na technologiach telefonii komórkowej. Wszechobecne pragnienie poprawy wydajności często powoduje zbieżność między systemami obsługującymi konwencjonalne operacje z systemami wspierającymi biznes online organizacji. Dlatego też często systemy wewnętrzne w sklepach stacjonarnych wykorzystują te same systemy zaplecza, z których korzystają klienci Web. Często zdarza się, że kioski i kasy fiskalne wykorzystują bezprzewodowe sieci lokalne do nawiązywania połączeń z systemami wewnętrznymi. Te połączenia mogą zapewnić intruzom bezpośredni dostęp do serca przedsiębiorstwa. Sprawa TJX, na którą zwrócono uwagę opinii publicznej na początku 2007 r., Była jednym z serii włamań na dużą skalę do informacji przechowywanych elektronicznie w systemach back-office i e-commerce. Przede wszystkim wydaje się, że sprawa TJX rozpoczęła się od niedostatecznie zabezpieczonej sieci korporacyjnej i powiązanych systemów zaplecza, a nie od penetracji strony internetowej. Naruszenie to przerodziło się w naruszenie bezpieczeństwa korporacyjnych systemów danych. Zgłoszono, że co najmniej 94 miliony kart kredytowych zostało naruszonych. W dniu 30 listopada 2007 roku ogłoszono, że TJX, organizacja macierzysta sklepów, w tym TJ Maxx i Marshall's, zgodziła się uregulować roszczenia bankowe związane z kartami VISA na kwotę 40,9 mln USD. Handel elektroniczny osiągnął obecnie pełnoletność, stwarzając ryzyko powiernicze, które jest ważne dla kierownictwa wyższego szczebla i dla zarządu. Bezpieczeństwo sieci danych, zarówno tych używanych przez klientów, jak i tych używanych wewnętrznie, osiągnęło poziom, na którym znacząco wpływa na wynik finansowy. TJX ucierpiał zarówno pod względem finansowym, jak i public relations, a historie dotyczące szczegółów tej sprawy pojawiły się w Wall Street Journal, New York Times, Business Week i wielu branżowych publikacjach. Bezpieczeństwo danych nie jest już abstrakcyjną kwestią, którą interesuje się tylko personel techniczny. Rozliczenia prawne znacznie przekraczają koszty bezpośrednio związane z rozwiązaniem problemu technicznego. Ochrona informacji związanych z handlem elektronicznym wymaga wielopłaszczyznowego podejścia, obejmującego zasady i strategie biznesowe, a także kwestie techniczne lepiej znane specjalistom ds. Bezpieczeństwa informacji. W całym przedsiębiorstwie ludzie i informacje są fizycznie chronieni. Nawet najmniejsze organizacje mają zamknięte drzwi i recepcjonistkę, która powstrzymuje osoby postronne przed wejściem do lokalu. Im większa organizacja, tym dokładniejsze środki ostrożności. Małe firmy mają proste, zamknięte drzwi; Większe przedsiębiorstwa często mają wiele poziomów zabezpieczeń, w tym zamki elektroniczne, ochronę i dodatkowe poziomy recepcjonistów. Firmy zazdrośnie strzegą też prywatności rozmów kierowniczych i projektów badawczych. Pomimo tych norm nie jest niczym niezwykłym stwierdzenie, że praktyki bezpieczeństwa informacji są słabsze niż fizyczne środki bezpieczeństwa. Połączenie z Internetem (i wewnątrz firmy, z intranetem) pogarsza problem, znacznie zwiększając ryzyko i zmniejszając trudność ataków. Wszechobecne urządzenia mobilne tylko potęgują trudności.

POLITYKI I STRATEGIE BIZNESOWE.

W złożonym świecie bezpieczeństwa e-commerce najlepsze praktyki nieustannie ewoluują. Nowe protokoły i produkty są regularnie ogłaszane. Przed eksplozją Internetu większość firm rzadko udostępniała swoje dane i własne aplikacje jakimkolwiek zewnętrznym podmiotom, a bezpieczeństwo informacji nie było priorytetem. Obecnie firmy korzystające z handlu elektronicznego potrzebują solidnych architektur bezpieczeństwa dla praktycznie wszystkich zastosowań. Skuteczne bezpieczeństwo informacji stało się głównym problemem biznesowym. Tu przedstawiono elastyczne ramy do tworzenia bezpiecznych aplikacji handlu elektronicznego oraz pomoc w identyfikacji odpowiednich i wymaganych usług bezpieczeństwa. W celu ułatwienia dołączono pokazane przykłady teoretyczne zrozumienie przez czytelnika struktury w środowisku biznes-klient (B2C) i biznes-biznes (B2B). Rozsądne ramy bezpieczeństwa handlu elektronicznego to takie, które:

1. Definiuje obawy związane z bezpieczeństwem informacji specyficzne dla aplikacji.

2. Definiuje usługi bezpieczeństwa potrzebne do rozwiązania problemów związanych z bezpieczeństwem.

3. Wybiera usługi bezpieczeństwa na podstawie analizy kosztów i korzyści oraz kwestii ryzyka i zysku.

4. Zapewnia stałą uwagę na zmiany technologii i wymagań w miarę zmieniania się zarówno zagrożeń, jak i wymagań aplikacji.

To czteroetapowe podejście jest zalecane do zdefiniowania wyboru usług bezpieczeństwa i procesów decyzyjnych.

Krok 1: Zdefiniuj obawy dotyczące bezpieczeństwa informacji specyficzne dla podania.

Pierwszym krokiem jest zdefiniowanie lub opracowanie architektury aplikacji i klasyfikacji danych związanych z każdą transakcją. Ten krok dotyczy sposobu działania aplikacji. Z reguły, jeśli kwestie bezpieczeństwa zostaną zdefiniowane pod kątem wpływu na biznes, łatwiej będzie omówić je z kierownictwem i łatwiej będzie zdefiniować wymagania dotyczące bezpieczeństwa. Zalecanym podejściem jest opracowanie diagramu transakcyjnego śledzenia przepływu, który śledzi transakcje i typy danych na różnych serwerach i sieciach. Powinien to być funkcjonalny i logiczny obraz tego, jak aplikacja będzie działać, czyli jak będą przebiegać transakcje, jakie systemy będą uczestniczyć w zarządzaniu transakcjami i gdzie te systemy będą wspierać cele biznesowe i łańcuch wartości produktu w organizacji. Należy zidentyfikować źródła danych i interfejsy danych, a przetwarzane informacje należy sklasyfikować. W ten sposób można przedstawić pełny przepływ transakcji.

Typowe punkty architektury warstwowej obejmują:

* Klienci. Mogą to być komputery PC, cienkie klienty (urządzenia, które korzystają ze współużytkowanych aplikacji z serwera i mają niewielką ilość pamięci), osobiste asystenty cyfrowe (PDA) i telefony obsługujące protokół aplikacji bezprzewodowych (WAP).

* Serwery. Mogą to być procesory WorldWideWeb, aplikacji, baz danych i oprogramowania pośredniego, a także serwery zaplecza i starsze systemy.

* Urządzenia sieciowe. Przełączniki, routery, zapory sieciowe, karty sieciowe, kodeki, modemy oraz wewnętrzne i zewnętrzne witryny hostingowe.

* Przestrzenie sieciowe. Strefy zdemilitaryzowane sieci (DMZ), intranety, ekstranety i Internet.

Na tym etapie procesu ważne jest, aby zidentyfikować krytyczność aplikacji dla firmy i nadrzędne kwestie związane z bezpieczeństwem: poufność transakcji, integralność transakcji lub dostępność transakcyjną. Zdefiniowanie tych kwestii bezpieczeństwa pomoże uzasadnić usługi bezpieczeństwa wybrane do ochrony systemu. Im dokładniej można opisać architekturę, tym dokładniej można chronić informacje za pomocą usług bezpieczeństwa.

Krok 2: Opracuj opcje usług bezpieczeństwa.

Drugi krok dotyczy alternatywnych usług bezpieczeństwa dla każdego komponentu architektury i danych związanych z każdą transakcją. Każdy komponent architektoniczny i punkt danych powinien zostać przeanalizowany i dla każdego zdefiniowane możliwe usługi bezpieczeństwa. Na tym etapie nie należy w znacznym stopniu rozważać kosztów i wykonalności. Celem jest stworzenie pełnej listy opcji usług ochrony z uwzględnieniem wszystkich alternatyw. Proces powinien być porównywalny z burzą mózgów lub wykorzystywać te same techniki, co burza mózgów. Należy uwzględnić wszystkie pomysły, nawet jeśli niepraktyczne lub naciągane. Na tym etapie nie należy podejmować decyzji; proces ten jest zarezerwowany dla kroku 3. Organizacja zajmująca się bezpieczeństwem informacji świadczy usługi na rzecz przedsiębiorstwa. Usługi świadczone przez organizacje zajmujące się bezpieczeństwem informacji różnią się w zależności od firmy. Wymagane usługi będą zależeć od kilku czynników, ale najważniejsze z nich to:

* Czynniki branżowe

* Apetyt firmy na ryzyko

* Dojrzałość funkcji bezpieczeństwa

* Podejście organizacyjne (scentralizowane lub zdecentralizowane)

* Wpływ poprzednich incydentów bezpieczeństwa

* Wewnętrzne czynniki organizacyjne

* Czynniki polityczne

* Czynniki regulacyjne

* Postrzegana strategiczna wartość bezpieczeństwa informacji

Na usługi świadczone przez organizacje zajmujące się bezpieczeństwem informacji składa się kilka czynników. „Usługi bezpieczeństwa" definiuje się jako zabezpieczenia i środki kontrolne mające na celu ochronę poufności, integralności i odpowiedzialności za informacje i zasoby komputerowe. Usługi bezpieczeństwa wymagane do zabezpieczenia transakcji handlu elektronicznego muszą opierać się na wymaganiach biznesowych i chęci przyjęcia lub ograniczenia ryzyka naruszenia bezpieczeństwa informacji. Specjaliści ds. Bezpieczeństwa informacji mogą być ekspertami merytorycznymi, ale rzadko są przygotowani do podejmowania decyzji biznesowych wymaganych przy wyborze niezbędnych usług. Zidentyfikowano dwanaście usług bezpieczeństwa, które mają kluczowe znaczenie dla skutecznego bezpieczeństwa handlu elektronicznego:

1. Polityka i procedury to usługa bezpieczeństwa, która definiuje poziom bezpieczeństwa informacji, którego wymaga organizacja i sposób, w jaki będzie on wdrażany. Skuteczna polityka i procedury będą współgrały ze strategią, rozwojem, wdrażaniem i obsługą systemu. Każda organizacja będzie miała inne zasady i procedury; najlepsza praktyka mówi, że organizacje mają zasady i procedury oparte na ryzyku, jakie organizacja jest gotowa podjąć w związku ze swoimi informacjami. Organizacje powinny

przynajmniej posiadać politykę wysokiego szczebla, która dyktuje właściwe wykorzystanie zasobów informacyjnych i konsekwencje nadużycia.

2. Poufność i szyfrowanie to usługi bezpieczeństwa, które zabezpieczają dane podczas ich przechowywania lub przesyłania z jednego komputera do drugiego. Istnieje wiele schematów i produktów szyfrowania; każda organizacja musi zidentyfikować produkty, które najlepiej integrują się z wdrażaną aplikacją. Omówienie kryptografii znajduje się w rozdziałach 7 i 37 niniejszego podręcznika.

3. Uwierzytelnianie i identyfikacja to usługa bezpieczeństwa, która rozróżnia użytkowników i weryfikuje, czy są tym, za kogo się podają. Zazwyczaj używane są hasła, ale silniejsze metody obejmują tokeny, karty inteligentne i dane biometryczne. Te silniejsze metody weryfikują to, co masz (np. Token) lub kim jesteś (np. Dane biometryczne), a nie tylko to, co wiesz (hasło). Uwierzytelnianie dwuskładnikowe łączy dwie z tych trzech metod i jest określane jako silne uwierzytelnianie. Więcej informacji na ten temat można znaleźć w rozdziale 28 tego podręcznika.

4. Autoryzacja określa, jakich uprawnień dostępu potrzebuje użytkownik w systemie. Dostęp obejmuje dane, system operacyjny, funkcje transakcyjne i procesy. Dostęp powinien zostać zatwierdzony przez kierownictwo, które jest właścicielem systemu lub go rozumie, przed udzieleniem dostępu. Upoważnieni użytkownicy powinni mieć dostęp tylko do informacji, których potrzebują do swojej pracy.

5. Autentyczność to usługa bezpieczeństwa, która weryfikuje transakcję i wiąże transakcję z jedną odpowiedzialną osobą lub podmiotem. Nazywana również niezaprzeczalnością, autentyczność zapewnia, że dana osoba nie może kwestionować szczegółów transakcji. Jest to szczególnie przydatne w przypadku umów i celów prawnych.

6. Monitorowanie i audyt zapewniają elektroniczną ścieżkę historycznego zapisu transakcji. Dzienniki inspekcji składają się z dzienników systemu operacyjnego, dzienników transakcji aplikacji, dzienników bazy danych i dzienników ruchu sieciowego. Monitorowanie tych dzienników pod kątem nieautoryzowanych zdarzeń jest uważane za najlepsze rozwiązanie.

7. Kontrola dostępu i wykrywanie włamań to usługi techniczne, fizyczne i administracyjne, które zapobiegają nieautoryzowanemu dostępowi do sprzętu, oprogramowania lub informacji. Dane są chronione przed modyfikacją, kradzieżą lub zniszczeniem. Kontrole dostępu zapobiegają wystąpieniu nieuprawnionego dostępu. Wykrywanie włamań wykrywa nieautoryzowany dostęp po jego wystąpieniu, dzięki czemu można zminimalizować szkody i odciąć dostęp. Kontrole te są szczególnie konieczne, gdy przetwarzane są informacje poufne lub krytyczne.

8. Zaufana komunikacja to usługa bezpieczeństwa, która zapewnia, że komunikacja jest bezpieczna. W większości przypadków związanych z Internetem oznacza to, że komunikacja będzie szyfrowana. W przeszłości komunikacja cieszyła się zaufaniem, ponieważ znajdowała się w granicach organizacji. Komunikacja jest obecnie wszechobecna i może pochodzić z dowolnego miejsca, w tym z ekstranetu i Internetu.

9. Antywirus to usługa bezpieczeństwa, która zapobiega, wykrywa i usuwa wirusy, konie trojańskie i inne złośliwe oprogramowanie.

10. Kontrole integralności systemu to usługi bezpieczeństwa, które pomagają zapewnić, że system nie został zmieniony lub naruszony przez nieuprawniony dostęp.

11. Zatrzymywanie i usuwanie danych to usługa bezpieczeństwa, która archiwizuje wymagane informacje lub usuwa dane, gdy nie są już potrzebne. Dostępność zatrzymanych danych ma kluczowe

znaczenie w sytuacji awaryjnej. Dzieje się tak niezależnie od tego, czy problemem jest awaria systemów, czy proces prawny, czy to spowodowany klęską żywiołową, czy atakiem terrorystycznym.

12. Klasyfikacja danych to usługa bezpieczeństwa, która określa wrażliwość i poufność informacji. Usługa zawiera przewodniki dotyczące etykietowania informacji i ochrony w trakcie życia informacji. Po zidentyfikowaniu aplikacji handlu elektronicznego zespół musi zidentyfikować problemy związane z bezpieczeństwem tej konkretnej aplikacji i niezbędne usługi bezpieczeństwa. Nie wszystkie usługi będą odpowiednie, ale użycie pełnej listy i wykluczenie tych, które nie są wymagane, zapewni kompleksową ocenę wymagań, z odpowiednim zabezpieczeniem wbudowanym w rozwój systemu. W rzeczywistości kierownictwo może pogodzić zaakceptowane usługi z poziomem akceptacji ryzyka.

Krok 3: Wybierz opcje usług bezpieczeństwa w oparciu o wymagania.

Trzeci krok wykorzystuje klasyczne techniki analizy kosztów i korzyści oraz zarządzania ryzykiem, aby dokonać ostatecznego wyboru opcji usług bezpieczeństwa. Zalecamy jednak, aby wszystkie opcje zidentyfikowane w kroku 3 były rozmieszczone wzdłuż kontinuum, tak jak pokazano na Rysunku 30.2, tak aby można je było przeglądać razem i porównywać. Pomiar i porównanie poziomu bezpieczeństwa dla każdej usługi bezpieczeństwa i danych w ramach transakcji ułatwi proces decyzyjny. Następnie można zidentyfikować wykonalne alternatywy i wybrać najlepsze rozwiązanie w oparciu o wymagania. Najważniejszym elementem do rozważenia jest względne zmniejszenie ryzyka każdej opcji w porównaniu z innymi alternatywami. Analiza kosztów i korzyści opiera się na kwestiach ryzyka i nagrody. Informacje o skuteczności są bardzo przydatne w modelu kosztów i korzyści. Cztery dodatkowe koncepcje decydują o wyborze opcji usługi bezpieczeństwa:

1. Ryzyko lub wykonalność wdrożenia

2. Koszt wdrożenia i wsparcia

3. Skuteczność w zwiększaniu kontroli, a tym samym zmniejszaniu ryzyka

4. Klasyfikacja danych

Ryzyko wdrożeniowe dotyczy możliwości wdrożenia opcji usługi bezpieczeństwa. Niektóre systemy zabezpieczeń są trudne do wdrożenia ze względu na takie czynniki, jak dojrzałość produktu, skalowalność, złożoność i możliwość obsługi. Inne czynniki do rozważenia to dostępne umiejętności, kwestie prawne, wymagana integracja, możliwości, wcześniejsze doświadczenie i ograniczenia technologii.

Koszt wdrożenia i wsparcia mierzy koszty wdrożenia sprzętu i oprogramowania, wsparcia i administracji. Rozważenie kwestii administracyjnych jest szczególnie krytyczne, ponieważ wsparcie usług bezpieczeństwa na wysokim poziomie ma kluczowe znaczenie dla sukcesu organizacji.

Skuteczność mierzy redukcję ryzyka proponowaną przez opcję usługi ochroniarskiej już w produkcji. Ryzyko można zdefiniować jako wpływ i prawdopodobieństwo wystąpienia negatywnego zdarzenia po wdrożeniu strategii łagodzących. Przykładem negatywnego zdarzenia jest kradzież numerów kart kredytowych z firmowej bazy danych. Takie zdarzenie powoduje nie tylko możliwe straty dla konsumentów, ale także negatywne relacje public relations, które mogą wpłynąć na przyszły biznes. Skuteczne opcje usług ochrony zmniejszają ryzyko wystąpienia negatywnego zdarzenia.

Klasyfikacja danych mierzy wrażliwość i poufność przetwarzanych informacji. Dane muszą być klasyfikowane i chronione przed niewłaściwym wykorzystaniem, ujawnieniem, kradzieżą lub zniszczeniem, niezależnie od formatu przechowywania, przez cały okres ich życia (od stworzenia do zniszczenia). Zwykle twórca informacji jest uważany za właściciela informacji i jest odpowiedzialny za

klasyfikację, identyfikację i etykietowanie. Im bardziej wrażliwe i poufne są informacje, tym więcej środków bezpieczeństwa informacji będzie potrzebnych do ich zabezpieczenia i ochrony.

Krok 4: Zapewnia ciągłą uwagę na zmiany technologii i wymagań.

Jedynym stałym elementem tej analizy jest potrzeba rozwoju i radzenia sobie z coraz większymi zagrożeniami i technologiami. Niezależnie od tego, jakie podejście do bezpieczeństwa zidentyfikowano w poprzednich krokach, należy je zawsze rozważać w kontekście ciągłej potrzeby aktualizowania wybranych podejść. Zmiany będą nieuniknione, niezależnie od tego, czy wynikną z zgodności, regulacji, postępu technologicznego, czy nowych zagrożeń.

Korzystanie z struktury usług bezpieczeństwa.

Kolejne dwie sekcje to przykłady pokazujące siłę metodologii usług bezpieczeństwa. Pierwszy przykład to model B2C; biznesem może być każda aplikacja do sprzedaży bezpośredniej. Drugi przykład to model B2B. Obie firmy wykorzystują Internet aby ulepszyć swój łańcuch wartości produktu. Przykłady są krótką demonstracją metodologii usług bezpieczeństwa, nie są kompletne ani reprezentatywne dla żadnej konkretnej aplikacji lub firmy.

