Budowanie bezpiecznej organizacji

„Chociaż cyberprzestrzeń stwarza nowe możliwości, szacunek dla osobistego prawa nigdy nie powinny być naruszane. „ - Emilienne Sybile Bayiha

Wprowadzenie

Dzisiaj, bardziej niż kiedykolwiek wcześniej, ze strachu można zaobserwować dwa krytyczne fakty. Jednym z nich jest to, że organizacje są całkowicie oparte na danych; po drugie, dane są bardzo niepewne, niezależnie od tego, czy są w tranzycie lub w magazynie. Biorąc pod uwagę te dwa fakty, musimy rozbić koncepcję bezpiecznej organizacji na podskładniki, które mogą wspólnie zapewnić niezbędną infrastrukturę zapewniającą poufność, integralność i dostępność, która jest niezbędna do pomyślnych operacji wewnątrz- i międzyorganizacyjnych. Bezpieczna organizacja zaczyna się od polityki bezpieczeństwa informacji udokumentowanej w podręczniku bezpieczeństwa organizacji, z którą każdy członek musi się zapoznać. Nie ma jednego komponentu, który mógłby zagwarantować bezpieczeństwo systemu informatycznego w organizacji, ale listę komponentów, które łącznie mogą zapewnić akceptowalny poziom bezpieczeństwa. Takie elementy zostały rozpoznane w wielu dokumentach i literaturze. Międzynarodowa norma ISO17799 wyraźnie identyfikuje i adresuje te komponenty

Business Continuity Planning

Podstawowym celem każdego przedsiębiorstwa jest zapewnienie nieprzerwanego dostępu do jego usług lub produktów wszystkim uprawnionym do ich otrzymania. Jednak „żadna organizacja nie jest odporna na przerwy w ciągłości działania". Plan ciągłości działania (BCP) to drukowany i w inny sposób dystrybuowany dokument, który w wyraźny sposób opisuje kroki, jakie należy podjąć, aby przywrócić firmę do pełnej sprawności po przerwie lub spowolnieniu. BCP można podzielić na dwa oddzielne plany, a mianowicie plan naprawy gospodarczej (BRP) i plan naprawy awaryjnej (DRP), przy czym ten pierwszy obejmuje niewielkie zakłócenia, a drugi dotyczy poważnych sytuacji kryzysowych. Niektóre źródła zdarzeń, które mogły spowodować niepowodzenie planu ochrony mogą być następujące:

• Akty naturalne - trzęsienie ziemi, powódź itp., Które bezpośrednio lub pośrednio spowodowały zakłócenie normalnej działalności

• Zaniedbanie ze strony członka organizacji

• Awaria spowodowana procesem bezpieczeństwa, który nie uwzględniał określonego zdarzenia lub kombinacji zdarzeń

• Niepokoje społeczne lub sytuacje kryzysowe w kraju

• Nie do obrony fizyczny lub cyberatak na system informacyjny

Naturalny akt może uderzyć bezpośrednio w przedsiębiorstwo lub może uderzyć w inną organizację, która zapewnia przedsiębiorstwu zasoby krytyczne. Na przykład, taki akt może spowodować utratę jednego lub więcej mediów - zasilania, telefonu, wody, Internetu, gazu, transportu, pracy itp.

Bardzo często, z powodu braku przeszkolenia lub staranności, osoby, którym powierzono opiekę nad poufnymi danymi, tracą lub uszkadzają dane w trakcie pełnienia swoich obowiązków. Dzieje się to wielokrotnie, ale można je złagodzić poprzez automatyczne tworzenie kopii zapasowych danych oraz poprzez polityki, w których krytyczne usuwanie danych wymaga zgody co najmniej dwóch osób.

