Planowanie i Zasady

Bezpieczeństwo to proces, a nie produkt. - BRUCE SCHNEIER

Obrona

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

TEST XVIII

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

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

ZARZĄDZANIE TO TRUDNA CZĘŚĆ

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

KOMPLEKSOWE BEZPIECZEŃSTWO

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

AWARIE NAJSŁABSZEGO OGNIWA

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

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

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

POTRZEBA OCHRONY WIELU ZASOBÓW

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

TEST XIX

a. Z jakich powodów zarządzanie bezpieczeństwem jest trudne?

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

c. Jakie są awarie najsłabszego łącza?

POTRZEBA OCHRONY WIELU ZASOBÓW

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

TEST XX

a. Z jakich powodów zarządzanie bezpieczeństwem jest trudne?

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

c. Jakie są awarie najsłabszego łącza?

Potrzeba zdyscyplinowanego procesu zarządzania bezpieczeństwem

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

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

Procesy to zaplanowane serie działań.

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

TEST XXI

a. Dlaczego procesy są niezbędne w zarządzaniu bezpieczeństwem?

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

Cykl Plan - Chroń – Reaguj

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

PLANOWANIE

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

OCHRONA

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

Ochrona to oparte na planie tworzenie i działanie środków zaradczych

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

ODPOWIEDŹ

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

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

Odpowiedź to powrót do zdrowia zgodnie z planem.

TEST XXII

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

b. Czy między etapami występuje sekwencyjny przepływ?

c. Który etap zajmuje najwięcej czasu?

d. Jak definiujemy ochronę?

e. Jak definiujemy odpowiedź?

Wizja w planowaniu

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

POGLĄD NA BEZPIECZEŃSTWO JAKO AKTYWATOR

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

TWORZENIE POZYTYWNYCH WIZJI UŻYTKOWNIKÓW

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

TEST XXIII

a. W jaki sposób dobre bezpieczeństwo może być bodźcem?

b. Jaki jest klucz do bycia bodźcem?

c. Dlaczego negatywny pogląd na użytkowników jest zły?

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

Strategiczne planowanie bezpieczeństwa IT

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

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

TEST XXIV

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

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

c. Co firma powinna zrobić dla każdego zasobu?

d. W jakim celu firma powinna opracować plany naprawcze?

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

PRZEPISY I REGULACJE ZGODNOŚCI

Siły napędowe

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

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

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

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

TEST XXV

a. Jakie są siły napędowe?

b. Co robią przepisy dotyczące zgodności?

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

Sarbanes-Oxley

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

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

TEST XXVI

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

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

Przepisy dotyczące ochrony prywatności

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

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

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

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

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

TEST XXVII

a. Do czego zmusiły firmy przepisy dotyczące ochrony prywatności?

b. Co znaleźli, kiedy to zrobili?

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

d. Jakie instytucje podlegają ustawie HIPAA?

Przepisy dotyczące powiadamiania o naruszeniu danych

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

TEST XXVIII

a. Czego wymagają przepisy dotyczące powiadamiania o naruszeniu danych?

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

Federalna Komisja Handlu

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

TEST XXIX

a. Kiedy Federalna Komisja Handlu może działać przeciwko firmom?

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

Akredytacja branżowa

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

TEST XXX

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

PCI-DSS

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

TEST XXXI

Na jakie firmy wpływa PCI-DSS?

FISMA

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

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

TEST XXXII

a. Kto podlega FISMA?

b. Rozróżnij certyfikację i akredytację w FISMA.

c. Dlaczego krytykowano FISMA?

ORGANIZACJA

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

Chief Security Officer

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

TEST XXXIII

a. Jak zwykle nazywa się kierownik działu bezpieczeństwa?

b. Jaki jest inny tytuł dla tej osoby?

Czy powinieneś umieścić bezpieczeństwo w IT?

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

BEZPIECZEŃSTWO WEWNĄTRZ IT

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

BEZPIECZEŃSTWO POZA IT

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

ROZWIĄZANIE HYBRYDOWE

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

TEST XXXIV

a. Jakie są zalety umieszczenia zabezpieczeń w IT?

b. Jakie są wady umieszczania zabezpieczeń w IT?

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

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

Wsparcie najwyższego kierownictwa

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

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

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

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

TEST XXXV

a. Dlaczego wsparcie najwyższego kierownictwa jest ważne?