Usługi w zakresie bezpieczeństwa dla klientów. Firma B2C

pragnie kontaktować się z klientami bezpośrednio przez Internet i umożliwić im wprowadzenie swoich danych do aplikacji. Poniższe założenia zostały przyjęte w celu przygotowania tego przykładu systemu B2C:

* Firma korzystająca z Internetu

* Obsługiwane główne transakcje

* Zewnętrzny system oparty na kliencie, w szczególności z wyłączeniem wsparcia, administracji i operacji

* Aplikacja o znaczeniu krytycznym dla biznesu

* Bardzo wrażliwa klasyfikacja danych

* Architektura trójwarstwowa

* Niezaufani klienci, ponieważ każdy w Internecie może być klientem

Należy zabezpieczyć pięć warstw:

1. Warstwa prezentacji to interfejs klienta, czyli to, co klient widzi lub słyszy na urządzeniu internetowym. Klient to niezaufany komputer lub inne urządzenie klienta. Wymagania bezpieczeństwa na tym poziomie są minimalne, ponieważ firma zwykle nie narzuca klientowi bezpieczeństwa. Identyfikacja i uwierzytelnienie wykonywane na poziomie prezentacji to kontrole związane z dostępem do urządzenia. Mnożenie się urządzeń w przestrzeni klienta (np. Tradycyjne komputery PC, cienkie komputery stacjonarne i PDA) utrudnia ustanowienie jednolitej procedury kontroli dostępu na tym poziomie. Chociaż ta warstwa jest końcowym punktem końcowym bezpiecznego połączenia, nie jest z natury godna zaufania, co zostało zilustrowane przez aż nazbyt wiele incydentów z udziałem komputerów publicznych w kawiarniach, hotelach i innych miejscach.

2. Warstwa sieciowa to połączenie komunikacyjne między firmą a klientem. Klient lub klient korzysta z połączenia internetowego, aby uzyskać dostęp do aplikacji B2CWeb. Wymagania dotyczące bezpieczeństwa są minimalne, ale wrażliwe, a ruch poufny będzie musiał być szyfrowany.

3. Warstwa środkowa to serwer WWW, który łączy się z przeglądarką klienta i może przekazywać i odbierać informacje. Serwer WWW wspiera aplikację będąc pośrednikiem pomiędzy biznesem a klientem. Serwer WWW musi być bardzo bezpieczny. Należy zapobiegać kradzieży, fałszowaniu i oszukańczemu wykorzystaniu informacji. Do typowych zagrożeń, którym należy zapobiegać w warstwie środkowej, należą również odmowa usługi i niszczenie witryn internetowych.

4. Warstwa aplikacji to miejsce, w którym przetwarzane są informacje. Aplikacja służy jako pośrednik między żądaniami klientów a systemami realizacji zamówień wewnątrz firmy. W niektórych przykładach serwer aplikacji i serwer bazy danych są takie same, ponieważ zarówno aplikacja, jak i baza danych znajdują się na tym samym serwerze. Jednak w innych przypadkach mogą znajdować się na serwerze WWW.

5. Warstwa wewnętrzna składa się ze starszych systemów biznesowych i baz danych, które wspierają obsługę klienta. Serwery zaplecza zawierają aplikacje wspierające, w tym przetwarzanie zamówień, należności, zapasy, dystrybucję i inne systemy.

Dla każdego z tych pięciu poziomów potrzebujemy czterech usług bezpieczeństwa:

1. Zaufana komunikacja

2. Uwierzytelnienie / identyfikacja

3. Audyt

4. Kontrola dostępu

Krok 1: Zdefiniuj obawy dotyczące bezpieczeństwa informacji specyficzne dla aplikacji.

Zdefiniowanie zagadnień bezpieczeństwa będzie dotyczyło wdrażanego systemu. Aby zrozumieć ryzyko systemu, najlepiej zacząć od ryzyka biznesowego; następnie zdefiniowanie zagrożeń dla każdego elementu architektury.

Ryzyko biznesowe

* Aplikacja wymaga wysokiej dostępności, ponieważ klienci będą żądać kontaktu poza godzinami pracy oraz w weekendy.

* Strony internetowe muszą być zabezpieczone przed manipulacją i cyberwandalizmem, ponieważ firma obawia się utraty zaufania klientów w wyniku negatywnej reklamy.

* Klienci muszą być zadowoleni z poziomu usług.

* System będzie przetwarzał dane karty kredytowej klienta i będzie podlegał przepisom o ochronie prywatności zawartym w ustawie Gramm-Leach-Bliley, 15 USC §§ 6801–09.

Obawy technologiczne

Z pięciu warstw architektonicznych w tym przykładzie należy zabezpieczyć cztery:

1. Warstwa prezentacji nie będzie zabezpieczona ani zaufana. Komunikacja między klientem a serwerem sieci Web będzie szyfrowana w warstwie sieciowej.

2. Warstwa sieciowa będzie musiała filtrować niepożądany ruch, zapobiegać atakom typu „odmowa usługi” (DoS) i monitorować ewentualne włamania.

3. Warstwa środkowa będzie musiała zapobiegać nieautoryzowanemu dostępowi, być odporna na manipulacje, zawierać skuteczny monitoring oraz wspierać wydajne i efektywne przetwarzanie.

4. Warstwa aplikacji będzie musiała zapobiegać nieautoryzowanemu dostępowi, wspierać terminowe przetwarzanie transakcji, zapewniać skuteczne ścieżki audytu i przetwarzać informacje poufne.

5. Warstwa wewnętrzna będzie musiała zapobiegać nieautoryzowanemu dostępowi, zwłaszcza poprzez połączenia internetowe, oraz chronić poufne informacje podczas transmisji, przetwarzania i przechowywania.

Krok 2: Opracuj opcje usług bezpieczeństwa.

Cztery usługi bezpieczeństwa omówione w tym przykładzie są najbardziej krytyczne w środowisku handlu elektronicznego. Inne usługi, takie jak niezaprzeczalność i klasyfikacja danych, są ważne, ale nie zostały uwzględnione w celu uproszczenia przykładu. Wybrane usługi to:

* Zaufana komunikacja

* Uwierzytelnianie i identyfikacja

* Monitorowanie i audyt

* Kontrola dostępu

W przypadku B2C dostępnych jest wiele opcji usług bezpieczeństwa, a na horyzoncie pojawia się więcej produktów i protokołów. Istnieje pięć warstw architektonicznych dla każdej usługi zdefiniowanej w kroku 1.

1. Warstwa prezentacji. Można wybrać kilka różnych opcji zaufanej komunikacji. Chociaż najpopularniejszym protokołem na poziomie aplikacji jest Hypertext Transfer Protocol (HTTP); stale rosnące zapotrzebowanie na prywatność i zapewnienie integralności przemawia za korzystaniem z jego bezpieczniejszego, zaszyfrowanego rodzeństwa, Transport Layer Security, następcy protokołu Secure Socket Layer (SSL), 4 w połączeniu

z certyfikatami w infrastrukturze klucza publicznego (PKI) w celu uwierzytelnienia i kryptograficznego zabezpieczenia ścieżki komunikacyjnej. Użycie lub ewentualne użycie połączeń bezprzewodowych gdzieś na ścieżce tylko zwiększa znaczenie zabezpieczonych, zaszyfrowanych ścieżek. Ponieważ klient nie jest zaufany, nie można polegać na jego metodach uwierzytelniania, audytu lub kontroli dostępu.

2. Warstwa sieciowa. Wirtualne sieci prywatne (VPN) są uważane za najlepsze praktyki w zakresie bezpiecznej komunikacji w warstwie sieciowej. Zapory to skuteczne urządzenia do zabezpieczania komunikacji sieciowej. Klient może mieć osobistą zaporę ogniową. Jeśli klient jest w dużej korporacji, istnieje duże prawdopodobieństwo, że zapora sieciowa będzie zakłócać komunikację. Jeśli klient korzysta z komputera domowego lub laptopa, ruch może chronić osobista zapora ogniowa. Po stronie firmy B2C w Internecie będzie również zapora ogniowa.

3. Warstwa środkowa. Serwer WWW i wymagania bezpieczeństwa serwera aplikacji są istotne. Nieautoryzowany dostęp do serwera internetowego może spowodować zniszczenie witryny przez hakerów, którzy zmienią dane w sieci. Co ważniejsze, dostęp do sieci WWW lub serwera aplikacji może prowadzić do kradzieży, manipulacji lub usunięcia danych klienta lub zastrzeżonych danych. Komunikacja pomiędzy serwerem Web a klientem musi być bezpieczna w transakcjach e-commerce. HTTP to najpowszechniejsza forma komunikacji przeglądarki. W 2000 roku zgłoszono, że ponad 33 procent transakcji dokonywanych przy użyciu kart kredytowych odbywało się przy użyciu niezabezpieczonego protokołu HTTP.5 W 2007 roku firma VISA poinformowała, że zgodność ze

standardem Payment Card Industry Data Security Standard (PCI DSS) poprawiła się do 77 procent największych sprzedawców w Stany Zjednoczone, 6 wciąż dalekie od uniwersalności. Ten brak szyfrowania stanowi naruszenie zarówno umowy handlowej, jak i PCI, ale epizody nadal się zdarzają. Z tego samego powodu organizacje nierzadko nadużywają szyfrowania, niezależnie od tego, czy dotyczy ono certyfikatów podpisanych przez siebie, wygasłych, czy też nieuznanych ogólnie. (Patrz rozdział 37 w tym podręczniku). HTTPS (HTTP przez TLS) jest najpowszechniejszym bezpiecznym rozwiązaniem protokołu, ale długość i zawartość klucza szyfrowania są krytyczne: im większy klucz, tym bezpieczniejsza jest transakcja przed odszyfrowaniem siłowym (patrz rozdział 7). Certyfikaty cyfrowe w PKI i podpisy cyfrowe nie są tak powszechne, ale są skuteczniejszymi formami zabezpieczeń.

4. Warstwa aplikacji. Serwer aplikacji zapewnia główne przetwarzanie dla serwera WWW. Ta warstwa może obejmować przetwarzanie transakcji i aplikacje bazodanowe; musi być bezpieczny, aby zapobiec błędnemu lub oszukańczemu przetwarzaniu. W zależności od wrażliwości przetwarzanych informacji dane mogą wymagać zaszyfrowania. Przechwytywanie i nieuprawniona manipulacja danymi to największe zagrożenia w warstwie aplikacji.

5. Warstwa wewnętrzna. W typowym przykładzie warstwa wewnętrzna jest zabezpieczona zaporą ogniową chroniącą system skierowany na zewnątrz. Ten firewall pomaga firmie B2C chronić się przed włamaniami do Internetu. Wymagane są hasła do baz danych i systemu operacyjnego oraz środki kontroli dostępu.

Kierownictwo może zdecydować, która funkcja bezpieczeństwa jest wymagana i na jakim poziomie. Ten format można powtórzyć, aby omówić usługi bezpieczeństwa na wszystkich poziomach i wszystkich systemach, a nie tylko systemy związane z handlem elektronicznym

Krok 3: Wybierz opcje usług bezpieczeństwa na podstawie wymagań.

W kroku 3 firma B2C może przeanalizować i wybrać usługi bezpieczeństwa, które najlepiej spełniają jej wymagania prawne, biznesowe i bezpieczeństwa informacji. Analiza ta wymaga czterech etapów:

1. Ryzyko lub wykonalność wdrożenia

2. Koszt wdrożenia i wsparcia

3. Skuteczność w zwiększaniu kontroli, a tym samym zmniejszaniu ryzyka

4. Klasyfikacja danych

Ryzyko wdrożeniowe jest funkcją zdolności organizacji do skutecznego wprowadzenia technologii. W tym przykładzie zakładamy, że ryzyko wdrożenia jest niskie, a zasoby są łatwo dostępne do wdrożenia technologii. Koszty wdrożenia i wsparcia mają nadrzędne znaczenie w procesie podejmowania decyzji. Oba koszty należy rozpatrywać łącznie. Niestety koszt wsparcia jest trudny do oszacowania i łatwo przeoczony. W tym przykładzie dostępne są zasoby zarówno do wdrażania, jak i do obsługi technologii. Skuteczność w zwiększaniu kontroli jest integralną częścią decyzji dotyczących korzyści i zarządzania ryzykiem. Należy wziąć pod uwagę każdy element, aby określić wzajemne korzyści w przypadku nakładania się kontroli i uzupełniać inne kontrole. W tym przypadku wzrost kontroli jest rozumiany i wspierany przez kierownictwo. Klasyfikacja danych jest podstawą wymagań. Pomoże to w prowadzeniu dyskusji na temat kosztów i korzyści, ponieważ oddają wartość informacji dla podstawowej działalności. W tym przykładzie dane są uważane za wystarczająco istotne, aby uzasadnić dodatkowe środki bezpieczeństwa w celu ochrony danych przed niewłaściwym wykorzystaniem, kradzieżą i utratą.

Aby zabezpieczyć przykładowe środowisko, potrzeba wielu decyzji technologicznych. Kierownictwo może zastosować to podejście do wykreślenia poziomów ochrony wymaganych przez system. Na przykład w przypadku usług audytu systemu w kolejności od minimalnej do maksymalnej:

* Minimalny poziom bezpieczeństwa to rejestrowanie systemów z ograniczoną liczbą zdarzeń systemowych. Na przykład używany jest domyślny poziom rejestrowania od producenta, ale nie zawiera wszystkich wymaganych informacji. Dzienniki nie są przeglądane, ale są dostępne do celów śledczych w przypadku incydentu związanego z bezpieczeństwem.

* Wyższy poziom bezpieczeństwa zapewnia dziennik, który rejestruje więcej działań w oparciu o wymagania, a nie, na przykład, domyślny poziom producenta. Podobnie jak w przypadku minimalnego poziomu bezpieczeństwa, działania są rejestrowane i dostępne w celu wsparcia kryminalistyki, ale nie są przeglądane. W takim przypadku w dzienniku systemowym zapisywanych jest więcej typów informacji, ale nadal mogą one nie zawierać wszystkiego, co jest wymagane.

* Odpowiedni dziennik jest przechowywany na każdym serwerze i jest ręcznie monitorowany pod kątem anomalii i potencjalnych zdarzeń związanych z bezpieczeństwem.

* Dziennik jest automatycznie przeglądany przez oprogramowanie na każdym serwerze.

* Dzienniki systemowe są konsolidowane na scentralizowanym serwerze bezpieczeństwa. Dane z dzienników systemowych są przesyłane do scentralizowanego serwera bezpieczeństwa, a oprogramowanie jest następnie używane do skanowania dzienników w poszukiwaniu określonych zdarzeń, które wymagają uwagi. Zdarzenia, takie jak próby uzyskania eskalowanych uprawnień administratora lub dostępu administratora, można oznaczać do ręcznego przeglądu.

* Maksymalny poziom usług to oparty na hoście system wykrywania włamań (IDS) używany do skanowania dzienników systemowych w poszukiwaniu anomalii i możliwych zdarzeń związanych z bezpieczeństwem. Po wykryciu włamania należy podjąć działania. Procedura powinna obejmować takie procesy, jak powiadomienie, eskalacja i automatyczna reakcja obronna.

Usługi bezpieczeństwa dla firm.

Drugie studium przypadku wykorzystuje strukturę usług bezpieczeństwa w przykładzie B2B. Poniżej znajduje się teoretyczna dyskusja na temat tego, jak ramy można zastosować do bezpieczeństwa handlu elektronicznego B2B. W tym przykładzie systemu B2B można przyjąć następujące założenia:

* Połączenie z Internetem.

* Obsługuje duże transakcje.

* Opisy będą dotyczyły podmiotów zewnętrznych i klientów (z wyłączeniem usług wsparcia, administracji i bezpieczeństwa operacji).

* Wymagana jest zaufana komunikacja.

* Architektura trzywarstwowa.

* Niezaufany klient.

* Aplikacja o znaczeniu krytycznym dla biznesu.

* Dane są klasyfikowane jako bardzo wrażliwe

W tym przykładzie jest pięć warstw, które należy zabezpieczyć:

1. Warstwa prezentacji to interfejs klienta i to, co klient widzi lub słyszy za pomocą urządzenia Web. Klient jest niezaufanym komputerem klienta, ale można zastosować więcej ograniczeń bezpieczeństwa, ponieważ firma może narzucić większe bezpieczeństwo. Jak wspomniano wcześniej, bezpieczeństwo warstwy prezentacji jest skomplikowane ze względu na szeroką gamę potencjalnych urządzeń klienckich, które można zastosować.

2. Warstwa aplikacji to miejsce, w którym przetwarzane są informacje. Aplikacja służy jako pośrednik między żądaniami klienta biznesowego a systemami realizacji wewnątrz firmy (serwer zaplecza). Serwer aplikacji jest serwerem pomocniczym i bazą danych.

3. Warstwa wewnętrzna klienta to interfejs między serwerem aplikacji obsługującym system w lokalizacji biznesowej klienta a własnymi wewnętrznymi starszymi aplikacjami i systemami klienta.

4. Warstwa sieciowa to połączenie komunikacyjne między firmą a inną firmą. Do połączenia obu firm wykorzystywany jest Internet. Wrażliwy i poufny ruch będzie musiał być szyfrowany. Najlepszą praktyką jest dalsze zabezpieczenie ruchu za pomocą zapory.

5. Warstwa wewnętrzna to starsze systemy firmy, które wspierają obsługę klienta. Serwer zaplecza zawiera systemy pomocnicze, w tym przetwarzanie zamówień, należności, zapasy, dystrybucję i inne systemy. Cztery usługi bezpieczeństwa to:

1. Zaufana komunikacja

2. Uwierzytelnienie / identyfikacja

3. Audyt

4. Kontrola dostępu

Krok 1: Zdefiniuj obawy dotyczące bezpieczeństwa informacji specyficzne dla aplikacji.

Zdefiniowanie zagadnień bezpieczeństwa będzie dotyczyło wdrażanego systemu. Aby zrozumieć ryzyko systemu, najlepiej zacząć od ryzyka biznesowego; następnie zdefiniuj ryzyko dla każdego elementu architektury.

Ryzyko biznesowe

* Komunikacja między serwerami aplikacji musi być bardzo bezpieczna. Danych nie wolno modyfikować, kradzić ani źle przekierowywać.

* Dostępność jest krytyczna w normalnych godzinach pracy.

* Oszczędności kosztów uzyskane dzięki przejściu z elektronicznej wymiany danych (EDI) na Internet są znaczne i z nawiązką pokryją koszty systemu.

Obawy technologiczne

W tym przykładzie występuje sześć warstw architektonicznych, z których pięć należy zabezpieczyć:

1. Warstwa prezentacji nie będzie zabezpieczona ani zaufana. Komunikacja między klientem a aplikacją klienta jest zaufana, ponieważ wykorzystuje prywatną sieć klienta.

2. Serwer aplikacji musi być bezpieczny. Ruch między dwoma serwerami aplikacji będzie musiał być szyfrowany. Serwer aplikacji znajduje się w sieci klienta i wykazuje potencjalnie wysoki i być może niepotrzebny poziom zaufania między obiema firmami.

3. Warstwa wewnętrzna klienta zostanie zabezpieczona przez klienta.

4. Warstwa sieciowa musi odfiltrowywać ruch, który nie jest wymagany, zapobiegać atakom DoS i monitorować możliwe włamania. Pokazane są dwie zapory: jedna do ochrony klienta, a druga do ochrony firmy B2B.

5. Warstwa aplikacji będzie musiała zapobiegać nieautoryzowanemu dostępowi, wspierać terminowe przetwarzanie transakcji, zapewniać skuteczne ścieżki audytu i przetwarzać informacje poufne.

6. Warstwa wewnętrzna będzie musiała zapobiegać nieautoryzowanemu dostępowi (zwłaszcza przez połączenia internetowe) i chronić poufne informacje podczas transmisji, przetwarzania i przechowywania

Krok 2: Opracuj opcje usług bezpieczeństwa.

W tym przykładzie omówiono cztery usługi bezpieczeństwa. Można było uwzględnić inne, takie jak autentyczność, niezaprzeczalność i poufność, ale zostały one wykluczone, aby uprościć ten przykład.

Wybrane usługi bezpieczeństwa obejmują:

1. Zaufana komunikacja

2. Uwierzytelnienie / identyfikacja

3. Audyt

4. Kontrola dostępu

W środowiskach B2B dostępnych jest wiele opcji usług bezpieczeństwa.