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

Relacje z innymi działami

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

SZCZEGÓLNE RELACJE

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

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

Działy zasobów ludzkich

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

Dział prawny

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

Działy audytu

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

Zarządzanie obiektami

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

Jednolite bezpieczeństwo

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

WSZYSTKIE DZIAŁY KORPORACYJNE

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

PARTNERZY BIZNESOWI

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

TEST XXXVI

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

b. Rozróżnij trzy główne typy jednostek audytu korporacyjnego.

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

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

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

f. Kim są partnerzy biznesowi?

g. Dlaczego są niebezpieczne?

h. Co to jest należyta staranność?

Outsourcing bezpieczeństwa IT

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

OUTSOURCING E-MAIL

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

Strategia i technologia bezpieczeństwa

ZARZĄDZANIE E-MAILEM DLA FIRM

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

Pobieranie odcisków palców

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

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

Czarne listy i kontrola stawek

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

DOSTAWCA ZARZĄDZANYCH USŁUG BEZPIECZEŃSTWA

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

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

TEST XXXVII

a. Co to jest MSSP?

b. Jakie są dwie główne zalety korzystania z MSSP?

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

d. Jakie funkcje bezpieczeństwa są zazwyczaj zlecane na zewnątrz?

e Jakie funkcje bezpieczeństwa zazwyczaj nie są zlecane na zewnątrz?

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

ANALIZA RYZYKA

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

Rozsądne ryzyko

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

TEST XXXVIII

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

b. Dlaczego uzasadnione ryzyko jest celem bezpieczeństwa IT?

c. Jakie są negatywne konsekwencje bezpieczeństwa IT?

Obliczenia klasycznej analizy ryzyka

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

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

WARTOŚĆ AKTYWÓW

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

CZYNNIK EKSPOZYCJI

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

OCZEKIWANIE POJEDYNCZEJ STRATY

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

ROCZNE PRAWDOPODOBIEŃSTWO (LUB WARTOŚĆ) WYSTĘPOWANIA

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

ROCZNE OCZEKIWANIE STRAT

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

ŚRODKI ZARADCZE

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

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

ROCZNY KOSZT ŚRODKÓW ŚRODKOWYCH I WARTOŚĆ NETTO

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

TEST XXXIX

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

b. Jak obliczyć ALE?

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

Problemy z obliczeniami klasycznej analizy ryzyka

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

NIERÓWNE WIELOLETNIE PRZEPŁYWY PIENIĘŻNE

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

CAŁKOWITY KOSZT SZKODY

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

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

WIELE DO WIELU RELACJI MIĘDZY ŚRODKAMI I ZASOBAMI

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

NIEMOŻLIWOŚĆ OBLICZENIA ROCZNIONYCH WSPÓŁCZYNNIKÓW WYSTĘPOWANIA

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

PROBLEM Z „TWARDYM MYŚLENIEM"

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

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

PERSPEKTYWICZNY

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

TEST XL

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

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

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

d. Jaki jest najgorszy problem z klasycznym podejściem?

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

Reagowanie na ryzyko

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

REDUKCJA RYZYKA

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

AKCEPTACJA RYZYKA

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

PRZENIESIENIE RYZYKA (UBEZPIECZENIE)

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

UNIKANIE RYZYKA

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

Unikanie ryzyka oznacza niepodejmowanie ryzykownych działań.

TEST XLI

a. Jakie są cztery sposoby reagowania na ryzyko?

b. Co oznacza nic nie robienie?

c. Co obejmuje ubezpieczenie?

d. Dlaczego ubezpieczenie nie jest sposobem na uniknięcie bezpieczeństwa?

e. Co to jest unikanie ryzyka?

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

ARCHITEKTURA ZABEZPIECZENIA TECHNICZNEGO

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

Architektury bezpieczeństwa technicznego

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

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

DECYZJE ARCHITEKTONICZNE

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

POSTĘPOWANIE ZE STARSZĄ TECHNOLOGIĄ BEZPIECZEŃSTWA

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

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

TEST XLII

a. Jaka jest techniczna architektura zabezpieczeń firmy?

b. Dlaczego potrzebna jest techniczna architektura zabezpieczeń?

c. Kiedy najlepiej je założyć?

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

Zasady

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

OBRONA W GŁĘBI

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

OBRONA W GŁĘBI A NAJSŁABSZE LINKI

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

POJEDYNCZE PUNKTY WRAŻLIWOŚCI

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

MINIMALIZACJA OBCIĄŻEŃ BEZPIECZEŃSTWA

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

REALISTYCZNE CELE

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

TEST XLIII

a. Dlaczego obrona głęboka jest ważna?

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

c. Dlaczego konsole centralnego zarządzania bezpieczeństwem są niebezpieczne?

d. Dlaczego są pożądane?

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

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

Elementy architektury bezpieczeństwa technicznego

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

ZARZĄDZANIE GRANICAMI

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

ZARZĄDZANIE BEZPIECZEŃSTWEM MIEJSCA WEWNĘTRZNEGO

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

ZARZĄDZANIE ZDALNYMI POŁĄCZENIAMI

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

SYSTEMY INTERORGANIZACYJNE

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

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

CENTRALNE ZARZĄDZANIE BEZPIECZEŃSTWEM

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

TEST XLIV

a. Dlaczego zarządzanie granicami jest ważne?

b. Dlaczego nie jest to kompletne rozwiązanie zabezpieczające?

c. Dlaczego połączenia zdalne z domu są szczególnie niebezpieczne?

d. Dlaczego systemy międzyorganizacyjne są niebezpieczne?

e. Dlaczego centralne zarządzanie bezpieczeństwem jest atrakcyjne?

WDRAŻANIE Z MYŚLĄ O ZASADACH

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

Zasady

CZYM SĄ ZASADY?

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

CO, NIE JAK

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

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

PRZEJRZYSTOŚĆ

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

TEST XLV

a. Jakie są zasady?

b. Rozróżnij zasady i wdrażanie.

c. Dlaczego zasady nie powinny szczegółowo określać implementacji?

Kategorie polityk bezpieczeństwa

POLITYKA BEZPIECZEŃSTWA FIRMY

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

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

GŁÓWNE POLITYKI

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

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

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

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

PRZYJĘTE ZASADY UŻYTKOWANIA

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

POLITYKI DOTYCZĄCE OKREŚLONYCH ŚRODKÓW PRZECIWŚRODKOWYCH LUB ZASOBÓW

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

TEST XLVI

a. Rozróżnij korporacyjną politykę bezpieczeństwa i główne zasady bezpieczeństwa.

b. Rozróżnij główne zasady bezpieczeństwa i zasady dopuszczalnego użytkowania.

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

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

Zespoły opracowujące zasady

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

TEST XLVII

Dlaczego ważne jest, aby zespoły korporacyjne tworzyły zasady?

Wskazówki dotyczące wdrażania

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

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

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

BRAK WYTYCZNYCH

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

NORMY I WYTYCZNE

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

TEST XLVIII

a. Rozróżnij normy i wytyczne.

b. Co jest obowiązkowe w przypadku wytycznych?

c. Kiedy wytyczne są odpowiednie?

Rodzaje wytycznych dotyczących wdrażania

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

PROCEDURY

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

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

Procedury określają szczegółowe działania, które muszą podjąć poszczególni pracownicy.

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

PROCESY

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

LINIE BAZOWE

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

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

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

NAJLEPSZE PRAKTYKI I ZALECANE PRAKTYKI

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

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

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

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

ODPOWIEDZIALNOŚĆ

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

ETYKA

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

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

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

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

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

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

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

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

TEST XLIX

a. Rozróżnij procedury i procesy

b. Kiedy będą używane?

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

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

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

f. Czym różnią się wytyczne od procedur i procesów?

g. Rozróżnij najlepsze praktyki i zalecane praktyki.

h. Rozróżnij właścicieli zasobów i powierników pod względem odpowiedzialności.

i. Co właściciel może przekazać powiernikowi?

j. Czego właściciel nie może przekazać powiernikowi?

a. Dlaczego etyka jest nieprzewidywalna?

b. Dlaczego firmy tworzą kodeksy etyczne?

c. Dlaczego dobra etyka jest ważna w firmie?

d. Kogo obowiązują kodeksy etyczne?

e. Czy wyżsi funkcjonariusze często otrzymują dodatkowy kodeks etyczny?

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

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

h. Jakie zostały podane przykłady konfliktów interesów?

i. Dlaczego łapówki i prowizje są złe?

j. Rozróżnij łapówki i prowizje.

k. Jakich informacji pracownik nie powinien ujawniać?

Obsługa wyjątków

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

• Tylko niektóre osoby powinny mieć prawo prosić o wyjątki.

• Jeszcze mniej osób powinno mieć możliwość autoryzacji wyjątków.

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

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

• Szczególną uwagę należy zwrócić na wyjątki w okresowych audytach.

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

TEST L

a. Dlaczego wyjątki nie powinny być absolutnie zabronione?

b. Dlaczego potrzebne są wskazówki dotyczące implementacji obsługi wyjątków?

c. Jakie są pierwsze trzy zasady dotyczące wyjątków?

d. Dlaczego dokumentacja i okresowe audyty byłyby ważne?