* Warstwa prezentacji. Do komunikacji można wybrać kilka różnych opcji. Najpopularniejszy jest protokół HTTP. Komunikacja między warstwą prezentacji znajdującą się na urządzeniu klienckim a serwerem aplikacji, w tym przykładzie, ma charakter wewnętrzny zaufanej sieci wewnętrznej klienta i jest przez niego zabezpieczona. Wcześniejsze odcinki z tym scenariuszem obejmują wspomnianą wcześniej sprawę TJX i odcinek z udziałem Hannaford. Niedawno sieć sklepów spożywczych Bashas w Arizonie została zaatakowana przez złośliwe oprogramowanie w sieci punktów sprzedaży. Te kompromisy w sieciach wewnętrznych przemawiają za wykorzystaniem protokołu HTTPS (HTTP przez TLS) jako warstwy prezentacji, nawet w sieciach „wewnętrznych", w których przesyłane informacje mogą zawierać dane osobowe (PII) w jakiejś formie. Ze względów bezpieczeństwa, w przypadku wątpliwości, o wiele bezpieczniej jest uruchomić zaszyfrowaną infrastrukturę jako zabezpieczenie przed ujawnieniem informacji umożliwiających identyfikację, niż później odkryć, że niektóre dane w pewnych okolicznościach są chronione. Szyfrowanie niewrażliwych danych generuje nadmierne koszty; niezaszyfrowanie nawet niewielkiej ilości danych osobowych może prowadzić do znacznych zobowiązań.

* Warstwa aplikacji. Komunikacja między dwoma serwerami aplikacji musi być bezpieczna. Najłatwiejszą i najbezpieczniejszą metodą komunikacji peer-to-peer jest sieć VPN.

* Klient wewnętrzny. Komunikacja między serwerem aplikacji klienta a serwerem zaplecza klienta odbywa się wewnątrz zaufanej sieci wewnętrznej klienta i jest przez niego zabezpieczona.

* Warstwa sieci. W środowisku B2B często zdarza się, że zaufana sieć jest tworzona za pośrednictwem sieci VPN. Zapory prawdopodobnie będą uczestniczyć w tej komunikacji, ale możliwe są również rozwiązania sprzętowe.

* Warstwa aplikacji. Serwer aplikacji znajduje się zarówno w siedzibie klienta, jak i firmy B2B. VPN to najbezpieczniejsza metoda komunikacji. Serwer aplikacji musi również komunikować się z warstwą wewnętrzną i ten ruch również powinien być szyfrowany.

* Warstwa wewnętrzna. Warstwę wewnętrzną można zabezpieczyć inną zaporą ogniową z systemu zewnętrznego. Ta zapora sieciowa pomaga firmie B2B chronić się przed włamaniami i nieautoryzowanym dostępem. W tym przykładzie nie zakłada się zapory, więc zewnętrzna zapora i strefa DMZ muszą być bardzo bezpieczne.

Wykrywanie włamań, odczytywanie dzienników i inne urządzenia można łatwo dodać i omówić z kierownictwem. Ten format można powtórzyć, aby omówić usługi bezpieczeństwa na wszystkich poziomach i wszystkich systemach, a nie tylko systemy związane z handlem elektronicznym

Krok 3: Opracuj opcje usług bezpieczeństwa.

W kroku 3 firma B2B może przeanalizować i wybrać usługi bezpieczeństwa, które najlepiej spełniają jej wymagania prawne, biznesowe i bezpieczeństwa informacji. Największą różnicą między systemami B2C i B2B jest to, że system B2C nie zakłada żadnego poziomu zaufania. TheB2Bsystem do pewnego stopnia zakłada zaufanie, ale wymagana jest dodatkowa koordynacja i interfejs z klientem lub partnerem B2B. Wiarygodność nie jest kwestią „albo / albo" i nie należy jej zakładać. Nie można lekceważyć tej koordynacji i interoperacyjności, ponieważ ich rozwiązanie może okazać się trudne i kosztowne. Analiza wymaga czterech etapów:

1. Ryzyko lub wykonalność wdrożenia

2. Koszt wdrożenia i wsparcia

3. Skuteczność w zwiększaniu kontroli, a tym samym zmniejszaniu ryzyka

4. Klasyfikacja danych

Ryzyko wdrożeniowe jest funkcją zdolności organizacji do skutecznego wprowadzenia technologii. W tym przykładzie zakładamy, że ryzyko wdrożenia jest niskie, a zasoby są łatwo dostępne do wdrożenia technologii.

Koszty wdrożenia i wsparcia są nadrzędne w procesie podejmowania decyzji. Należy wziąć pod uwagę koszty obu firm. Niestety koszt wsparcia jest trudny do oszacowania i łatwo przeoczony. W tym przykładzie zasoby są dostępne zarówno do wdrożenia, jak i do obsługi technologii.

Skuteczność w zwiększaniu kontroli jest integralną częścią analizy korzyści i zarządzania ryzykiem. Należy wziąć pod uwagę każdy komponent bezpieczeństwa, aby określić wzajemne korzyści, w których kontrole nakładają się i uzupełniają inne. W tym przykładzie kierownictwo rozumie i wspiera zwiększony poziom kontroli.

Klasyfikacja danych jest podstawą wymagań i pomoże prowadzić dyskusje na temat kosztów i korzyści, ponieważ oddaje wartość informacji dla podstawowej działalności. W tym przykładzie dane są uważane za wystarczająco istotne, aby uzasadnić dodatkowe środki bezpieczeństwa w celu ochrony danych przed niewłaściwym wykorzystaniem, kradzieżą i utratą.

Każdą usługę bezpieczeństwa można zdefiniować w sposób ciągły, biorąc pod uwagę ryzyko wdrożenia, koszty i klasyfikację danych. Kierownictwo może użyć tego wykresu do wykreślenia poziomów ochrony wymaganych przez system. Ten przykład przedstawia skuteczność opcji usług bezpieczeństwa w stosunku do innych protokołów lub produktów. Każda organizacja powinna opracować własne kontinua i zapewnić wskazówki dla twórców stron internetowych i programistów aplikacji w zakresie

prawidłowego wykorzystania i standardowych ustawień usług bezpieczeństwa. Na przykład w przypadku usług uwierzytelniania / identyfikacji, aby usługa była minimalna do maksimum:

* Minimalny poziom bezpieczeństwa to brak haseł.

* Słabe hasła (np. Łatwe do odgadnięcia, współdzielone, słaba konstrukcja) są lepsze niż brak haseł, ale nadal zapewniają tylko minimalny poziom bezpieczeństwa.

* Hasła na poziomie systemu operacyjnego lub bazy danych zwykle zapewniają zbyt duży dostęp do systemu, ale można nimi skutecznie zarządzać.

* Hasła aplikacji są trudne w zarządzaniu, ale mogą być używane do ograniczania dostępu do danych w większym stopniu.

* Dostęp oparty na rolach wyróżnia użytkowników potrzebą wiedzy, aby wspierać ich zadania. Role są ustalane, a użytkownicy są grupowani według wymaganej funkcji.

* Tokeny są przekazywane użytkownikom i umożliwiają dwuczęściowe uwierzytelnianie. Hasła i tokeny są łączone w celu silnego uwierzytelniania.

* Biometria to sposób weryfikacji osoby podającej się za użytkownika poprzez odciski palców, skany siatkówki lub inne unikalne funkcje ciała.

Konkluzja ramowa.

Internetowy handel elektroniczny zmienił sposób, w jaki korporacje prowadzą interesy ze swoimi klientami, sprzedawcami, dostawcami i jednostkami biznesowymi. Sektory B2B i B2C będą się nadal rozwijać. Pomimo obaw związanych z bezpieczeństwem, postęp w kierunku zwiększonego wykorzystania Internetu jako kanału sprzedaży, logistyki i marketingu nadal trwa. Wyzwaniem dla specjalistów ds. Bezpieczeństwa informacji jest dotrzymanie kroku tej zmianie z punktu widzenia bezpieczeństwa, ale nie hamowanie postępu. Innym równym wyzwaniem jest to, że produkty zabezpieczające Internet są nowe i nie w pełni funkcjonalne lub dojrzałe. Produkty zostaną ulepszone, ale w międzyczasie istniejące produkty muszą zostać wdrożone, a później wyposażone w ulepszone i bezpieczniejsze usługi bezpieczeństwa. To zmieniające się środowisko, w tym wprowadzanie coraz poważniejszych i bardziej wyrafinowanych zagrożeń, jest nadal trudne do zabezpieczenia. Procesy opisane w tej sekcji pozwolą specjaliście na zapewnienie bezpieczeństwa jednostki biznesowej dysponującej potężnym narzędziem do komunikacji, wyboru i wdrażania usług bezpieczeństwa informacji. Trzy kroki zostały opisane i zademonstrowane na dwóch przykładach. Proces wspiera podejmowanie decyzji. Decyzje mogą zostać podjęte i łatwo udokumentowane, aby wykazać opłacalność doboru zabezpieczeń. Ryzyko związane z określonymi decyzjami może zostać omówione i zaakceptowane przez kierownictwo. Można obliczyć i omówić kompromisy między kosztami a korzyściami. Dlatego krytyczne staje się przeanalizowanie alternatyw i podjęcie dobrych decyzji. Procesy wspierające te decyzje muszą być sprawne i szybko wdrażane. Podejście oparte na usługach bezpieczeństwa informacji umożliwi firmom wdrażanie zabezpieczeń w praktycznym tempie. Niewybrane usługi są łatwo widoczne. Ryzyko niewybrania określonych usług ochrony musi zostać zaakceptowane przez kierownictwo.

ZASADY ZAANGAŻOWANIA.

Internet to szybko rozwijające się, złożone środowisko. Obsługa klientów drogą elektroniczną jest wyzwaniem. Kwestie bezpieczeństwa związane z Internetem wiążą się z wieloma delikatnymi kwestiami dotyczącymi bezpieczeństwa i prywatności. Ataki na strony internetowe nie są incydentami prywatnymi; często są publiczne i zawsze należy je traktować poważnie. Prawidłowe odróżnienie

„fałszywych alarmów" od prawdziwych ataków jest ciągłym wyzwaniem, z niewielką nadzieją na czyste rozwiązania. Odróżnienie gwałtownego wzrostu popularności od ataku DDoS (Distributed Denial of Service) jest nieprecyzyjne i podatne na błędy. Rzeczywiście, pojedynczy wzrost ruchu może mieć miejsce jednocześnie. Internetowy pokaz bielizny Victoria's Secret w lutym 1998 r. Był popularny, przekraczając nawet najbardziej optymistyczne oczekiwania jego twórców, a liczba odwiedzających spowodowała poważne problemy. Oczywiście tysiące ludzi nie atakowało witryny; byli po prostu wirtualnym tłumem próbującym uzyskać dostęp do tego samego miejsca w tym samym czasie. Podobne epizody miały miejsce, gdy witryny były opisywane jako interesujące na grupach dyskusyjnych Usenet lub w serwisach społecznościowych (np. YouTube, Facebook, witter i inne). Prośby o tsunami często pojawiają się z niewielkim lub żadnym ostrzeżeniem. Fizyczne moby są ograniczone przez transport, czas i koszty; wirtualne moby są ograniczone wyłącznie tym, ile może próbować jednocześnie uzyskać dostęp do zasobu z lokalizacji na całym świecie. Niedawnym przykładem był debiut ograniczonego produktu Missoni wprowadzonego przez Target 13 września 2011 r., Który spowodował wzrost popytu, który sprawił, że witryna Target była faktycznie niedostępna (93% żądań zostało odrzuconych) na wiele godzin

Środki specyficzne dla witryn internetowych.

Ochrona Witryny oznacza zapewnienie, że witryna i jej funkcje są dostępne 24 godziny na dobę, siedem dni w tygodniu i 365 dni w roku. Oznacza to również zapewnienie, że informacje wymieniane z witryną są dokładne i bezpieczne. Ta sekcja koncentruje się na kwestiach specyficznych dla interakcji sieci Web z klientami, a także łańcuchów dostaw i dystrybucji. Praktycznie rzecz biorąc, witryna internetowa jest ważnym, jeśli nie najważniejszym, elementem interfejsu organizacji ze światem zewnętrznym. Ochrona stron internetowych znajduje się na przecięciu technologii, strategii, operacji, relacji z klientami i zarządzania biznesem. Dostępność i integralność witryny internetowej bezpośrednio wpływa na główne strumienie przepływu gotówki i handlu: klientów organizacji, łańcuchy produkcyjne i łańcuchy dostaw. Dostępność jest kamieniem węgielnym strategii związanych z allWeb. Czasy bezczynności stały się stopniowo coraz rzadsze. W zależności od branży i jej rynków mogą wystąpić okresy mniejszej aktywności. W społeczności zajmującej się handlem finansowym pozostaje tylko kilka małych okienek w ciągu 24 godzin, w których można przeprowadzić aktualizacje i konserwację. W miarę jak globalny biznes staje się normą, klienci, dostawcy i dystrybutorzy coraz częściej oczekują informacji i możliwości przeprowadzania transakcji o każdej porze dnia i nocy, nawet od niewielkich przedsiębiorstw. W Internecie „nikt nie wie, że jesteś psem" oznacza również „nikt nie wie, że nie jesteś dużą firmą". Pole gry zostało wprawdzie wyrównane, ale nie zostało jednakowo podniesione ani obniżone. Oczekiwania wzrosły, podczas gdy kapitał i koszty operacyjne drastycznie spadły. Przyczynowość nie ma związku z wpływem. Przytłaczająca większość przerw w dostępie do Internetu jest spowodowana mało efektownymi problemami. Głośne, celowe ataki są znacznie rzadsze niż awarie sprzętu i personelu. Wpływ na organizację biznesową jest nie do odróżnienia. Niski profil nie stanowi obrony przed przypadkowym atakiem skanującym ani przed kimś, kto szuka trampoliny do ataku na osobę trzecią. Ponadto, chociaż aktywa pojedynczej firmy mogą nie być atrakcyjnym celem, firma nadal może być użyteczną trampoliną do ataku na osobę trzecią. Takie ataki mogą mieć miejsce ze względu na związek (np. Sprzedawca lub dostawca) lub mogą być jedynie oportunistycznymi próbami rekrutacji (np. Rekrutacją, a może bardziej właściwymi, komputerami stacjonarnymi służącymi do łączenia się z prasą dla botnetów). Zdarzenia zewnętrzne i ich następstwa również mogą siać spustoszenie, zarówno bezpośrednio, jak i pośrednio. Ataki terrorystyczne z 11 września 2001 r., Które zniszczyły kompleks World Trade Center w Nowym Jorku, wywarły wpływ na cały świat, nie tylko na systemy i firmy zlokalizowane w zniszczonym kompleksie. Infrastruktura telekomunikacyjna została uszkodzona lub zniszczona, przerywając łącza internetowe wielu organizacjom. Dostawy części i wszystkie podróże zostały zakłócone, gdy przestrzeń powietrzna Ameryki Północnej została zamknięta

na kilka dni. Manhattan był zabezpieczony przed wyjściami i wejściami, podczas gdy w samym mieście i na całym świecie zawieszono normalne operacje. Ataki z 11 września były wyjątkowo uciążliwe, ale środki ostrożności podobne do tych opisanych w tym podręczniku służyły zmniejszeniu szkód w operacjach internetowych i innych elementach infrastruktury związanych z problemami, które je zaimplementowały. Rzeczywiście, istnienie sieci i wynikająca z tego zdolność do organizowania grup bez fizycznej obecności okazały się sposobem na złagodzenie szkód spowodowanych atakami, nawet dla firm, które miały dużą obecność w World Trade Center. W okresie następującym po atakach na World Trade Center Morgan Stanley i inne firmy z biurami na dotkniętym obszarze wdrożyły szeroko zakrojone interakcje telepracownicze i internetowe, najpierw w celu uwzględnienia swoich pracowników11, a następnie w celu umożliwienia kontynuowania pracy. . Niektóre praktyki, problemy i obawy na pierwszy rzut oka wydają się istotne tylko dla bardzo dużych organizacji, takich jak firmy z listy Fortune 500. W rzeczywistości tak nie jest. Rozpatrywanie zagadnień w kontekście dużej organizacji pozwala ukazać je w powiększeniu i z pełną szczegółowością. Mniejsze organizacje mają te same problemy i obawy, ale mogą być w stanie wdrożyć mniej formalne rozwiązania. „Formalne" niekoniecznie oznacza pisemne procedury. Może to oznaczać, że pewne praktyki związane z komputerami, takie jak modyfikowanie istniejących obiektów produkcyjnych, są z natury kiepskimi pomysłami i należy ich unikać. Bardzo duże przedsiębiorstwa mogą rozwiązać te problemy poprzez wydzielenie oddzielnej grupy, dysponującej oddzielnym sprzętem, odpowiedzialnej za obsługę środowiska programistycznego. Przyrostowe rozmieszczenie etapowe to doskonała technika kalibracji narażenia na ryzyko.

Definiowanie ataków.

Powtarzające się, wielokrotne próby połączenia się z serwerem mogą być złowieszcze lub mogą być niczym więcej niż klientem z problemem technicznym. W zależności od źródła duża liczba nieudanych połączeń lub przerwanych operacji pochodzących z węzłów bramy należących do organizacji może stanowić problem w sieci, atak na serwer lub połączenie obu. Może również przedstawiać coś nie bardziej złowieszczego niż grupa użytkowników w okolicy uzyskujących dostęp do zasobu internetowego przez zaporę ogniową.

Definiowanie ochrony.

Istnieje różnica między ochroną zasobów widocznych w Internecie a ochroną witryn internetowych. W większości zasoby widoczne w Internecie nie są przeznaczone do użytku publicznego. W związku z tym często znacznie łatwiej jest przewidzieć wielkość wykorzystania i uwzględnić wzorce ruchu. Witryny internetowe podlegają zmianom związanym z powszechnym użytkowaniem na całym świecie. Dramatyczny wzrost ruchu może być atakiem lub może to być nieoczekiwane wyświetlenie adresu URL witryny w programie telewizyjnym lub w relatywnie niezwiązanych z nimi wiadomościach.

Odróżnienie wojowniczości od popularności jest trudne, jeśli nie niemożliwe. Zawsze dopuszczalne są środki ochrony własnej, które nie mają wpływu na klientów. Należy jednak zachować ostrożność, aby zapewnić, że środki są naprawdę wolne od skutków. Na przykład niektóre witryny, w szczególności publiczne serwery FTP, często wymagają, aby adres protokołu internetowego (IP) komputera żądającego zawierał wpis w odwrotnym systemie nazw domen, który odwzorowuje adresy IP na nazwy hostów (np. Węzeł 192.168.0.1 ma PTR [rekord wskaźnika] 1.0.168.192.in-addr.arpa) (RFC1034, RFC1035; Mockapetris 1987a, 1987b) w przeciwieństwie do bardziej znanej bazy danych systemu nazw domen, która odwzorowuje nazwy hostów na adresy IP. Prawdą jest, że wiele komputerów ma takie wpisy, ale prawdą jest również, że wiele witryn, w tym sieci firmowe i wielu dostawców usług internetowych, nie udostępnia informacji o odwróconym systemie DNS. To, czy cała populacja powinna zostać wykluczona z terenu, jest decyzją polityczną i zarządczą, a nie decyzją czysto

techniczną. Nawet niewielka liczba incydentów na popularnej stronie internetowej może być katastrofalna, zarówno dla dostawcy, jak i dla naiwnego użytkownika końcowego, który nie ma możliwości zrozumienia lub rozwiązania problemu.

Zachowanie prywatności.

Poważnym problemem jest również rejestrowanie interakcji między klientami a Serwisem. Polityka prywatności Witryny ponownie jest kwestią zarządczą, prawną i relacjami z klientami, która ma poważne podteksty. Personel techniczny musi mieć świadomość, że zasady, przepisy i inne kwestie mogą dyktować, jakie informacje mogą być rejestrowane, gdzie mogą być przechowywane i jak mogą być używane. Na przykład ustawa o ochronie prywatności dzieci w Internecie z 1998 r. (COPPA) (15 U.S.C. § 6501 i nast.) Zabrania w Stanach Zjednoczonych uzyskiwania informacji o nazwisku i adresie od dzieci poniżej 13 roku życia. Wiele firm jest stronami umów z organizacjami zewnętrznymi, takimi jak TRUSTe13, regulującymi wykorzystanie i ujawnianie danych osobowych.

Praca z organami ścigania.

Podobnie skomplikowane jest postępowanie z organami prawnymi. Próby oszukańczych zakupów i inne podobne problemy można rozwiązać za pomocą praktycznie tych samych procedur, które są stosowane w przypadku konwencjonalnych prób oszustw przy zamówieniach pocztowych lub telefonicznych. Radzenie sobie z atakami i podobnymi nadużyciami jest bardziej skomplikowane i zależy od zasad i procedur organizacji oraz otoczenia prawnego. Istotną kwestią jest również status Serwisu. Jeśli serwer znajduje się w obiekcie hostingowym lub jest własnością i jest obsługiwany przez osobę trzecią, sytuacja staje się jeszcze bardziej skomplikowana pod względem prawnym. Zaangażowanie organów ścigania w danej sytuacji prawdopodobnie będzie wymagać, aby śledczy mieli dostęp do serwerów internetowych i sieci wspierającej, co może być trudne. Na koniec pojawia się pytanie, jakie informacje są rejestrowane iw jakich okolicznościach.

Akceptowanie strat.

Żaden schemat bezpieczeństwa nie jest niezawodny. Zdarzają się incydenty. Pewne uspokojenie można czerpać z faktu, że najczęstsze przyczyny kompromisów systemowych w 2001 roku wydają się pozostać takie same, jak wtedy, gdy Clifford Stoll napisał The Cuckoo's Egg w 1989 roku. Wcześniej i teraz słabo zabezpieczone systemy:

* Konta zarządzania z oczywistymi hasłami

* Niezabezpieczone pliki systemowe

* Niezałatane znane dziury w zabezpieczeniach

Jednak wyeliminowanie najprostszych i najczęstszych sposobów, w jakie osoby postronne mogą włamać się do witryn internetowych, nie rozwiązuje wszystkich problemów. Rosnąca złożoność zawartości witryny i kodu aplikacji obsługujących witryny dynamiczne oznacza, że istnieje ciągłe wyzwanie związane z projektowaniem, wdrażaniem, testowaniem i zapewnianiem jakości. Oprogramowanie oparte na serwerze i rozproszone na serwerze (np. Dynamiczne witryny WWW) podlega tym samym zagrożeniom związanym z rozwojem, co inne formy oprogramowania. Zagrożenia bezpieczeństwa przedostaną się na stronę internetową pomimo najlepszych wysiłków deweloperów i testerów. Akceptacja tej rzeczywistości jest ważną częścią planowania niezbędnego do radzenia sobie z nieuniknionymi incydentami. W przypadku podejrzenia, że witryna lub pojedynczy komponent zostały naruszone, należy aktywować plany reakcji. Różnica polega na tym, że plan reakcji dotyczący

witryny internetowej musi uwzględniać fakt, że grupą, na którą plan ma największy wpływ, będą klienci firmy. Podstawowym celem planu reakcji jest powstrzymanie szkód.

Unikanie nadmiernej reakcji.

Poważne reakcje mogą spowodować tyle samo, jeśli nie więcej szkód niż rzeczywisty atak. Plan reakcji musi określać organ decyzyjny i wytyczne umożliwiające podejmowanie skutecznych decyzji. Jest to szczególnie prawdziwe w przypadku dużych witryn, w których ataki mogą występować regularnie. Metody określania momentu, w którym Witryna musi zostać odłączona, aby zapobiec dalszym szkodom, należy wcześniej określić. Klony offline powinny być przygotowane, aby umożliwić szybkie odpowiedzi. Kiedy pod presją czasu podczas sytuacji awaryjnej, ostatnią rzeczą, jakiej pragniemy, jest budowanie obrazów systemu produkcyjnego.

Podsumowując, w przypadku ochrony stron internetowych i klientów działania obronne są prawie zawsze dozwolone, a wszelkiego rodzaju działania obraźliwe są prawie zawsze niedopuszczalne. Najlepsze są działania obronne, które są przejrzyste dla klienta.

Odpowiednie reakcje na ataki.

Na długo przed pojawieniem się komputera, zanim rozwinęła się natychmiastowa komunikacja, prawo międzynarodowe uznawało, że ostrzelanie okrętu wojennego było aktem wojny. Kapitanom okrętów wojennych wydawano rozkazy stałe, podsumowane jako ogień w przypadku ostrzału. Na obszarach bez łatwo dostępnej ochrony policyjnej prawo obywateli do samoobrony jest powszechnie uznawane przez większość organów prawnych. W ramach prawa międzynarodowego takie formalne standardy postępowania sił zbrojnych są znane jako zasady zaangażowania, pojęcie o globalnym znaczeniu. . W cyberprzestrzeni kuszące jest odrzucenie standardów realnego świata. Łatwo jest wyobrazić sobie siebie jako mistrza własnego kawałka cyberprzestrzeni, bez związku z prawami świata rzeczywistego i ograniczeniami zachowania. Jednak personel informatyczny (IT) nie ma legitymacji prawnej kapitanów statków, którzy nie mają kontaktu ze światem zewnętrznym. Niektórzy twierdzą, że „ogień w przypadku ostrzału" jest akceptowalnym standardem zachowania w Internecie. Takie podejście nie bierze pod uwagę kwestii prawnych i etycznych dotyczących strategii i taktyk reagowania. Może to być niezadowalające, ale jedyną odpowiedzią względnie wolną od konsekwencji prawnych (karnych, cywilnych i regulacyjnych) jest „Tylko akcja obronna". Blokowanie zakresów adresów jest obronne; oddanie strzału przekracza linię ataku. Każdy konkretny incydent związany z bezpieczeństwem ma szereg potencjalnych odpowiedzi. Odpowiednia reakcja zależy od przedsiębiorstwa oraz jego otoczenia politycznego, prawnego i biznesowego. Dopuszczalność reakcji jest również kwestią zarządzania, a także potencjalnie polityczną. Określenie, jakie reakcje są dopuszczalne w różnych sytuacjach, wymaga wkładu kierownictwa w zakresie polityki, radcy prawnego w zakresie legalności, działu public relations w zakresie opinii publicznej oraz personelu technicznego w zakresie technicznej wykonalności. W zależności od organizacji może być również konieczne zaangażowanie związków zawodowych i innych stron w negocjowanie tego, co stanowi odpowiednią odpowiedź. To, co jest akceptowalne lub odpowiednie w jednym obszarze, niekoniecznie jest akceptowalne lub odpowiednie w innym. Często na arenie bezpieczeństwa narodowego standardy dowodu są niższe niż byłyby dopuszczalne w normalnych sporach biznesowych. W amerykańskich sądach cywilnych sprawy są rozstrzygane na podstawie przewagi dowodów. Standardy dowodowe dopuszczalne w postępowaniu cywilnym nie są rozstrzygające, gdy toczy się sprawa karna, w której winę należy ustalić ponad wszelką wątpliwość. Gambity lub odpowiedzi, które są całkowicie legalne w środowisku bezpieczeństwa narodowego, mogą być całkowicie nielegalne i lekkomyślnie nieodpowiedzialne w sektorze prywatnym, narażając organizację na znaczną odpowiedzialność prawną. Zasady etykiety i zachowania są podobnie złożone. Prawa osadzonych w więzieniach w Stanach Zjednoczonych pozostają znaczące, mimo że podlegają

zasadom i przepisom znacznie bardziej restrykcyjnym niż w przypadku ogółu społeczeństwa. Również środki bezpieczeństwa muszą być odpowiednie dla osób i sytuacji, w których są stosowane.

Przeciwbateria.

Niektórzy sugerują, że właściwą reakcją na domniemany atak jest zastosowanie cyberprzestrzeni odpowiednika baterii przeciwdziałającej, czyli wycelowanie w artylerię, która właśnie do ciebie wystrzeliła. Jednak taktyka kontratakowania, stosowana jako środek obronny przed atakami internetowymi, będzie postrzegana pod względem technicznym i prawnym jako atak jak każdy inny. Taktyki kontratakowania mogą być emocjonalnie satysfakcjonujące, ale są podatne zarówno na błędy, jak i szkody uboczne. Kontratak może być skuteczny tylko wtedy, gdy złoczyńca zostanie prawidłowo zidentyfikowany, a skutki wzajemnego ataku są ograniczone do sprawcy. Jeśli osoby trzecie zostaną w jakikolwiek sposób skrzywdzone, działanie odwetowe stają się atakiem samym w sobie. Jednym z bardziej znanych ataków przeciwdziałających pobiciu, które zakończyły się niepowodzeniem, był przypadek z 1994 r., Kiedy dwóch prawników z Phoenix w Arizonie spamowało ponad 5000 grup dyskusyjnych Usenet, aby przekazać niezamówione informacje na temat loterii US Immigration and Naturalization Service za 55 000 zielonych kart (zezwoleń imigracyjnych). Wynikające z tego fale protestów e-mailowych przeciwko przestępcom zalały ich dostawcę usług internetowych (ISP) i spowodowały awarię co najmniej jednego serwera, powodując odmowę usługi dla wszystkich innych, niewinnych klientów usługodawcy internetowego.

Trzymaj za nieszkodliwe.

Polityki operacyjne dotyczące operacji internetowych muszą zajmować nieszkodliwe stanowisko wobec działań w dobrej wierze w ramach polityki. Radzenie sobie z kryzysem internetowym często wymaga szybkiej reakcji. Jeżeli pracownicy działają w dobrej wierze, zgodnie ze swoimi obowiązkami i zgodnie z udokumentowanymi procedurami, osoby podejmujące decyzje powinny być chronione przed odwetem. Kara za działania podjęte w dobrej wierze przynosi efekt przeciwny do zamierzonego. Jeśli procedury są złe, popraw zasady i procedury; nie obwiniaj pracowników za przestrzeganie ustalonych zasad. W takich okolicznościach działania dyscyplinarne są oczywiście niewłaściwe.

ANALIZA RYZYKA.

Jak wspomniano wcześniej, ochrona witryn internetowych organizacji zależy od dokładnej, racjonalnej oceny ryzyka. Opracowanie skutecznych strategii i taktyk w celu zapewnienia dostępności i integralności miejsca wymaga przeanalizowania po kolei wszystkich potencjalnych zagrożeń. Nieograniczona działalność komercyjna jest dozwolona w Internecie od 1991 r. Od tego czasu duże i małe przedsiębiorstwa coraz częściej integrują dostęp do sieci Web w swoich działaniach „sekundowych". Ryzyko związane z daną konfiguracją i strategią zależy od wielu czynników, w tym od skali przedsiębiorstwa i względnego znaczenia podmiotu internetowego w przedsiębiorstwie. Praktycznie wszystkie witryny internetowe o wysokiej widoczności (np. Yahoo !, America Online, cnn.com, Amazon.com i eBay) doświadczały w różnych okresach poważnych awarii. Im ważniejszy składnik sieciowy organizacji, tym ważniejsza jest dostępność i integralność. Duże, tradycyjne firmy ze stosunkowo małymi komponentami sieci Web mogą tolerować duże przerwy przy niewielkich uszkodzeniach. Firmy duże lub małe, które w dużej mierze polegają na sieci Web, muszą zwracać większą uwagę na swoją obecność w sieci, ponieważ poważna awaria może szybko przekształcić się w katastrofę finansową lub public relations.

Strata biznesowa.

Straty biznesowe można podzielić na kilka kategorii, z których każda może wystąpić w połączeniu z obecnością organizacji w Internecie. W kontekście tego rozdziału klienci są zarówno osobami z zewnątrz, które mają dostęp do Internetu, jak i osobami wewnętrznymi, które uzyskują dostęp do aplikacji intranetowych. W praktyce osoby wewnętrzne korzystające z aplikacji hostowanych w intranecie stanowią takie same wyzwania, jak użytkownicy zewnętrzni.

Obraz PR.

Witryna jest publiczną twarzą organizacji 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Ta ciągła obecność jest zaletą, dzięki czemu firma jest zawsze widoczna, ale wysoki publiczny profil witryny sprawia, że jest ona głównym celem. Witryny rządowe w Stanach Zjednoczonych i za granicą często były celem ataków. W styczniu 2000 r. „Thomas", witryna internetowa Kongresu Stanów Zjednoczonych, została zniszczona. Wcześniej, w 1996 roku, zdewastowano witrynę internetową Departamentu Sprawiedliwości Stanów Zjednoczonych. Zniszczone zostały również witryny należące do rządów Japonii, Wielkiej Brytanii i Meksyku. Ataki na strony internetowe nadal stanowią coraz większy problem. 21 marca 2013 r. seria infekcji złośliwym oprogramowaniem sparaliżowała nadawców i instytucje finansowe w Korei Południowej w czasie narastających napięć związanych z północnokoreańskimi testami jądrowymi i rakietowymi, w tym zrzeczeniem się przez Koreę Północną rozejmu z 1953 r., Zawieszającego wojnę koreańską. strony różnych problemów atakujących obecność drugiej strony w Internecie. Chociaż nie są powszechnie znane żadne rozstrzygające dowody zaangażowania państw narodowych w takie działania, jest to nieuniknione. Wzrost tej aktywności zbiegł się w czasie z ważnymi wydarzeniami publicznymi, w tym z incydentem między USA a Chinami w 2001 r., Obejmującym zderzenie lotnicze między samolotami wojskowymi, operacjami afgańsko-irackimi, wojną izraelsko-libańską w 2006 r., Konfliktem rosyjsko-gruzińskim16 i Estonią. .17 Taka działalność nie ogranicza się jednak do sfery bezpieczeństwa narodowego. Wiele witryn zostało zniszczonych podczas incydentów po opublikowaniu karykatur w duńskiej gazecie, które według niektórych zniesławiały proroka Mahometa. W niektórych przypadkach firmy poniosły dodatkowe szkody w wyniku konkursów hakerskich, w których hakerzy udowadniają swoją siłę, niszcząc jak najwięcej witryn. Fakt, że nie ma bezpośredniego motywu lub niechęci do firmy, nie ma znaczenia; szkoda nadal została wyrządzona. W świecie korporacji witryny firmowe były celem ataków mających na celu zniesławienie korporacji za prawdziwe lub wyimaginowane pomyłki. Niektóre takie epizody zostały zgłoszone w mediach, podczas gdy inne nie były przedmiotem obszernych relacji. Skala i wartość odcinka nie mają znaczenia; szkoda wyrządzona docelowej organizacji jest prawdziwą miarą. Niezgłoszone zdarzenie, które jest zdarzeniem inicjującym niepowodzenie w biznesie, jest bardziej szkodliwe dla zainteresowanych stron niż pozornie bardziej znacząca awaria z mniej poważnymi konsekwencjami. Inni cyberwandale (np. Sadmind / IIS) używali skanerów adresów do namierzania losowo wybranych maszyn. Niewidzialność nie jest obroną przed atakami skanera adresów.

Utrata klientów / firmy.

Klienci internetowi są bardzo mobilni. Problemy ze stroną internetową szybko przekładają się na trwale utraconych klientów. Przyczyna przestoju jest nieistotna; sam fakt, że wystąpił problem, często wystarcza, aby sprowokować ucieczkę klienta. W większości obszarów konkurencja się pokrywa. Na przykładzie firmy zajmującej się przesyłkami z dnia na dzień, w większości obszarów metropolitalnych Stanów Zjednoczonych istnieją (w porządku alfabetycznym) Federal Express, United Parcel Service i United States Postal Service. Wszystkie firmy oferują śledzenie przesyłek przez Internet, bardzo popularną usługę. Problemy lub trudności ze śledzeniem przesyłek szybko doprowadzą do utraty biznesu na rzecz innej firmy z łatwiejszym śledzeniem.

Przerwy. Coraz częściej nowoczesne przedsiębiorstwa budowane są w oparciu o wszechobecne systemy informacyjne 24/7/365, najczęściej w których główną rolę odgrywają strony internetowe. W tym środowisku wszelkiego rodzaju przerwy są katastrofalne.

Produkcja. W ciągu ostatnich 20 lat usprawniono procesy produkcyjne we wszystkich obszarach. Dwadzieścia lat temu często zdarzało się, że zakłady miały na stanie wielodniowe dostawy komponentów. Obecnie środowiska bez opóźnień lub just-in-time (JIT) są powszechne, co pozwala dużym obiektom działać przy minimalnych zapasach. Fiskalnie środowiska bez opóźnień mogą być optymalnie opłacalne, jednak paradygmat pozostawia niewielki margines na zakłócenia wspierającego łańcucha logistycznego. Łańcuch ten jest czasami kruchy i może zostać przerwany przez dowolną liczbę zagrożeń.

Łańcuch dostaw. Coraz częściej witryny internetowe stanowią integralną część łańcucha dostaw. Firmy mogą zachęcać swoich dostawców do korzystania z portalu internetowego w celu uzyskania dostępu do strony dostawcy systemu zakupów. Oparte na XML19 bramy i podejścia oparte na architekturze zorientowanej na usługi (SOA), wraz z innymi technologiami sieciowymi, są wykorzystywane do organizowania przepływu surowców i komponentów wymaganych do obsługi procesów produkcyjnych oraz zarządzania nimi. To samo usprawnienie, które przyspiesza wymianę informacji między dostawcą a producentem, może również spowodować poważne szkody i pociągnąć do odpowiedzialności.

Łańcuch dostaw. Witryny internetowe, zarówno wewnętrzne, jak i zewnętrzne, czytelne dla człowieka i międzysystemowe, stały się preferowanym narzędziem do śledzenia statusu zamówień i wysyłek. Coraz częściej łącza system-system, wdrażane jako dokumenty elektroniczne (np. XML lub JSON), stały się podstawą łańcucha dostaw wielu przedsiębiorstw systemu zarządzania i zapytań.

Dostarczanie informacji. Banki, domy maklerskie, przedsiębiorstwa użyteczności publicznej i gminy coraz częściej sięgają po Internet jako wygodną i niedrogą metodę zarządzania relacjami z konsumentami. Firmy wspierają również pobieranie zapisów transakcji i innych informacji o relacjach w formatach wymaganych przez osobiste programy baz danych i organizatorów. Te dane wyjściowe z kolei są często wykorzystywane jako dane wejściowe do innych procesów, które następnie generują inne transakcje. Nic dziwnego, że w miarę upływu czasu coraz więcej osób i firm jest uzależnionych od dostępności informacji na żądanie. Dzisiejsi klienci internetowi zakładają, że informacje są dostępne wszędzie tam, gdzie mogą używać smartfona lub tabletu. Przypomina to wzorce korzystania z bankomatów we wcześniejszej dekadzie, co pozwoliło ludziom oprzeć swoje plany na dostępie do bankomatów, często dokonując kilkukrotnych wypłat 20 dolarów zamiast wypłaty czeku 200 dolarów tygodniowo.

Zagrożenia proaktywne a zagrożenia reaktywne.

Niektórymi zagrożeniami i zagrożeniami można zająć się proaktywnie, podczas gdy inne są z natury reaktywne. Kiedy opracowywane są strategie i taktyki mające na celu ochronę obecności w Internecie, same strategie i taktyki mogą powodować problemy z dostępnością. Jako przykład rozważmy powszechną strategię posiadania wielu serwerów nazw odpowiedzialnych za tłumaczenie nazw domen na adresy IP. Zanim nazwa domeny (właściwie nazywana strefą systemu nazw domen [DNS]) może zostać wprowadzona do serwerów nazw na poziomie głównym, wymagane jest zidentyfikowanie co najmniej dwóch serwerów nazw w celu przetwarzania żądań rozpoznawania nazw. Serwery nazw są najlepszym przykładem zasobów, które powinny być zróżnicowane geograficznie. Aktualizowanie stref DNS wymaga ostrożności. Jeśli aktualizacja zostanie przeprowadzona nieprawidłowo, zasoby, do których odwołuje się symbolicDNSnames, staną się nierozwiązywalne, niezależnie od faktycznego stanu serwerów sieci Web i powiązanej infrastruktury. Rachunek ryzyka związany z nazwami DNS

dodatkowo komplikuje powszechna, wydajna i odpowiednia praktyka wyznaczania serwerów nazw ISP jako głównego mechanizmu rozpoznawania nazw domen. Krótko mówiąc, tłumaczenie nazw stanowi dobry przykład możliwych zagrożeń, które mogą wpływać na obecność w Internecie.