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

Przeoczenie

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

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

POLITYKI I NADZÓR

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

OPUBLIKOWANIE

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

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

MONITOROWANIE ELEKTRONICZNE

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

MIERNIKI BEZPIECZEŃSTWA

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

Metryki bezpieczeństwa są mierzalnymi wskaźnikami powodzenia lub niepowodzenia bezpieczeństwa.

AUDYT

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

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

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

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

ANONIMOWA ZABEZPIECZONA INFOLINIA

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

ŚWIADOMOŚĆ BEHAWIORALNA

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

OSZUSTWO

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

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

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

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

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

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

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

SANKCJE

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

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

TEST LI

a. Co to jest nadzór?

b. Jak nadzór jest powiązany z polityką?

c. Co to jest promulgacja?

d. Czym są kłujący pracownicy?

e. Jakie są jego koszty i korzyści?

f. Czy monitoring elektroniczny jest szeroko stosowany?

g. Co powinieneś powiedzieć pracownikom przed rozpoczęciem monitorowania?

h. Czym są metryki bezpieczeństwa?

RAMY ZARZĄDZANIA

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

Ramy zarządzania określają sposób planowania i wdrażania zabezpieczeń.

TEST LII

a. Czym są ramy zarządzania?

b. Porównaj koncentrację COSO z koncentracją CobiT.

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

d. Dlaczego pomiary okresowe są korzystne?

a. Jaki jest cel audytu?

b. Rozróżnij pliki dziennika i dokumentację.

c. Dlaczego unikanie zgodności jest poważnym sygnałem ostrzegawczym?

d. Rozróżnij audyt wewnętrzny i zewnętrzny.

e. Dlaczego regularnie zaplanowane audyty są dobre?

f. Dlaczego przeprowadzane są nieplanowane audyty?

a. Dlaczego firmy powinny instalować anonimowe chronione infolinie?

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

c. Dlaczego ogólne złe zachowanie pracowników powinno być problemem?

d. Jakie są trzy elementy trójkąta oszustwa i nadużycia?

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

f. Dlaczego racjonalizacje są ważne?

g. Podaj dwa przykłady racjonalizacji nie podane w tekście.

a. Co to jest test podatności?

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

c. Co powinno znaleźć się w umowie?

d. Czego należy szukać w zewnętrznej firmie testującej podatności?

e. Dlaczego potrzebne są dalsze działania dotyczące zalecanych poprawek?

Dlaczego ważne jest nakładanie sankcji na osoby naruszające przepisy?

COSO

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

RAMY COSO

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

CELE

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

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

• Operacje - efektywne i wydajne wykorzystanie jej zasobów

• Raportowanie – wiarygodność raportowania

• Zgodność - zgodność z obowiązującymi przepisami i regulacjami

ROZSĄDNE ZABEZPIECZENIE

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

KOMPONENTY RAMOWE COSO

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

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

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

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

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

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

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

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

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

TEST LIII

a. Jakie są cztery cele COSO?

b. Wymień osiem komponentów COSO.

c. Czym jest czynność kontrolna i dlaczego jest ważna?

CobiT

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

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

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

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

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

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

DOMINACJA W STANACH ZJEDNOCZONYCH

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

TEST LIV

a. Rozróżnij obszary zainteresowania COSO i CobiT.

b. Wymień cztery domeny CobiT.

c. Ile celów kontroli wysokiego poziomu ma CobiT?

d. Która domena ma najwięcej celów kontrolnych?

e. Ile szczegółowych celów kontrolnych ma CobiT?

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

Rodzina ISO/IEC 27000

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

ISO/IEC 27002

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

• Polityka bezpieczeństwa

• Organizacja bezpieczeństwa informacji

• Zarządzanie aktywami

• Bezpieczeństwo zasobów ludzkich

• Bezpieczeństwo fizyczne i środowiskowe

• Zarządzanie komunikacją i operacjami

• Kontrola dostępu

• Pozyskiwanie, rozwój i utrzymanie systemów informatycznych

• Zarządzanie incydentami związanymi z bezpieczeństwem informacji

• Ciągłości działania

• Zgodność

ISO/IEC 27001

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

INNE 27000 STANDARDÓW

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

TEST LV

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

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

c. Wymień 11 szerokich obszarów w 27002.

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

WNIOSEK

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

Przemyślane pytania

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

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

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