Ocena zagrożeń

Niektóre zagrożenia są uniwersalne. Inne są specyficzne dla indywidualnego środowiska. Najbardziej niszczycielskimi i poważnymi zagrożeniami są te, które dotykają jednocześnie duże obszary lub populacje, gdzie wysiłki mające na celu naprawienie szkód i naprawienie problemu są utrudnione ze względu na skalę problemu. Różnice w perspektywie mogą utrudniać skuteczną reakcję. To, co wydaje się drobną awarią dla operatora, może być przestojem zagrażającym biznesowi dla klienta. Na podstawowym poziomie zagrożenia można podzielić na kilka kategorii. Pierwsza dotyczy umyślnych czynów i wypadków. Działania umyślne obejmują działania podejmowane w celu zniszczenia Serwisu lub jego infrastruktury. Wypadki obejmują zjawiska naturalne (klęski żywiołowe) oraz niezdarność, nieostrożność i nieprzemyślane konsekwencje (akty zbryleń). Mówiąc najogólniej, celowe działanie to takie, które ma na celu osłabienie systemu. Celowe działania obejmują szerokie spektrum umiejętności i zamiarów. Dla celów analizy ryzyka i planowania, umyślne działania przeciwko dostawcom infrastruktury często mogą wydawać się działaniami Bożymi. Dla organizacji prowadzącej stronę internetową atak pracownika na operatora telefonicznego jawi się po prostu jako kolejna przerwa w świadczeniu usług niewiadomego pochodzenia. Żadne przedsiębiorstwo ani agencja nie powinny uważać się za mało prawdopodobny cel. Wcześniejsze głośne incydenty były wymierzone w FBI (26 i 27 maja 1999), główne partie polityczne i grupy interesu w Stanach Zjednoczonych. Na poziomie konsumenckim liczne systemy domowe połączone z cyfrową linią abonencką (DSL) były celem wywrotu jako przygotowanie do przeprowadzenia ataków DDoS. W 2007 r. W wyniku kilku dochodzeń aresztowano kilka osób za prowadzenie tak zwanych botnetów (grup zaatakowanych komputerów). Sieci te liczyły setki tysięcy maszyn. Niedawno Aramco padł ofiarą poważnego ataku; podobnie jak główne koreańskie instytucje finansowe. Nie można nie doceniać możliwości wykorzystania takich sieci w celach intrygujących.

WYMAGANIA EKSPLOATACYJNE

Systemy widoczne w Internecie to takie, które mają dowolne połączenie z Internetem na całym świecie. Kuszące byłoby rozważenie ochrony systemów widocznych w Internecie jako kwestii czysto technicznej. Jednak kwestie techniczne i biznesowe są nierozłączne w dzisiejszym zarządzaniu ryzykiem. Na przykład, jak wspomniano wcześniej w tym rozdziale, stopień, w jakim systemy powinny być narażone na działanie Internetu, jest zasadniczo kwestią związaną z zarządzaniem ryzykiem biznesowym. Technologie ochrony i zasady stojące za ochroną można omówić dopiero po rozważeniu i podjęciu decyzji w sprawie ryzyka biznesowego, ustalając kontekst dla dyskusji technicznych. Z kolei ocena zarządzania ryzykiem biznesowym musi obejmować pełną świadomość wszystkich ryzyk technicznych. Jak na ironię, nietechniczni menedżerowie biznesowi mogą dokładnie ocenić stopień ryzyka biznesowego dopiero po całkowitym ujawnieniu ryzyka technicznego. Dodatkowe ryzyka biznesowe i techniczne wynikają z outsourcingu. Obecnie wiele przedsiębiorstw obejmuje sprzęt będący własnością stron trzecich, który jest przez nie konserwowany i zarządzany. Część tego sprzętu znajduje się we własnych pomieszczeniach organizacji, a inny sprzęt znajduje się poza siedzibą, na przykład w obiektach dostawców usług aplikacyjnych. Ochrona witryny internetowej rozpoczyna się od wstępnego doboru i konfiguracji sprzętu oraz jego elementów pomocniczych i trwa przez cały okres ich użytkowania. Ogólnie rzecz biorąc, troska i proaktywne uwzględnienie aspektów dostępności i bezpieczeństwa witryny od samego początku zmniejszy koszty i problemy operacyjne. Chociaż praktycznie niemożliwe do osiągnięcia, celem jest zaprojektowanie i wdrożenie automatycznego systemu, którego architektura i implementacja działają nawet w obliczu problemów, przy minimalnym

wpływie na klienta. Nie oznacza to, że witryna internetowa może działać bez nadzoru. Ciągłe, proaktywne monitorowanie ma kluczowe znaczenie dla zapewnienia bezpiecznego działania witryny. Nadmiarowość ogranicza tylko potrzebę reakcji w czasie rzeczywistym, tymczasowo omijając problem; nie eliminuje przyczyny. Początkowa awaria musi zostać wykryta, odizolowana i skorygowana tak szybko, jak to możliwe, aczkolwiek w sposób bardziej planowy. W przeciwnym razie system będzie działał w swoich sukcesywnie degradowanych trybach redundancji, aż do awarii ostatniego nadmiarowego komponentu, po czym system ulegnie całkowitej awarii.

Wszechobecne protokoły internetowe w sieci.

Biznes zajmuje się bezpieczeństwem sieci Internet (tj. Połączonych ze sobą sieci) od czasu pojawienia się intersieci pod koniec lat sześćdziesiątych XX wieku. Jednak wszechobecność sieci protokołu kontroli transmisji / protokołu internetowego (TCP / IP) i publicznego Internetu naraziła na ataki znacznie więcej sprzętu niż w czasach zamkniętych sieci korporacyjnych. Ponadto znacznie szersza gama urządzeń, takich jak telefony głosowe oparte na technologii VoIP, faksy, kopiarki, a nawet dystrybutory napojów bezalkoholowych, jest teraz dostępna w sieci. Łączność IP była wielkim dobrodziejstwem dla produktywności i łatwości użytkowania, ale nie obyło się bez ciemniejszej strony. Dostępność sieci stworzyła również bezprecedensowe możliwości niewłaściwego, nieautoryzowanego dostępu do zasobów sieciowych i innych szkód. Nierzadko zdarza się, że sondy i próby włamania występują w ciągu godzin lub nawet minut niezapowiedzianego połączenia z globalnym Internetem. Ochrona zasobów widocznych w Internecie jest z natury konfliktem między łatwością dostępu a bezpieczeństwem. Najbezpieczniejsze systemy to te, które nie są połączone ze światem zewnętrznym. Podobnie, najłatwiejsze w obsłudze systemy to takie, które nie mają dostrzegalnych ograniczeń użytkowania. Dostosowanie limitów działań użytkowników i dostępu musi równoważyć sprzeczne wymagania. Na przykład wiele sieci jest zarządzanych w paśmie, co oznacza, że przełączniki, routery, zapory i inne elementy infrastruktury sieciowej są zarządzane przy użyciu rzeczywistej sieci jako medium połączeniowego. Gdyby interfejsy zarządzania nie były zarządzane przez odpowiednio zaszyfrowane połączenia, hasła zarządzania byłyby widoczne w sieci. Osoba postronna lub osoba nieupoważniona może więc monitorować sieć, uzyskując informacje wystarczające do jej sparaliżowania. Może to spowodować poważne szkody i odpowiedzialność dla organizacji.

Partycje wewnętrzne.

Złożone środowiska korporacyjne można często skutecznie zabezpieczyć, dzieląc organizację na różne wzajemnie powiązane i zagnieżdżone domeny zabezpieczeń, z których każda ma własne wymagania prawne, techniczne i kulturowe. Na przykład istnieją określone wymogi prawne dotyczące dokumentacji medycznej i ochrony prywatności. Partnerzy i dostawcy, jak również konsultanci, kontrahenci i klienci często potrzebują dwukierunkowego dostępu do swoich danych firmowych i obiektów. Te zróżnicowane wymagania oznaczają, że pojedynczy firmowy firewall jest często niewystarczający. Różne domeny w organizacji często wymagają własnych zapór i zasad bezpieczeństwa. Śledzenie różnorodności typów danych, wymagań dotyczących ochrony i dostępu oraz różnych jurysdykcji i regulacji prawnych powoduje, że poziom złożoności był wcześniej niespotykany. Po prostu nie jest możliwe skonfigurowanie pełnego zestawu reguł, aby zaimplementować wiele różnych wymagań bezpieczeństwa bez tworzenia luk w zabezpieczeniach lub sprzeczności. Wiele napisano o tak zwanych zaawansowanych trwałych zagrożeniach. Chociaż terminologia jest stosunkowo nowa, koncepcja taka nie jest, o czym była mowa we wcześniejszych wydaniach tego podręcznika.24 Podstawową zmianą leżącą u podstaw zaawansowanych zagrożeń jest stopień ukierunkowania i zamiar atakującego pozostania w ukryciu. Pod tym względem użytecznym historycznym precedensem jest zaangażowanie w zbieranie informacji wywiadowczych przez siły podwodne. Podczas II wojny światowej okręty podwodne otrzymały po raz pierwszy wyraźne zadanie

zbierania informacji wywiadowczych. Wydane polecenia można podsumować jako „zdobądź informacje i / lub zdjęcia; unikaj wykrycia za wszelką cenę ”. Tłumaczenie jest proste: nie ważne jak atrakcyjne, nie ogłaszaj swojej obecności atakiem; Twoim celem jest pozostanie w ukryciu i wydobycie pożądanych informacji. To jest dokładnie model dzisiejszych ukierunkowanych ataków polegających na ekstrakcji informacji. Kontrola uszkodzeń to kolejna właściwość sieci z wewnętrznymi partycjami. System zainfekowany przez niewykryty składnik złośliwego oprogramowania będzie miał ograniczoną zdolność do rozprzestrzeniania się wirusa poza swój własny przedział.

Krytyczna dostępność.

Sieci są często krytyczne dla operacji sekundowych. Skutki uboczne źle przemyślanych środków zaradczych mogą być gorsze niż szkody spowodowane rzeczywistym atakiem. Na przykład zamknięcie sieci lub nawet jej części w celu konserwacji lub naprawy może spowodować większe spustoszenie niż penetracja przez złośliwego hakera. Kontrola szkód, często rozpoczynająca się od podziału na grupy, jest krytycznym elementem ograniczania skutków ataku.

Dostępność.

Użytkownicy muszą być zaangażowani w ewolucję zasad i procedur. Dziś nadal nie jest niczym niezwykłym, że wydział uniwersytecki przyjmuje stanowisko, że jakikolwiek stopień bezpieczeństwa podważy samą naturę ich społeczności, zagrażając ich zdolności do prowadzenia badań i dociekań. To skrajne stanowisko utrzymuje się pomimo uwagi mediów, uzasadnionych przekonań społeczności technicznej i udokumentowanych dowodów, że brak ochrony jakiegokolwiek systemu podłączonego do Internetu zagraża bezpieczeństwu całej podłączonej społeczności. Podłączenie wcześniej odizolowanego systemu komputerowego lub sieci do globalnego Internetu tworzy drogę komunikacyjną do każdego zakątka świata. Klienci, partnerzy i pracownicy mogą uzyskiwać informacje, wysyłać wiadomości, składać zamówienia i wchodzić w interakcje 24 godziny na dobę, siedem dni w tygodniu, 365 dni w roku, dosłownie z dowolnego miejsca na Ziemi lub w jej pobliżu. Wahadłowiec miał dostęp do Internetu; podobnie jak Międzynarodowa Stacja Kosmiczna. W tych okolicznościach możliwości ataku lub nieumyślnego niewłaściwego użycia są nieograniczone. Pomimo ogromnego wzrostu liczby połączeń, niektóre firmy i osoby prywatne nie potrzebują szerokiego dostępu do globalnego Internetu w swoich codziennych działaniach, chociaż mogą czuć się urażeni wykluczeniem. Argumentacja za powszechnym dostępem jest zatem kwestią polityki biznesowej i względów

Projektowanie aplikacji.

Ochrona witryny internetowej zaczyna się od najbardziej podstawowych kroków. Po pierwsze, witryna przetwarzająca informacje poufne powinna zawsze obsługiwać protokół HTTPS (Secure Hypertext Transfer Protocol), zwykle przy użyciu portu 443 protokołu kontroli transmisji (TCP). Prawidłowe wsparcie protokołu HTTPS wymaga obecności odpowiedniego certyfikatu cyfrowego. Gdy wymagania dotyczące bezpieczeństwa są niepewne, projekt witryny powinien być błędny po stronie korzystania z protokołu HTTPS do komunikacji. Podsłuchiwanie w Internecie jest zawsze obecnym zagrożeniem. Zdarzały się przypadki manipulacji bazą danych routingu i nadzoru sponsorowanego przez państwo. Epizody Hannaford i TJ Maxx opisane wcześniej w tym rozdziale obejmowały zastosowanie czegoś, co można opisać jedynie jako techniki klasycznej inteligencji sygnałowej (SIGINT). Chociaż szczegóły dotyczące takich ataków często nie są upubliczniane, obszerna literatura historyczna na temat wywiadu komunikacyjnego (COMINT) i SIGINT z okresu II wojny światowej wyjaśnia jedno: Szyfrowanie całego potencjalnie wrażliwego ruchu jest jedynym sposobem ochrony informacji. Szyfrowanie powinno być również stosowane w organizacji, możliwie z innym certyfikatem cyfrowym, do poufnej komunikacji wewnętrznej i transakcji. Wcześniej zauważono, że organizacje nie są monolitycznymi domenami bezpieczeństwa. Nigdzie nie jest to dokładniejsze niż w przypadku zasobów ludzkich, ocen

pracowników, wynagrodzeń, świadczeń i innych wrażliwych informacji o pracownikach. Istnieją pozytywne wymagania, aby te informacje były chronione, ale niewiele organizacji naprawdę zabezpieczyło swoje sieci wewnętrzne przed wewnętrznym monitorowaniem. O wiele bezpieczniej jest kierować całą taką komunikację przez bezpiecznie zaszyfrowane kanały. Takie środki są również wyrazem starań w dobrej wierze o zapewnienie prywatności i poufności informacji wrażliwych. Takie wysiłki są ważnym elementem obrony organizacji w przypadku wystąpienia incydentu. Opieka z góry może znacznie zmniejszyć odpowiedzialność prawną. Brak uwzględnienia tych zagrożeń był przyczyną wielu incydentów, w tym spraw TJ Maxxa i Hannaforda. Ważne jest również, aby unikać podawania wszystkich informacji uwierzytelniających na pojedynczej stronie lub w sekwencji stron. W przypadku ukrywania części informacji, jak na przykład części numeru karty kredytowej lub konta, należy zachować podział na części ukryte i wyświetlane. Wyświetlanie wszystkich informacji, nawet jeśli znajdują się one na różnych ekranach, jest zaproszeniem do naruszenia bezpieczeństwa.

Zaopatrzenie.

Chociaż dzisiejszy sprzęt ma bezprecedensową niezawodność, każda awaria sprzętu między klientem a centrum danych wpłynie negatywnie na obecność przedsiębiorstwa w Internecie. W przypadku strony internetowej pierwszej linii o wysokiej dostępności efektywnym wymogiem są co najmniej dwa zróżnicowane obiekty, każdy z co najmniej dwoma serwerami. Niekoniecznie jest to kosztowna propozycja. Dość wydajne serwery internetowe można kupić za mniej niż 5000 USD, więc całkowity koszt sprzętu na cztery serwery jest rozsądny, znacznie mniejszy niż roczny koszt pojedynczego technika. Przetwarzanie w chmurze, dostępność serwerów wirtualnych w centrum danych jako usługi (np.Amazon, Verizon, RackSpace, Google) stanowi kolejną opcję o niskich kosztach wejścia. W większości przypadków koszt dodatkowego sprzętu jest więcej niż rekompensowany przez biznesowy koszt przestoju, który czasami może przekroczyć całkowity koszt powielanego sprzętu nawet o 100 razy w pojedynczym odcinku. Zduplikowany sprzęt i różnorodność geograficzna zapewniają klientom stały dostęp do pewnego stopnia funkcjonalności. Stopień funkcjonalności, którą należy zachować, zależy od rynku i klientów. Firmy finansowe obsługujące handel akcjami online mają inne wymagania operacyjne, regulacyjne i prawne niż supermarkety. Kluczem jest dopasowanie poziomu wsparcia do działań. Pewien stopień planowanej degradacji jest ogólnie akceptowalny. Całkowita niedostępność nie wchodzi w grę. Usługi zdalnego hostingu określane ogólnie jako „przetwarzanie w chmurze" nie eliminują zagrożeń. Wynajem czasu i innych zasobów od dostawcy zmniejsza kapitał i koszty operacyjne, ale wiąże się to z utratą widoczności i kontroli. Awaria w zdalnym obiekcie obsługiwanym przez sprzedawcę może spowodować przerwanie krytycznej usługi. W zależności od aplikacji, branży, środowiska regulacyjnego i prawnego, ryzyko związane z przetwarzaniem w chmurze może być policzalne lub niewymierne. Trudności w relacjach z dostawcami mogą powodować sytuacje związane z „danymi zakładników". Z punktu widzenia bezpieczeństwa i zapewniania informacji, planowanie z wyprzedzeniem w celu uwzględnienia zmian u dostawców chmury powinno być częścią planowania. Istnieją również nierozwiązane kwestie prawne dotyczące korzystania ze wspólnych urządzeń komputerowych obsługiwanych przez strony trzecie. Jeśli nakaz przeszukania zostanie doręczony w obiekcie wewnętrznym, organizacja będzie wyraźnie świadoma tego, co się stało. Jeśli sprzedawca obiektów wspólnych otrzyma nakaz, pozostaje kwestią otwartą, czy ma on chęć (lub możliwość) do przedstawienia środków ochronnych w sposób przejrzysty i dostępny z danymi przechowywanymi w firmie.

Ograniczenia.

Wszystkie serwery WWW powinny znajdować się za firewallem w strefie DMZ. Usługi przychodzące i wychodzące powinny być ograniczone przy użyciu protokołów, takich jak HTTP, HTTPS i Internet Control Message Protocol (ICMP). Do celów rozwiązywania problemów pożądane jest

zaimplementowanie protokołu ICMP, który jest używany przez PING, requester echa, jako sposób sprawdzania łączności. Wszystkie nieużywane porty powinny być wyłączone. Ponadto wyłączone porty powinny być blokowane przez zapory ogniowe oddzielające strefę DMZ od świata zewnętrznego. Informacje o klientach powinny, w miarę możliwości, być przechowywane w systemach oddzielonych od systemów faktycznie zapewniających obsługę sieci Web. Wiele epizodów związanych z bezpieczeństwem wykorzystywało błędy ochrony plików na serwerach WWW, aby uzyskać bezpośredni dostęp do baz danych. Oddzielenie danych klientów na oddzielnych maszynach i upewnienie się, że jedynym sposobem uzyskania dostępu do danych klientów jest udokumentowane ścieżki, prawdopodobnie poważnie utrudni niewłaściwe próby uzyskania dostępu do informacji i ich modyfikacji. Te zabezpieczenia są szczególnie ważne w przypadku informacji o wysokim stopniu bezpieczeństwa, takich jak numery kart kredytowych. Liczba incydentów, w których przestępcy pobrali numery kart kredytowych bezpośrednio z Serwisu, świadczy o znaczeniu takich środków ostrożności. Systemy faktycznie przechowujące wrażliwe informacje nigdy nie powinny być dostępne z publicznego Internetu. Przechowywanie i przetwarzanie informacji o kartach płatniczych również podlega wytycznym branżowym, w szczególności PCI DSS. Sprawa TJX, na którą zwrócono uwagę opinii publicznej na początku 2007 r., Była jednym z serii włamań na dużą skalę do informacji przechowywanych elektronicznie w systemach back-office i e-commerce. Przede wszystkim wydaje się, że sprawa TJX rozpoczęła się od niedostatecznie zabezpieczonej sieci korporacyjnej i powiązanych z nią systemów zaplecza, a nie od penetracji strony internetowej. Naruszenie to przerodziło się w naruszenie bezpieczeństwa korporacyjnych systemów danych. Na stronie internetowej TJX podano, że co najmniej 45,7 mln kart kredytowych zostało przejętych (oryginalne raporty w USA Today i inne publikacje podają 94 mln numerów kart kredytowych jako przejęte). W dniu 30 listopada 2007 r. Poinformowano, że TJX, organizacja macierzysta sklepów, w tym TJ Maxx i Marshall's, zgodziła się uregulować roszczenia bankowe związane z kartami VISA na kwotę 40,9 mln USD.26 Ponadto od marca 2008 r. Pozew zbiorowy proces w imieniu klientów był w trakcie załatwiania. Wezwał do wniesienia opłat na rzecz każdego ze powodów za monitorowanie kredytu i kradzież tożsamości oraz za licencje dla nowego kierowcy, a także 6,5 miliona dolarów na rzecz obrońcy powoda. Pomimo kilku tak głośnych ataków wydaje się, że nie wyciągnięto wniosków. Jeszcze w marcu 2008 r. Firma Hannaford Bros. Co. poinformowała, że ujawniono 4,2 miliona numerów kart kredytowych, a na ten dzień zgłoszono około 1800 przypadków nieuczciwego użycia. Incydent z udziałem sieci obsługującej konsolę Sony PlayStation 327 ujawnił dane osobowe około 70 milionów subskrybentów. Oczywiście potrzebne są bardziej rygorystyczne kontrole, opieka i zabezpieczenia.

Wiele domen zabezpieczeń.

Serwery sieci Web pierwszej linii oraz serwery baz danych obsługujące ich działania obejmują dwie różne domeny bezpieczeństwa. Jak wspomniano wcześniej, serwery sieci Web muszą być dostępne globalnie za pośrednictwem protokołów HTTP, HTTPS i ICMP (chociaż nie są potrzebne do rzeczywistych operacji, protokół ICMP jest często potrzebny do rozwiązywania problemów z łącznością zarówno przez klientów, jak i dostawców). Z kolei muszą mieć dostęp do serwerów aplikacji lub baz danych i tylko do tych serwerów. W środowisku produkcyjnym zalecane jest, aby serwery aplikacji lub bazy danych współpracowały z serwerami sieci Web za pomocą dedykowanego protokołu o ograniczonym użyciu. Prawidłowo wdrożone ograniczenie takie uniemożliwia przejętemu serwerowi WWW wykorzystanie jego dostępu do aplikacji lub serwera bazy danych. Te serwery drugiego poziomu powinny znajdować się w domenie bezpieczeństwa oddzielonej restrykcyjnymi zaporami ogniowymi od zewnętrznie dostępnych serwerów pierwszej linii sieci Web. Wydaje się to dużym wydatkiem, ale często wiąże się z mniejszymi kosztami i mniejszym ryzykiem niż koszty związane z naprawą pojedynczego znaczącego incydentu.

Co należy ujawnić?

Dostępne publicznie Strony internetowe potrzebują publicznie dostępnych serwerów WWW do wykonywania swoich funkcji. Wyzwaniem jest dostarczenie pożądanych usług społeczeństwu bez jednoczesnego zapewniania dostępu, który można wykorzystać w nieautoryzowany sposób do osłabienia witryny. Incydent związany z penetracją może prowadzić do znacznych strat finansowych, zażenowania oraz finansowej i (w niektórych przypadkach) odpowiedzialności karnej. Ogólnie rzecz biorąc, serwery sieci Web nie powinny być podłączane do publicznego Internetu (chyba że można sprawdzić, czy wszystkie inne porty są zamknięte dla ruchu). Wszystkie połączenia z siecią publiczną powinny być nawiązywane przez system firewall, który powinien być skonfigurowany tak, aby przekazywał do tych hostów tylko ruch sieciowy. Strefa DMZ chroniona przez zaporę ogniową często tworzy łatwiejszą do kontrolowania bramę bezpieczeństwa. Wiele witryn zdecyduje się umieścić serwery sieci Web widoczne z zewnątrz w oddzielnym przedziale bezpieczeństwa, na oddzielnym porcie zapory (jeśli nie w całkowicie oddzielnej zaporze), używając oddzielnej strefy DMZ od innych publicznie dostępnych zasobów. Te środki ostrożności mogą wydawać się przesadne, ale posiadanie niewłaściwie zabezpieczonych systemów może prowadzić do naruszeń bezpieczeństwa, które są niezwykle trudne do naprawienia i mogą prowadzić do dłuższych przestojów podczas analizowania i usuwania problemów. W tym przypadku uncja prewencji jest warta znacznie więcej niż funt lekarstwa.

Systemy odsłonięte.

Odsłonięte systemy stanowią z natury zagrożenie bezpieczeństwa. Systemy bez dostępu z lub do sieci publicznej nie mogą zostać naruszone z sieci publicznej. Tylko systemy, które absolutnie muszą być publicznie dostępne, powinny być tak skonfigurowane. Minimalizacja liczby odsłoniętych systemów jest ogólnie pożądana, ale najlepiej jest rozważać to w kategoriach ról maszyn, a nie faktycznej liczby systemów. Zwiększenie obciążenia każdego publicznie dostępnego serwera poprzez zwiększenie rozmiaru serwera, a tym samym zwiększenie pojemności, na którą ma wpływ pojedyncza awaria systemu, nie jest korzyścią. Należy to jednak zrównoważyć z nowym trendem w kierunku wirtualizacji serwerów, który nie zwiększa rozmiaru serwera, ale zwiększa jego wykorzystanie, w celu obniżenia kosztów i poprawy niezawodności. Wprowadzenie opartych na SSL implementacji i usług VPN obsługujących zdalny dostęp za pośrednictwem bezpiecznych połączeń HTTPS (np. Gotomypc.com) tworzy zupełnie nową klasę zagrożenia bezpieczeństwa. SSL i inne zaszyfrowane techniki zostały wykorzystane do wydobycia danych z penetracji zabezpieczeń. Chociaż zaszyfrowane połączenia mogą być trudne lub niemożliwe do zaobserwowania, połączenia z nieoczekiwanymi lokalizacjami są sygnałem możliwego naruszenia bezpieczeństwa.

Ukryte podsieci.

Serwery bezpośrednio obsługujące Serwis muszą być dostępne ze świata zewnętrznego, a zatem generalnie muszą mieć normalne, widoczne z zewnątrz adresy internetowe. Alternatywnie dyrektorzy ruchu, zapory lub podobne urządzenia mogą mapować numer portu zewnętrznego na adres wewnętrzny i numer portu. Jednak w większości przypadków inne systemy obsługujące serwery internetowe generalnie nie mają uzasadnionej potrzeby nieograniczonego dostępu z lub do sieci publicznej. Najbezpieczniejszymi przypisywanymi adresami dla wspierających, niewidocznych z zewnątrz systemów są adresy IPv4 przydzielone do użytku w prywatnych sieciach internetowych i ich równoważne adresy IPv6. 29 Nie trzeba dodawać, że systemy te powinny znajdować się w przedziale bezpieczeństwa oddzielonym z publicznie dostępnych serwerów internetowych, a przedział ten powinien być odizolowany od przedziału publicznie dostępnego za pomocą bardzo restrykcyjnej zapory ogniowej.

Kontrola dostępu.

Publicznie dostępne systemy są zarówno przedmiotem wysiłków organizacji w zakresie bezpieczeństwa, jak i głównym celem prób złamania tego zabezpieczenia. Liczba osób upoważnionych do wprowadzania zmian w systemach oraz sposoby wprowadzania zmian muszą być uważnie kontrolowane, zgłaszane i monitorowane. Weryfikowane osoby powinny korzystać z kont indywidualnych, a dostęp do funkcji wrażliwych za pośrednictwem takich kont powinien zostać natychmiast unieważniony, jeśli dostęp danej osoby nie jest już autoryzowany lub jeśli pracownik zaprzestaje zatrudnienia, jest badany z powodu niewłaściwego działania lub z innego powodu. Najbardziej wydajnym i skutecznym sposobem implementacji tych wymagań jest kontrola dostępu oparta na rolach, która wykorzystuje podstawowy model ochrony systemu operacyjnego do wymuszenia bezpieczeństwa plików. Kluczowym aspektem ochrony opartej na rolach jest to, że dostęp do plików jest chroniony rolą, a nie identyfikatorem. W ten sposób można usunąć dostęp użytkownika do plików produkcyjnych za pomocą jednego polecenia. Kontrola dostępu to nie tylko kwestia tradycyjnej kontroli opartej na rolach. Coraz częściej klienci mają bezpośredni dostęp do aplikacji. Taki bezpośredni dostęp wymaga więcej środków ostrożności i staranności niż personel obsługi klienta. Często personel obsługi klienta powinien mieć dostęp do większości kont; równie niewłaściwe jest udzielanie odpowiedniego, nieograniczonego dostępu klientom końcowym, którzy powinni mieć dostęp tylko do swojego konkretnego konta. Ataki na poziomie aplikacji (np. Wstrzyknięcie SQL) stają się coraz bardziej niebezpieczne. Przejście na interfejsy oparte na przeglądarce internetowej i urządzeniach mobilnych wymaga dodatkowych środków ostrożności. Klienci zdalni podlegają kompromisom i inżynierii wstecznej. Na przykład, używając zwykłego tekstu, informacje dostarczone przez klienta w celu kontroli dostępu (np. Pliki cookie lub zakodowane w adresie URL) mogą łatwo doprowadzić do ataku SQL (lub równoważnego), po prostu edytując niezakodowane informacje. Przełączenie na odpowiedni zmienny, oparty na sesjach schemat numerowania sprawiłby, że manipulacje byłyby znacznie mniej skuteczne (w rzeczywistości większa liczba błędów wynikających z zastosowania takiej nieprzezroczystej liczby byłaby łatwo wykrywalna przez aplikacje i systemy rejestrowania bezpieczeństwa). Wyzwaniem dla takich systemów jest to, że zabezpieczenia muszą być wdrożone w aplikacji. Takie zabezpieczenia są potrzebne, aby zapewnić bezpieczeństwo aplikacji. Tego typu ataki typu SQL injection miały miejsce w dużych organizacjach. W 2011 roku dane 200 000 rachunków kart kredytowych w Citibanku zostały w ten sposób przejęte.

Konserwacja witryny.

Utrzymywanie i aktualizowanie Witryny wymaga dużej staranności. Bezpośredni charakter sieci WWW sprawia, że błąd jednoznakowy w dużej aplikacji korporacyjnej może w ciągu kilku chwil spowodować szkody o wartości setek tysięcy dolarów. Serwery internetowe należy traktować z szacunkiem; całe przedsiębiorstwo jedzie na elektronicznym obrazie wyświetlanym przez serwer. Cyberwandalizm, który najczęściej polega na zniszczeniu strony głównej znanej witryny, wymaga nieautoryzowanej aktualizacji plików wchodzących w jej skład. Tylko w 2000 r. Poszkodowane zostały w ten sposób znane podmioty publiczne i prywatne, w tym FBI, OPEC, Światowa Organizacja Handlu i NASA, a także instytucje edukacyjne, w tym Uniwersytet w Limerick. Ataki te nadal stanowią zagrożenie, zarówno jeśli chodzi o uszkodzenie wizerunku organizacji, jak i potajemnie, ponieważ wykorzystuje witrynę WWW jako platformę startową dla exploitów internetowych. Internet jest z natury środowiskiem o wysokim stopniu dźwigni. Niewielkie zmiany w zawartości jednej strony pojawiają się w całej sieci w ciągu kilku minut. Informacje są rozpowszechniane łatwo i szybko przy niskich kosztach. Dźwignia bardzo pomaga, gdy sprawy idą dobrze; kiedy sprawy idą źle, dźwignia dramatycznie potęguje szkody.

Utrzymanie integralności witryny.

Celem jest EveryWebsite i jej serwery. Antagonistami mogą być studenci, aktywiści, terroryści, niezadowoleni byli pracownicy lub niezadowoleni klienci, a także podmioty państwowe. Ponieważ

strony internetowe są najbardziej publiczną twarzą przedsiębiorstwa, stanowią niezwykle pożądane cele. Utrzymanie integralności wymaga, aby aktualizacje i zmiany w witrynie były przeprowadzane w zdyscyplinowany sposób. Dostęp do zapisu w witrynie musi być ograniczony, a osoby upoważnione muszą korzystać z bezpiecznych metod dostępu do serwerów internetowych. Wydaje się, że większość zgłoszonych incydentów jest wynikiem słabych zabezpieczeń procesu aktualizacji. Na przykład niezabezpieczony dostęp FTP z ogólnego Internetu jest złą praktyką. Bezpieczniejsze mechanizmy obejmują:

* FTP z określonego węzła w wewnętrznej zaporze

* KERMIT na bezpośrednio przewodowym porcie lub przez zabezpieczone połączenie

* Loginy i transfery plików (np.SFTP) przez bezpieczne uwierzytelnione połączenia za pośrednictwem podstawowego transportu SSH

* Fizyczne transfery mediów

Większość technologii z natury nie wymaga, aby osoba na miejscu przeprowadzała aktualizacje serwera, co wykluczałoby zdalną konserwację. Oznacza to, że aby dostać się do maszyny, z której można przeprowadzić aktualizację, konieczne jest przejście przez wirtualną sieć prywatną z protokołem tunelowania punkt-punkt lub protokołem tunelowania warstwy 2 (VPN PPTP / L2TP) uwierzytelnionym przez at co najmniej jedną z bezpiecznych bram

KWESTIE TECHNICZNE.

Z ochroną zasobów dostępnych w Internecie wiąże się wiele problemów technicznych. Technologie używane do ochrony zasobów sieciowych obejmują routery, zapory, serwery proxy, nadmiarowość i rozproszenie. Właściwie zaprojektowane i wdrożone środki bezpieczeństwa tworzą pętlę pozytywnego sprzężenia zwrotnego, w której ulepszenia w zakresie bezpieczeństwa i solidności sieci wzmacniają się same. Każde ulepszenie sprawia, że inne ulepszenia są możliwe i skuteczniejsze.

Wewnątrz / Na zewnątrz.

Niektóre wizje przyszłości obejmują utopijny świat, w którym wszystko jest bezpośrednio dostępne z dowolnego miejsca, bez wysiłku i tylko z korzystnymi rezultatami. Pierwotny Internet działał na tej podstawie, dopóki szereg incydentów (w tym Morrisworm z 1988 r.) Nie zmusił ludzi do ponownego przemyślenia postrzeganego wewnętrznego spokoju świata sieciowego. To trend, który tylko przyspieszył, jako suma liczb systemów rośnie. Architektura i projekt środków ochronnych dla sieci zależą od rozróżnienia wewnątrz zaufanych systemów od zewnętrznych niewiarygodnych systemów. Dotyczy to również intranetów, Internetu czy ekstranetu, czyli tzw. Rozróżnienia prywatnych połączeń sieci od publicznego Internetu. Niestety zaufanie nie jest kwestią czarno-białą. System może być godny zaufania z jednej perspektywy i niewiarygodny od innego, komplikując w ten sposób projekt zabezpieczenia. Ponadto uważa się, że zdecydowana większość niewłaściwego użytkowania komputera jest dokonywana przez osoby mające legalny dostęp do niektórych aspektów systemu i jego danych. Alternatywnie, nie wszędzie można być silnym. Zaufane, ale skompromitowane systemy stanowią poważne zagrożenie. Podstawowa konfiguracja łączności to jeden z niewielu obszarów, które są czysto techniczne, bez elementu ryzyka biznesowego. Jednym z najbardziej oczywistych elementów są tablice zaimplementowane w routerach łączących przedsiębiorstwo z publicznym łączem IP dostarczanym przez operatora. Reguły tabeli muszą zapobiegać fałszowaniu adresu IP, czyli fałszywej interpretacji pochodzenia pakietów IP. Dotyczy to również sytuacji, gdy pomysłodawcy są w organizacji. Istnieją trzy podstawowe zasady zapobiegania fałszowaniu adresów IP, mające zastosowanie do wszystkich prawidłowo skonfigurowanych sieci:

1. Pakiety wchodzące do sieci z zewnątrz nigdy nie powinny mieć adresów nadawcy w sieci docelowej.

2. Pakiety opuszczające sieć i przechodzące do sieci publicznej muszą mieć adresy nadawcy w sieci źródłowej.

3. Pakiety opuszczające sieć i przechodzące do sieci publicznej nie mogą mieć adresów docelowych w sieci źródłowej.

Wyjątkiem od tych reguł jest korzystanie z ukrytych sieci wewnętrznych, których adresy wewnętrzne odpowiadają legalnym adresom zewnętrznym. Następstwem tych reguł jest to, że pakiety z adresami nadawcy lub docelowymi w najbardziej lokalnym zakresie adresów intranetowych lub dynamiczne adresy IP nigdy nie powinny mieć możliwości wchodzenia do sieci wewnętrznej ani jej opuszczania. Zagnieżdżone przestrzenie adresowe mogą celowo tworzyć aliasowane przestrzenie adresowe

Ukryte podsieci.

Zapory sieciowe kierują ruch sieciowy przez jeden lub więcej wąskich gardeł, koncentrując zadanie bezpieczeństwa w niewielkiej liczbie systemów. Przyczyną takiej koncentracji jest gwałtowny wzrost prawdopodobieństwa naruszenia bezpieczeństwa całej sieci wraz z liczbą niezależnych punktów dostępowych. Zapory i serwery proxy działają tylko w topologiach, w których zapora filtruje cały ruch między chronionymi systemami a mniej zaufanym światem poza jej granicami. Jeśli w jakikolwiek sposób można uzyskać dostęp do chronionych systemów bez przechodzenia przez zaporę, oznacza to, że sama zapora stała się nieistotna. Audyty bezpieczeństwa często ujawniają systemy, które naruszają tę politykę; poleganie na sankcjach administracyjnych w celu wykluczenia takich luk w granicach bezpieczeństwa generalnie nie działa. Obowiązuje zasada międzynarodowej dyplomacji „Ufaj, ale sprawdzaj”. Najprostszym rozwiązaniem tego problemu jest użycie adresów RFC 191837 w sieciach chronionych.38 RFC1918 zapewnia szereg adresów IPv4, których organizacja IANA gwarantuje, że nigdy nie pojawią się w normalnym, publicznym Internecie. Zakresy adresów używane do dynamicznego przypisywania adresów IP mają podobne właściwości. Sieci IPv6 są podobnie regulowane przez RFC 4193. Filtrowanie tych adresów zarówno w przychodzących, jak i wychodzących strumieniach danych jest proste i bardzo skuteczne w powstrzymywaniu szerokiego zakresu ataków. Wymóg korzystania z takich adresów i zakazywanie wewnętrznego korzystania z adresów zewnętrznych, które są ważne, znacznie przyczyniają się do zapobiegania używaniu nieautoryzowanych protokołów i połączeń.

Co należy ujawnić?

Wdrażanie zabezpieczeń rozpoczyna się od analizy misji, potrzeb i wymagań przedsiębiorstwa. Wszystkie projekty i wdrożenia są kompromisem pomiędzy absolutnym bezpieczeństwem, osiągniętym tylko w systemie wyłączonym lub odłączonym, a całkowitą otwartością, w której system jest całkowicie otwarty na każdy dostęp z zewnątrz. Chociaż w większości przypadków należy umożliwić komunikację między przedsiębiorstwem a światem zewnętrznym dla normalnych funkcji biznesowych, całkowite odłączenie, znane jako szczelina powietrzna, jest czasami potrzebne i odpowiednie między określonymi komponentami. Przemysłowe systemy sterowania w czasie rzeczywistym, systemy krytyczne dla życia i systemy o wysokich wymaganiach poufności pozostają odpowiednimi kandydatami do całkowitej szczeliny powietrznej. Często systemy, które nie muszą otrzymywać informacji ze źródeł zewnętrznych, muszą publikować informacje statystyczne lub inne informacje w mniej bezpiecznych systemach. Wymaganie to często można spełnić poprzez wykorzystanie łączy o ograniczonej funkcjonalności, takich jak wymiana mediów, lub poprzez ściśle kontrolowane transfery w jedną stronę. Mechanizmy te można wdrożyć z technologiami związanymi z własnością intelektualną lub z bardziej ograniczonymi technologiami, w tym KERMIT, UUCP lub rozwiązaniami specyficznymi dla

dostawcy. W innych przypadkach ograniczenia odzwierciedlają zasady dotyczące dozwolonego użytku i dostępu, a nie ochronę przed atakiem z zewnątrz. Na przykład rozsądne i właściwe jest, aby biblioteka publiczna ograniczała dostęp do protokołów HTTP i pokrewnych, jednocześnie zabraniając dostępu do takich obiektów, jak FTP i TELNET. Dostęp zdalny przy użyciu protokołu Secured Shell Protocol (SSH) jest niezwykle przydatny, ponieważ umożliwia uwierzytelnianie dwukierunkowe (zarówno klient, jak i serwer mogą być uwierzytelniani za pomocą kluczy publicznych / prywatnych). Istnieje dodatkowa kwestia dotycząca tego, jakie przepisy należy wprowadzić, aby systemy w granicach obszaru łączyły się z sieciami zewnętrznymi przy użyciu różnych protokołów. Najbardziej znane są PPTP i L2TP. To, czy te metody dostępu do sieci zewnętrznych powinny być dozwolone, czy też nie, jest kwestią niemałego znaczenia, równoważną całkowitemu wyeliminowaniu komunikacji zewnętrznej. Z punktu widzenia bezpieczeństwa tunele prowadzące do świata zewnętrznego są idealną burzą, potencjalnie umożliwiającą nieograniczoną, niemonitorowaną komunikację na zewnątrz. Z punktu widzenia umożliwienia prowadzenia działalności taki dostęp może być praktyczną koniecznością. Sprzedawcy, wykonawcy, dostawcy i klienci wszyscy potrzebują dostępu do systemów wewnętrznych w swoich organizacjach, a taki dostęp zawsze będzie wymagał użycia tunelu VPN. Być może najlepszym rozwiązaniem jest odwrócenie tradycyjnej dychotomii wewnątrz / na zewnątrz, czyniąc LAN niezaufaną siecią. Sieć LAN staje się wówczas uniwersalnym sygnałem wybierania. Dostęp do wewnętrznych systemów korporacyjnych można wtedy zabezpieczyć oddzielnie za pomocą technologii VPN. Pojawienie się tuneli opartych na protokole SSL / HTTP stanowi kolejne wyzwanie. gotomypc.com oferuje taką usługę, a osoby prywatne wykorzystywały ją do omijania zapór ogniowych i zaimplementowania zdalnego dostępu ad hoc. Koszt jest nominalny, często stanowi niewielką część miesięcznych wydatków bieżących na codzienne dojazdy do biura. Rozwiązanie polegające na blokowaniu połączeń na adresy IP przypisane takiemu dostawcy jest często zalecaną, ale z natury wadliwą, profilaktyką. Zablokowanie jednej lub więcej takich usług nie zabezpiecza sieci przed jeszcze niezidentyfikowaną usługą tego typu, taką jak usługa hostowana na serwerze domowym. Ograniczanie czasu trwania połączeń SSL jest również jedynie przyspieszeniem w przypadku takich schematów. Pozostają one wyzwaniem, podobnie jak pojawienie się bezpośrednio użytecznych tuneli SSL / HTTP komunikujących się przy użyciu standardowych portów HTTP (port TCP 80) i HTTPS (port TCP 443). W takich przypadkach firewalle są rozsądnym rozwiązaniem, o ile rozpoznawane są ich ograniczenia. Na przykład zapory nie uniemożliwiają kodom mobilnym, takim jak Active-X i JAVA, obchodzenia się z niedozwolonymi funkcjami. Opublikowano ataki sieciowe wykorzystujące kod dostarczany do przeglądarek w celu wykonania lokalnego w kontekście sieci lokalnej. Ataki te mogą utrzymywać się w czasie i stanowią jedną z klas ataków w tak zwanym spektrum zaawansowanych trwałych zagrożeń. Taki kod w połączeniu ze słabymi praktykami bezpieczeństwa infrastruktury sieciowej może spowodować poważne szkody

Wiele domen zabezpieczeń.

Wiele sieci wdraża zabezpieczenia wyłącznie w punkcie wejścia, gdzie sieć organizacji łączy się z publicznym Internetem. Takie monolityczne zapory ogniowe nie są skutecznym wyborem dla wszystkich, z wyjątkiem najprostszych małych organizacji. Na początek systemy dostępne dla ogółu ludności powinny znajdować się poza obszarem bezpieczeństwa wewnętrznego na ziemi niczyjej między publicznym Internetem a prywatną siecią wewnętrzną. Taka izolacja jest określana jako strefa zdemilitaryzowana (DMZ). Systemy te powinny mieć pewien stopień ochrony poprzez umieszczenie ich pomiędzy zewnętrzną zaporą ogniową (chroniącą strefę zdemilitaryzowaną przed siecią publiczną) a wewnętrzną zaporą ogniową (chroniącą sieć wewnętrzną przed siecią publiczną i kontrolując komunikację między publicznie dostępnymi serwerami znajdującymi się w DMZ do sieci wewnętrznej). Alternatywnie strefa DMZ może być ślepą uliczką połączoną z oddzielnym portem na pojedynczej zaporze przy użyciu innego zestawu reguł zarządzania ruchem. Taka topologia pozwala na

implementację różnych ograniczeń bezpieczeństwa mających zastosowanie do obu sieci. Podejrzane powinny być również systemy zlokalizowane w strefie DMZ, ponieważ stanowią one cel kompromisu. Chociaż cała branża zgadza się co do potrzeby konfiguracji DMZ, mniej docenia się, że takie ograniczenia mają również miejsce w organizacjach. Różne grupy, działy i funkcje w organizacji mają różne wymagania dotyczące bezpieczeństwa i dostępu. Na przykład w firmie świadczącej usługi finansowe wymagania dotyczące bezpieczeństwa różnią się znacznie w poszczególnych działach. Trzy oczywiste przykłady działów o różnych wymaganiach to personel, fuzje i przejęcia oraz badania i rozwój. Dział personalny jest opiekunem szerokiego zakresu wrażliwych informacji o firmie, jej pracownikach i często osobach z zewnątrz, które albo regularnie przebywają na terenie firmy, albo regularnie współpracują z firmą przy projektach. Niektóre z tych informacji, takie jak adresy zamieszkania, poziomy płac i tablice rejestracyjne, są poufne ze względów osobistych lub kulturowych. Inne informacje narażają organizację na sankcje prawne lub regulacyjne, jeśli zostaną nieprawidłowo ujawnione lub wykorzystane. W Stanach Zjednoczonych przykłady danych wrażliwych obejmują numery ubezpieczenia społecznego, wiek, orientację seksualną i obecność ludzkiego wirusa niedoboru odporności (HIV) lub inne dane medyczne. Jeszcze inne informacje mogą podlegać określonym prawnym lub umownym przepisom dotyczącym poufności.

Dział fuzji i przejęć obsługuje różnego rodzaju poufne informacje. Informacje o negocjacjach biznesowych lub planach na przyszłość podlegają ścisłym wymogom poufności. Ponadto ujawnienie takich informacji podlega różnym przepisom na szczeblu rządowym i branży papierów wartościowych. W dziale fuzji i przejęć dostęp do informacji często musi być konieczny, zarówno w celu ochrony transakcji, jak i ochrony firmy przed narażeniem na odpowiedzialność cywilną i karną. Niektóre informacje w dziale badań i rozwoju są całkowicie jawne, podczas gdy inne informacje są w różnym stopniu ograniczone. Pełne wdrożenie odpowiedniego środowiska bezpieczeństwa będzie wymagało zabezpieczeń, które nie tylko różnią się logicznie w zależności od działu, ale także wymagają wzajemnej ochrony różnych działów. Dlatego też, jeśli nie jest to topologicznie niemożliwe, pojedyncza zapora ogniowa, znajdująca się na połączeniu ze światem zewnętrznym, może wdrożyć wymagane środki bezpieczeństwa. Trudno jest zapewnić, że szkielet korporacyjny jest wolny od potajemnego monitorowania. Ponadto nawet autoryzowane monitorowanie może tworzyć dzienniki komunikacji zawierające wrażliwe chronione informacje. Dzienniki sieciowe stają się wtedy zagrożeniem same w sobie. Zabezpieczanie systemów w izolowanych obszarach logicznych jest przykładem niezbędnej nieufności, a jedynie kwestia zapewnienia, że interakcje między systemami stron trzecich a światem zewnętrznym są dozwolone w takim zakresie, w jakim są oczekiwane. Jako przykład rozważ prostą sytuację w Hipotetycznym Domu Maklerskim. Hipotetyczny dom maklerski korzysta z dwóch sieci handlowych, Omega i Gamma.

Na pierwszy rzut oka wydaje się, że byłoby dopuszczalne umieszczenie bram sieciowych Omegi i Gamma w zwykłej strefie DMZ, razem z serwerami WWW firmy Hypothetical. Jednak daje to duże zaufanie firmom Omega i Gamma oraz całemu ich personelowi, dostawcom i wykonawcom. Najważniejszym pytaniem operacyjnym jest to, czy istnieje wiarygodne zagrożenie. Każda z dwóch bramek jest dobrze usytuowana, aby:

- Monitorować ruch komunikacyjny do i z serwerów WWW firmy Hypothetical
- Monitorować ruch między Hypothetical a inną, konkurencyjną siecią
- Zaatakować drugą bramę
- Przerwać komunikację do i z drugiej bramy

Sieć Attack Hypothetical

Dostawcy sieci również stanowią atrakcyjną opcję ataku. Pojedyncze włamanie do komponentu systemu dostarczonego przez dostawcę sieci skutkuje naruszeniem bezpieczeństwa dużej liczby witryn użytkowników końcowych. Istnieje bogata historia preferowanych celów przełączników prywatnych (PBX) i publicznych (należących do operatora). Routery SOHO dostarczone przez dostawcę ze zdalnym zarządzaniem lub funkcją Wi-Fi mogą również stać się wektorem ataku, jeśli konfiguracja dostarczona przez dostawcę jest wadliwa lub jeśli hasła zarządzania wygenerowane przez dostawcę zostaną naruszone. Rozwiązaniem jest odizolowanie systemów innych firm w oddzielnych strefach DMZ, przy czym ruch między każdą z DMZ a resztą sieci jest skrupulatnie sprawdzany pod kątem protokołu kontroli transmisji i protokołu datagramów użytkownika (TCP / UDP), numeru portu i źródła i adresy docelowe, aby upewnić się, że cały ruch jest autoryzowany. Jedną z metod jest użycie pojedynczej zapory z wieloma portami sieci lokalnej (LAN), z których każdy ma inne reguły filtrowania, w celu przekształcenia oryginalnej pojedynczej strefy DMZ firmy Hypothetical w rozłączne, chronione strefy DMZ.

Podział na przedziały.

Podział sieci na oddzielne przedziały bezpieczeństwa zmniejsza ryzyko całkowitego załamania sieci. Ograniczenie potencjalnych szkód spowodowanych incydentem jest ważnym krokiem w rozwiązywaniu problemów. Ta sama zasada dotyczy stref DMZ. Na przykład w przedsiębiorstwach zajmujących się handlem finansami lub produkcją często zdarza się, że bramy reprezentują punkty dostępu do sieci handlowych i partnerskich. Problematyczne jest umieszczenie tych przyjaznych systemów. Wiele organizacji zdecydowało się umieścić te systemy w swojej zwykłej strefie DMZ. Witryny z opóźnieniem odkryły, że takie bramy czasami okazały się działać jako routery, przejmując tę funkcję od zamierzonych routerów. W innych przypadkach bramy działały nieprawidłowo i zakłócały działanie pozostałej części sieci (lub strefy zdemilitaryzowanej). Jak zawsze, jedynymi pewnymi rozwiązaniami są wyłączenie lub izolacja. Podział na przedziały zapobiega również kaskadowaniu wypadków. Awaria pojedynczej bramy prawdopodobnie nie rozprzestrzeni się w całej sieci, ponieważ nieoczekiwany ruch zostanie zatrzymany przez zaporę ogniową izolującą bramę od sieci. Takie zdarzenie może wywołać alarmy ataku zapory. Problem z siecią nie ogranicza się do węzłów dostarczanych z zewnątrz. Błędny system działający w sieci pozbawionej przedziałów, znajdującej się w zewnętrznej strefie bezpieczeństwa, może siać spustoszenie w całej korporacji. Skonstruowanie sieci jako szeregu zagnieżdżonych i powiązanych ze sobą domen bezpieczeństwa, z których każda jest chroniona przez odpowiednie zapory ogniowe, lokalizuje wpływ nieuniknionych incydentów, podczas gdy sieć bez przedziałów umożliwia rozprzestrzenianie się infekcji w całej organizacji. Większe sieci dramatycznie podnoszą koszty incydentu. Można sobie wyobrazić, że cały budżet przeznaczony na podział sieci korporacyjnej będzie mniejszy niż koszt jednej godziny przestoju wynikającego z pierwszego błędnego systemu. Łatwa dostępność przenośnych urządzeń pamięci masowej, w tym pamięci USB i zewnętrznych dysków twardych, sprawia, że podział na segmenty jest jeszcze poważniejszym problemem. Exploity pokazały celowość wyłączenia automatycznego wykonywania oprogramowania przechowywanego na urządzeniach typu plug-in.

Konieczność dostępu.

Czasami łatwo jest określić, kto potrzebuje dostępu, do jakich zasobów i do jakich informacji. Jednak kwestia kontroli dostępu często wiąże się z bolesnymi wyborami, z wieloma niuansami i subtelnościami. Odpowiedzialność prawna i umowna dodatkowo komplikuje sprawę. Na przykład brak dostępu może uniewinnić osoby podejrzewane o niewłaściwe wykorzystanie informacji. Fizyczne i logiczne kontrole dostępu należy wdrożyć w przypadku systemów dostępnych w Internecie, podobnie jak w przypadku każdego innego wrażliwego i krytycznego systemu. Kontrole takich systemów muszą być egzekwowane i przestrzegane przez wszystkich członków organizacji. Ważne jest, aby personel o

ograniczonym dostępie do sieci i infrastruktury bezpieczeństwa rozumiał i rozumiał powody wprowadzenia zasad bezpieczeństwa i nie podejmował środków pozwalających na obejście tych zasad. Integralność zapór sieciowych i infrastruktury sieciowej organizacji jest tak dobra, jak fizyczne i logiczne bezpieczeństwo personelu, sprzętu, infrastruktury i systemów składających się na zaporę i sieć. Regularne kontrole fizycznego i logicznego dostępu do zasobów infrastruktury są krytyczne i konieczne. Rozsądne jest również skanowanie w poszukiwaniu nieautoryzowanych (fałszywych) punktów dostępu Wi-Fi. Tak jak w przeszłości z modemami telefonicznymi; fałszywe punkty dostępu Wi-Fi mogą zagrozić całej organizacji bezpieczeństwa. Potrzeba utrzymania bezpieczeństwa informacji w komunikacji wewnątrz organizacji przemawia za szerokim wykorzystaniem technologii bezpieczeństwa, nawet jeśli pakiety danych nigdy nie opuściłyby siedziby. Rozsądne planowanie, nawet w przedsiębiorstwie, wymaga, aby aplikacje z wymaganiami prywatności lub poufności korzystały z infrastruktury prywatności, takiej jak Secure Sockets Layer (SSL) dla aplikacji internetowych lub tunelowania, takich jak Layer 2 Tunneling Protocol44 i Point-to -Point Tunneling Protocol. Pomaga to zapewnić, że dystrybucja poufnych informacji jest ograniczona. Nie trzeba dodawać, że w tych podejściach należy stosować wysokiej jakości szyfrowanie i odpowiednio podpisane certyfikaty X.509 od dobrze uznanych urzędów certyfikacji. Nie należy używać certyfikatów z podpisem własnym, które utraciły ważność i nie są powszechnie akceptowane.

Odpowiedzialność.

Ludzie często mówią o nieprzeniknionych systemach. Pomimo analogii z zamkiem i fosą, które są używane w wielu dyskusjach o bezpieczeństwie, obwody są niedoskonałe. Biorąc pod uwagę prawdopodobieństwo udanych ataków, pracownicy ochrony muszą stosować środki techniczne i zarządcze w celu skutecznej reakcji. Zabezpieczając infrastrukturę, należy priorytetowo traktować środki ochronne, które zapewniają rozliczalność działań. Tak jak pożądane jest zapobieganie niewłaściwym działaniom, jeszcze ważniejsze jest zapewnienie, że można je policzyć. Na przykład istnieje wiele sposobów przeprowadzania ataków typu „odmowa usługi". Najbardziej kłopotliwe są te, które są całkowicie legalne. Chociaż niektóre z tych ataków, takie jak rozproszona odmowa usługi, są wojownicze lub motywowane politycznie i ideologicznie i obejmują zdalnie sterowane programy zombie i botnety, wiele przypadkowych ataków DoS może wystąpić bez złośliwości w trakcie tworzenia oprogramowania. Na przykład dwa najbardziej znane robaki, które nieumyślnie doprowadziły do DoS, robak Morris i robak WANK, zostały wykryte nieumyślnie w wyniku błędów implementacji w ich mechanizmach replikacji. Błędy te spowodowały, że oba robaki bardzo szybko się rozprzestrzeniły, skutecznie powodując niezamierzone ataki DoS i późniejsze wykrycie. Podczas analizy kryminalistycznej zaatakowanej maszyny obecność ataku może pozostać niewykryta. Jest to szczególnie prawdziwe, gdy atak dotyczy szkodliwego oprogramowania projektanta, którego nie ma w ogólnym obiegu. Ważne jest, aby przeanalizować naruszenia bezpieczeństwa, aby rozróżnić ataki, wypadki i eksperymenty. Lepiej jest odkryć, choćby przypadkowo, słabości organizacji, niż zająć się naprawdę wojowniczym naruszeniem bezpieczeństwa. Zasady i praktyki powinny zatem zachęcać pracowników do zgłaszania wypadków, zamiast próbować je ukrywać. Jeśli chodzi o fałszywe alarmy wywoływane przez nadmiernie entuzjastycznych neofitów zajmujących się bezpieczeństwem, kierownictwo powinno unikać karania tych, którzy zgłaszają iluzoryczne naruszenia lub ataki. Odpowiedzialność zapewnia surowiec do ustalenia, co faktycznie się wydarzyło. Uzyskane w ten sposób informacje stanowią kluczową podstawę analizy i edukacji, umożliwiając w ten sposób przedsiębiorstwu ewolucję na wyższy poziom bezpieczeństwa i integralności.

Bezpieczeństwo plików tylko do odczytu.

Wiele witryn umożliwia pobieranie, zwykle przez FTP i HTTP, dużej liczby plików. Pliki te mogą zawierać kopie formularzy, instrukcji, instrukcji, map i przewodników serwisowych. Jeśli takie udostępnianie plików jest zapewniane, ważne jest, aby upewnić się, że:

* Serwery obsługujące usługę pobierania są bezpieczne.

* Zawartość publicznie dostępnego magazynu plików jest tylko do odczytu i może podlegać kontroli zmian.

* Cała zawartość publicznego magazynu plików może zostać szybko przywrócona w przypadku możliwego kompromisu.

* Istnieje wyraźnie wyznaczona strona odpowiedzialna za utrzymanie i ochronę usługi plików publicznych.

Przechodzenie w tryb offline.

Systemy połączone z Internetem wymagają szybkości reakcji, która jest bezpośrednio związana z kosztami przestoju. Może to być koszt utraconego biznesu; w innych organizacjach kosztem może być stracony czas zawodowy, zniszczone relacje z mediami i obniżone morale. W każdym razie im większy odsetek organizacji (lub jej klientów) dotkniętych problemem, tym wyższe koszty i większa pilność wykonania napraw. Dzisiejszy świat wzajemnych połączeń sprawia, że rozłączanie się z Internetem jest naprawdę bolesną opcją dla menedżera sieci lub bezpieczeństwa. Chociaż koszt odłączenia (lub częściowego odłączenia) może sięgać setek tysięcy dolarów w przypadku utraty działalności i produktywności, odłączenie w pewnych sytuacjach jest zarówno konieczne, jak i właściwe. Czasami odłączenie stanowi najtańszy i najskuteczniejszy sposób ochrony użytkowników, systemów i społeczeństwa. W dniu 4 maja 2000 r., podczas epidemii „I Love You", Microsoft Outlook - wykorzystujący atak wirusów, menedżerowie sieci w Ford Motor Company odłączyli sieć Forda od świata zewnętrznego, aby ograniczyć przedostawanie się zanieczyszczonych wiadomości e-mail do systemów Forda i zapobiec Systemy Forda przed rozprzestrzenianiem się zakażenia. Odpowiedź osiągnęła swoje cele. Odłączenie skutkowało mniejszym bólem niż rozwiązania alternatywne. Sieci podzielone na segmenty pomagają zapewnić podział na segmenty, umożliwiając bardziej szczegółową odpowiedź niż zwykłe odłączenie. Podstawowym problemem związanym z rozłączaniem jest: Co można odłączyć? Kto ma władzę? Prawo Murphy'ego często interweniuje. Takie ważne incydenty wymagają krótkich czasów reakcji, nieuchronnie w przypadkach, gdy menedżerowie wyższego szczebla nie są dostępni. Najlepszym sposobem zabezpieczenia tej sytuacji awaryjnej jest dostarczenie wytycznych dla personelu posiadającego uprawnienia do obrony systemów oraz zagwarantowanie, że działania zgodne z wytycznymi będą odporne na odwet. Jeśli organizacja nie zezwoli na takie działania, zrzeka się również korzyści wynikających z działań mających na celu powstrzymanie szkód.

Audyt.

W każdej organizacji należy monitorować i analizować wykorzystanie obiektów, w tym aktywność sieciową. Ponieważ osoby zainteresowane atakiem lub niszczeniem sieci przedsiębiorstwa będą atakować, kiedy zechcą, takie monitorowanie i analiza muszą być częścią ciągłego procesu. Bieżąca obserwacja i przegląd powinny obejmować:

* Fizyczna infrastruktura komunikacyjna

* Zapory, tabele routerów i reguły filtrowania

* Bezpieczeństwo hosta

* Bezpieczeństwo plików

* Wzorce ruchu w sieciach szkieletowych, strefach DMZ i innych segmentach sieci

* Fizyczne bezpieczeństwo systemów i infrastruktury komunikacyjnej

Obszary te są synergiczne i niezależne. Są synergiczne, ponieważ połączenie ich wszystkich wzajemnie się wzmacnia w promowaniu bezpiecznego środowiska komputerowego. Są niezależne, ponieważ każdy z nich może stanowić słaby punkt w bezpiecznym środowisku.

Nowe technologie.

Nowe technologie w dalszym ciągu zmieniają wyzwania na arenie technologii internetowych. Jedno z takich wyzwań pojawia się przy korzystaniu z zapór ogniowych opartych na SSL / TLS. Korzystanie z protokołu HTTPS jako podstawy do budowania zaszyfrowanych tuneli wydaje się na pierwszy rzut oka niesamowitą technologią. Większość zapór ogniowych zezwala na inicjowanie połączeń ze strefy chronionej na porcie TCP 443 w celu umożliwienia połączenia z wieloma różnymi witrynami internetowymi, które wymagają zabezpieczenia informacji, o czym wspomniano w innych miejscach w tym rozdziale. Ze względu na prywatność i bezpieczeństwo taki ruch powinien być nieprzejrzysty do monitorowania. Użycie protokołu HTTPS jako podstawy tunelowania zapewnia również dostosowaną do potrzeb technikę nadużyć. Na przykład takie technologie umożliwiają zainfekowanemu komputerowi stacjonarnemu monitorowanie sieci, wyodrębnianie interesujących go danych i bezpieczne przesyłanie wynikowych danych do lokalizacji zewnętrznej przez zaporę ogniową. Nieprzezroczysty charakter połączenia opartego na protokole SSL / TLS uniemożliwia skanowanie wychodzących danych. Ta technologia może z powodzeniem stanowić koniec sieci LAN korzystających ze współdzielonej łączności. Coraz ważniejsze jest zabezpieczenie infrastruktury sieciowej przed atakami, które umożliwiają nieuczciwej maszynie gromadzenie danych poprzez monitorowanie ruchu sieciowego. Konieczne może być również przeprojektowanie systemów wykrywania włamań, aby zidentyfikować połączenia HTTPS o znacznym natężeniu ruchu w celu wykrycia oznak włamania lub nadużycia. W celu ochrony przed takimi atakami i nadużyciami konieczne może być podejście, które traktuje całą sieć jako z natury zagrożone, z wykorzystaniem technologii IPSec VPN z serwera stacjonarnego w celu zabezpieczenia infrastruktury komunikacyjnej. W tym kontekście używanie telnetu do komunikacji konsoli jest zdecydowanie odradzane. Należy używać protokołu SSH i innych szyfrowanych protokołów.

KWESTIE ETYCZNE I PRAWNE.

Zarządzanie witryną wiąże się z szeregiem problemów etycznych i prawnych, głównie związanych z informacjami gromadzonymi przez witrynę podczas przetwarzania transakcji, a także ze śledzenia wydajności, identyfikacji problemów i audytów. Zasady muszą być publikowane, aby zapewnić, że informacje nie są wykorzystywane do nieautoryzowanych celów, a personel obsługujący takie systemy musi znać te zasady i przestrzegać ich. Wiele z tych kwestii etycznych ma również podłoże cywilne i karne.

Pasywa.

Środowisko odpowiedzialności otaczające serwery WWW jest zbyt nowe, aby spory mogły się toczyć. Jednak nie ma powodu, aby sądzić, że niezliczone przepisy regulujące ujawnianie danych osobowych nie będą w pełni egzekwowane w kontekście witryn internetowych.

Witryny internetowe coraz częściej obsługują poufne informacje. Witryny branży finansowej rutynowo obsługują transakcje bankowe i transakcje papierami wartościowymi. Usługi e-mail obsługują duże

ilości ruchu konsumenckiego, a coraz więcej firm ubezpieczeniowych, działów świadczeń pracowniczych i innych korzysta z witryn internetowych do przetwarzania niezwykle wrażliwych informacji objętych różnymi przepisami. Jednym z powodów, dla których zaleca się zwrócenie szczególnej uwagi na kontrolę serwerów internetowych i ich systemów wspierających, jest potrzeba stworzenia środowiska należytej staranności, w którym organizacja może wykazać, że podjęła rozsądne kroki w celu zapewnienia integralności, bezpieczeństwa i poufności informacji.

Monitorowanie klienta, prywatność i ujawnianie informacji.

Monitorowanie klientów jest z natury delikatnym tematem. Na przykład możliwość gromadzenia szczegółowych informacji o wzorcach wydatków jest przedmiotem nadużyć. Nieprawidłowe wykorzystanie tych informacji pomaga wskazać oferty sprzedaży, które klient uznałby za istotne, jednocześnie eliminując kontakty, które nie byłyby interesujące. Wykorzystane nieetycznie lub nawet nielegalnie, takie informacje mogłyby zostać wykorzystane do zebrania dokumentacji, która mogłaby być przedmiotem kłopotliwego ujawnienia, odmowy ubezpieczenia, a nawet rozwiązania stosunku pracy. Ogólny problem poprzedza Internet. W rzeczywistości ponad 20 lat temu główny segment wiadomości w sieci zrekonstruował czyjeś życie, wykorzystując tylko informacje zawarte w anulowanych czekach, uzupełnione publicznie dostępnymi informacjami. Wynikowa analiza była zaskakująco szczegółowa. Podobny eksperyment został zgłoszony w 1999 roku przy użyciu Internetu. Organizacje czasami naruszają najbardziej podstawowe praktyki bezpieczeństwa w zakresie ochrony informacji online, gdy wszystkie informacje wymagane do nieprawidłowego dostępu do konta znajdują się na jednej stronie wyciągu rozliczeniowego. Zdarzały się powtarzające się incydenty (np. CDUniverse, CreditCard.com), w których znajdowały się niezwykle wrażliwe informacje przechowywane w postaci niezaszyfrowanej w systemach dostępnych w Internecie. Incydenty te powtarzają się regularnie i prawie zawsze są wynikiem przechowywania dużej ilości poufnych informacji o klientach w systemach dostępnych w Internecie. Nie ma wątpliwości, że przechowywanie kart kredytowych klienta i podobnie wrażliwych danych w narażonych systemach jest niewłaściwe. Bezpieczeństwo i integralność systemów przechowujących informacje o zamówieniach klientów mają kluczowe znaczenie. Ujawnienie informacji o zamówieniach klienta stanowi poważne zagrożenie dla prywatności. Brak ochrony informacji bankowych klientów (np. Numerów kart kredytowych i dat ich ważności) może być niezwykle kosztowny, zarówno pod względem ekonomicznym, jak i z powodu zniszczenia relacji z klientami. Firmy przetwarzające karty płatnicze podlegają również PCI DSS organizacji Payment Card Industry Security Standards Council; które mogą rodzić dodatkowe zobowiązania i zobowiązania na przedsiębiorstwie. Witryna internetowa, monitorując aktywność klientów, będzie gromadzić zbiór wrażliwych materiałów. Można założyć, że informacje są przydatne tylko dla witryny i są z natury ważne, ale istnieje tutaj wiele zagrożeń, z których większość nie jest oczywista:

* Informacje, które wydają się pochodzić z jednego źródła, mogą rzeczywiście być kompilacją danych z wielu źródeł. Współdzielone komputery, zapory i serwery proxy mogą powodować to zjawisko.

* Mogą pojawić się przypadkowe korelacje między innymi niepowiązanymi przedmiotami. Na przykład nierzadką akceptowalną praktyką biznesową jest opłacenie przez jednego członka grupy biznesowej wszystkich kosztów grupy podróżujących kolegów. Brak prawidłowej interpretacji takiego zdarzenia może zostać niewłaściwie zinterpretowany jako dowód niedozwolonego lub niewłaściwego zachowania.

* Osoby często pełnią różne role społeczne (np. Rodzic, partner domowy, zawodowy, organizacja non-profit). Wnioski wyciągnięte z takich danych mogą nie odzwierciedlać osoby, ale łatwo mogą być niepowiązaną konsekwencją innego zaangażowania (np. Zapytanie o SAT lub GRE może wskazywać na

zamiar uczęszczania do college'u; może również oznaczać, że dziecko, siostrzenica , sąsiad lub inny znajomy mógł zasięgnąć porady).

Problem z przypadkowymi skojarzeniami polega na tym, jakie szkody mogą spowodować. W obszarze bezpieczeństwa narodowego wykorzystywanie przypadkowych stowarzyszeń do gromadzenia danych wywiadowczych jest użytecznym narzędziem, chociaż uznaje się, że ma ono poważne ograniczenia. W innych sytuacjach jest to niezwykle niebezpieczne narzędzie, które może zaszkodzić osobom i przedsiębiorstwom. Przykład:

Żonaty biznesmen z Kalifornii leci do Nowego Jorku. Po przyjeździe melduje się w dużym hotelu, po chwili wykonuje telefon, po czym do jego pokoju idzie młoda kobieta i zostaje ciepło przywitana. Najwyraźniej kompromitująca sytuacja. Biznesmen jest na tyle dorosły, że może być ojcem kobiety. W rzeczywistości jest jej ojcem. Ten jeden fakt zmienia pozornie niewłaściwe zachowanie w nieszkodliwe rodzinne spotkanie. Peter Lewis z The New York Times słusznie zauważa, że ten pojedynczy fakt, łatwo przeoczony, radykalnie zmienia znaczenie informacji.

Niebezpieczeństwo związane z korelacjami i monitorowaniem klientów polega na tym, że często nie ma kontroli nad ekspansywnym wykorzystaniem wygenerowanych wniosków. Informacje często mają pewien stopień ważności, ale zarówno łatwo jest przekroczyć granice ważności, jak i trudno jest, jeśli nie niemożliwe, później naprawić szkody, gdy już zostały one wyrządzone.

Spory sądowe.

Rosnąca wszechobecność sieci Web doprowadziła do zwiększenia liczby powiązanych sporów sądowych. W tym rozdziale nacisk położono na spory sądowe lub dochodzenia regulacyjne dotyczące transakcji handlowych lub konsumenckich, a także kwestie związane z postępowaniem karnym za działalność przestępczą związaną z witryną internetową.

Cywilne: dzienniki i rejestry witryn internetowych mogą być zaangażowane w spory sądowe na wiele sposobów. W coraz większej liczbie przypadków ani właściciel terenu, ani operator nie są stroną w akcji; zapisy dokumentują jedynie transakcje i zdarzenia związane ze sporem. Spór może dotyczyć ogólnej sprawy handlowej, sprawy personalnej, a nawet sprawy dotyczącej stosunków domowych obejmującej rozwód. Ważne jest, aby zasady postępowania z dokumentacją i jej przechowywania były opracowywane w porozumieniu z prawnikami. Kierownictwo i doradca firmy muszą również określić, jakie zasady mają obowiązywać w odniesieniu do wezwań sądowych i powiązanych wniosków. Radca prawny określi również, jakie materiały podlegają jakim procedurom i przepisom. Na przykład w przypadku dostawcy poczty elektronicznej (np. Hotmail.com) materiały mogą podlegać ustawie o prywatności w komunikacji elektronicznej z 1986 r. (18 U.S.C.A. § 2510 i nast.). Inne materiały mogą podlegać innym zobowiązaniom prawnym lub umownym.

Regulacje: wiele różnych przepisów jest egzekwowanych (i często ogłaszanych) przez różne agencje regulacyjne. W Stanach Zjednoczonych takie agencje istnieją na szczeblu federalnym, stanowym, regionalnym i lokalnym. (Poza Stanami Zjednoczonymi wiele krajów ma agencje tylko na szczeblu krajowym i prowincjonalnym). Wiele z tych agencji ma uprawnienia do żądania dokumentacji i prowadzenia różnego rodzaju dochodzeń. W przypadku wielu organizacji takie dochodzenia są znacznie bardziej prawdopodobne niż dochodzenia cywilne lub karne. Agencje regulacyjne mogą również nałożyć na firmy podlegające ich jurysdykcji wymogi dotyczące prowadzenia dokumentacji i przechowywania.

Sprawy karne: śledztwom poświęca się więcej uwagi niż dwóm poprzednim kategoriom dochodzeń, ale są one znacznie rzadsze. Śledztwo i ściganie w sprawach karnych jest kosztowne i muszą przejść

wyższy standard dowodu niż przepisy regulacyjne lub postępowanie cywilne. Stosunkowo niewiele incydentów komputerowych dochodzi do etapu postępowania karnego, choć ze względu na swoją wagę proces ten jest najbardziej widoczny.

Dzienniki, dowody i rejestrowanie tego, co się wydarzyło: Kluczem do skutecznego postępowania w przypadku każdego postępowania prawnego związanego z witryną internetową jest prowadzenie dokładnych, kompletnych zapisów w bezpieczny sposób.

W kontekście ochrony Strony internetowej, zapisy i dzienniki aktywności powinny być przenoszone na zewnętrzne nośniki i przechowywane do ewentualnego późniejszego wykorzystania, zgodnie z polityką witryny i jej zobowiązaniami prawnymi. Po wyładowaniu, dokumentacja ta powinna być przechowywana z zastosowaniem ścisłych procedur odpowiednich dla dowodów w sprawie karnej. Pojawienie się niedrogich nagrywarek CD-ROM i DVD znacznie upraszcza fizyczne kwestie bezpiecznego przechowywania takich nośników. Przestroga dotycząca nośników CD-ROM i DVD jest w porządku: Podczas tworzenia takich zapisów należy zachować ostrożność, aby używać czystych nośników wyprodukowanych zgodnie ze standardami archiwalnymi. Nośniki o jakości archiwalnej są droższe niż łatwiej dostępne nośniki o niższej jakości; jednakże nośniki archiwalne mają żywotność ocenianą na dziesięciolecia, tańsze nośniki mają żywotność kilku lat. Akta archiwalne, które nie są przeznaczone do celów dowodowych, również powinny być przechowywane w trybie offline. Powinno to przybrać formę fizycznego trybu offline lub przynajmniej w systemach, które nie są dostępne z publicznego Internetu.

Nośnik powinien być przechowywany w podpisanych, zaplombowanych pojemnikach w zinwentaryzowanym, bezpiecznym magazynie z kontrolowanym dostępem. Z tego powodu kopie archiwizowane do celów archiwalnych nie powinny być kopiami normalnie używanymi do odzyskiwania systemu. W przypadku dochodzenia lub innego problemu, zapisy te zostaną dokładnie sprawdzone pod kątem możliwych modyfikacji lub niewłaściwego wykorzystania.

Dostawcy usług aplikacji.

W ostatnich latach coraz częściej zleca się outsourcing całych usług aplikacji i hostingu. Organizacje zewnętrzne świadczące takie usługi są znane jako dostawcy usług aplikacji, częściej określani jako ASP. Niedawno zostało to ponownie ochrzczone jako oprogramowanie jako usługa (SaaS). Obydwa wiążą się z podobnymi obawami dotyczącymi bezpieczeństwa i integralności. W obu przypadkach istotne aplikacje i dane są przechowywane poza organizacją, przy czym organizacja zachowuje odpowiedzialność za integralność i poufność tych zapisów. Bardziej prozaiczna oferta, hosting wirtualny, doświadczyła eksplozji popularności, często nazywanej infrastrukturą jako usługą (IaaS). Wiele z tych samych problemów z SaaS dotyczy środowisk zakupionych jako IaaS. Linia podziału odpowiedzialności jest inna, ale występują te same klasy problemów. Pod względem koncepcyjnym ASP nie są nowe. Wiele organizacji w przeszłości zlecało przetwarzanie płac i inne aplikacje na zewnątrz. Teoretycznie za całą aplikację odpowiada ASP. Często płacenie ceny pakietu za aplikację wydaje się atrakcyjne: brak opłat za konserwację, brak kosztów amortyzacji, niższe koszty personelu, najnowsza technologia i umiarkowane ceny aktualizacji. Jednak tak jak kapitan statku zachowuje odpowiedzialność za bezpieczeństwo swojego statku pomimo obecności pilota portowego, przedsiębiorca nie może zapominać, że jeśli coś pójdzie nie tak, to przedsiębiorstwo, a nie ASP, prawdopodobnie poniesie pełne konsekwencje. Krótko mówiąc, od ASP należy wymagać, aby odpowiadały na te same pytania i przestrzegały tych samych standardów, co wewnętrzna organizacja IT, jeśli chodzi o kwestie prywatności, bezpieczeństwa i integralności. Kwestie bezpieczeństwa i integralności związane z używaniem ASP są takie same, jak te dotyczące korzystania z wewnętrznej usługi korporacyjnej. Kwestie prywatności, uczciwości i niezawodności pozostają aktualne, ale tak jak

w przypadku każdej formy outsourcingu, pojawiają się dodatkowe pytania. Na przykład, czy przechowywane informacje są pomieszane z informacjami innych firm, być może konkurentów? Czy przechowywane informacje są zaszyfrowane? Jakie istnieją rezerwy? Czy istnieje przechowywanie kopii zapasowych poza siedzibą firmy? Jaką łączność ma ASP? Gdzie są serwery ASP i czy są rozproszone? Jakie są praktyki kadrowe ASP? Czy sama ASP posiada i obsługuje swoje obiekty, czy z kolei zawiera umowy z innymi dostawcami? Najważniejsze jest to, że chociaż outsourcing obiecuje szybkie wdrożenie, niższe koszty personelu i korzyści skali, organizacja klienta poniesie znaczne szkody, jeśli wystąpi problem z ASP, z dostępnością, wynikami lub poufność. Ostatecznie organizacja zachowuje odpowiedzialność za swoje działania i swoje dane. Chociaż pocieszające jest uznanie, że system prawny zaakceptuje stwierdzenie „zrobił to mój dostawca" jako wymówkę dla utraconych, skompromitowanych lub niewiarygodnych danych, pozostaje on nieprzetestowaną teorią i prawdopodobnie nie zwycięży. Ostatnie doświadczenia z głównymi producentami, podwykonawcami i skażonymi produktami wydają się wskazywać, że ryzyko outsourcingu pozostaje poważną potencjalną odpowiedzialnością. Wnioski o proces sądowy, czy to nakazów karnych, czy wezwań cywilnych, skierowane przeciwko ASP w sprawie danych osób trzecich stanowią kolejne zagrożenie. Jeśli dane należące do osób trzecich są pomieszane w systemie ASP, należy zachować ostrożność, aby zapobiec nieuprawnionemu i niewłaściwemu ujawnieniu niepowiązanych danych należących do stron trzecich innych niż ta, której dotyczy żądanie. Żadna z przytoczonych pozycji nie jest wystarczająca, aby uzasadnić negatywny wynik dotyczący ASP jako grupy. Powinny jednak służyć jako przypomnienie, że każdy z problemów związanych z utrzymaniem bezpieczeństwa, dostępności i skuteczności obecności w sieci WWW dotyczy nie mniej ASP niż wewnętrznej organizacji IT.

PODSUMOWANIE.

Dostępność jest podstawą wszystkich strategii związanych z Internetem. W tym rozdziale zauważono, że nadmiarowy hosting i routing były niezbędne, aby zapewnić dostępność 24/7/365. Zwrócono również uwagę, że chociaż niektórzy usługodawcy oferują różne gwarancje, gwarancje te prawie nigdy nie zapewniają odpowiedniego odszkodowania za szkody następcze wyrządzone przedsiębiorstwu. Ostatecznie jedyną ochroną przedsiębiorstwa jest podjęcie odpowiednich środków w celu zapewnienia własnego bezpieczeństwa i integralności. Wytyczne operacyjne i uprawnienia są również krytyczne dla zapewnienia dostępności zasobów internetowych w trybie 24/7/365. Systemy muszą być zaprojektowane i wdrożone, aby zwiększyć dostępność na poziomie ogólnym. Personel operacyjny musi mieć swobodę i uprawnienia do podejmowania działań, które uważają za konieczne, bez obawy o odwet, jeśli procedury nie przyniosą pożądanego rezultatu. Ważna jest również prywatność i integralność informacji wymienianych z Witryną. Wdrożenie i działanie witryny i jej komponentów musi być zgodne z odpowiednimi przepisami prawa, regulacjami i obowiązkami właściciela witryny, a także musi być zgodne z oczekiwaniami społeczności użytkowników. Ochrona zasobów Internetu i sieci Web to wieloaspektowe zadanie obejmujące wiele dziedzin. Jest to obszar wymagający uwagi na wszystkich poziomach, począwszy od najwyższych poziomów strategii biznesowej, a kończąc na coraz bardziej szczegółowych zagadnieniach wdrożeniowych i technologicznych. Jest to również obszar, w którym najmniejszy szczegół może mieć katastrofalne skutki. Niedawne wydarzenia pokazały, że wnioski z historii komunikacji mają zastosowanie. Nawet mały błąd w architekturze sieci, zarządzaniu kluczami lub implementacji może spowodować lawinę, aż pojawi się problem, który da się odczuć w korporacyjnej sali konferencyjnej.