Bezpieczeństwo systemu informatycznego i ogólnie bezpieczeństwo zawsze pozostawia coś niezrozumiałego. W przypadku łat po wprowadzeniu szkodliwego oprogramowania o kilka miesięcy planowanie bezpieczeństwa musi być aktualizowane na bieżąco. Istnieją pewne ataki, przed którymi przedsiębiorstwo może zdecydować się nie być chronionym, ponieważ koszty są wygórowane. Do tej kategorii należą ataki typu „odmowa usługi". BCP musi zająć pozycję awaryjną dla każdej znanej potencjalnej przyczyny możliwego zakłócenia operacji. Opracowanie BCP jest wynikiem metodologii obejmującej następujące etapy:

• Analiza wpływu na biznes

• Strategia naprawy biznesu

• Opracowanie BCP

• Testowanie BCP

• Szkolenie z wdrażania BCP

• Wskaźniki wydajności BCP

Analiza wpływu na biznes (BIA)

W tej początkowej fazie wszystkie procesy przedsiębiorstwa są weryfikowane i klasyfikowane na podstawie poziomu ważności w misji przedsiębiorstwa. Analiza ujawnia istniejące luki identyfikujące związki przyczynowo-skutkowe. Potencjalne zagrożenia wymieniono w raporcie BIA, który stanowi podstawę do opracowania BCP. BIA zakończy się trójwymiarową mapą (X, Y, Z) ilustrującą dotknięte usługi (X), podatności (Y) i poziom potencjalnych strat jako trzeci wymiar (Z). Taki wykres wyraźnie wskazuje priorytety, jakie przedsiębiorstwo powinno mieć na podstawie wyszczególnionych potencjalnych strat. W oparciu o BIA i przed przystąpieniem do opracowywania kroków, które należy podjąć po wystąpieniu sytuacji awaryjnej, należy rozważyć ulepszenia bezpieczeństwa, które zmniejszą zidentyfikowane luki i poprawią stan bezpieczeństwa systemu informatycznego. Po zakończeniu tego badania zespół ds. bezpieczeństwa informacji może przejść do następnego etapu BCP, jakim jest Strategia odzyskiwania biznesu.

Strategia naprawy biznesu (BRS)

Strategia rozpoczyna się od identyfikacji punktu centralnego, czyli zespołu, który wdroży kroki niezbędne do przywrócenia zakłóceń w działaniu. W organizacji wszyscy będą musieli wiedzieć że ta drużyna ze wskazanym liderem zespołu złapie byka za rogi, gdy zakwestionowana zostanie ciągłość biznesu. Z komunikacją , będącą najważniejszym zasobem, szczególnie w wyjątkowych okolicznościach, zespół będzie musiał ustanowić drzewo komunikacyjne, dzięki któremu informacje będą mogły podróżować w górę, w dół i na boki w niezawodny i wydajny sposób. Zespół we współpracy z kierownikami odpowiedzialnych jednostek określi i uszereguje pod względem ważności zasoby organizacyjne, które muszą być chronione i dostępne przez cały czas. Dla każdego takiego zasobu zostaną określone wymagane zasoby i zapewniona będzie ich dostępność. Dostępność zasobu, czy to danych, czy procesów, można zabezpieczyć poprzez ochronę lub replikację. Zespół, po ustaleniu zależności zasobów od zasobów, może teraz przystąpić do faktycznego opracowania Podręcznika planowania odzyskiwania biznesu.

Opracowanie planu ciągłości działania

Przy znanych krytycznie potrzebnych zasobach opracowywany jest plan ich przywrócenia, jeśli z jakiegoś powodu staną się one niedostępne. Jeśli są to dane, replikowane bazy danych powinny

znajdować się w innym fizycznym lub wirtualnym serwerze lokalizacji, obiekcie lub w chmurze, z której dane mogą być w równym stopniu dostępne. Oczywiście replikacja oznacza, że dane będą tworzone w regularnych odstępach czasu. CIO wraz z właścicielem danych muszą określić relację replikacji do nominalnego miejsca przechowywania danych. Replikacja może odbywać się w określonych odstępach czasu lub w czasie rzeczywistym. Ponadto może istnieć więcej niż jedna witryna replikacji. Podobnie dostępność procesów będzie musiała być zabezpieczona przez wiele serwerów, które mogą się automatycznie włączać, zastępując niezdolne do pracy. Oznacza to, że w przypadku rozszerzonego ataku typu „odmowa usługi" usługa będzie świadczona z różnych adresów IP, a system nazw domen (DNS) będzie natychmiast aktualizowany. DNS konwertuje adresy nazw domen na adresy IP.

Testowanie planu ciągłości działania

Po opracowaniu, przejrzeniu i zatwierdzeniu planu należy go przetestować poprzez serię emulowanych sytuacji awaryjnych, z wynikami testu i poprawą planu. Zanim przejdziemy do wyrafinowanych możliwości awarii ciągłości biznesowej, należy przeprowadzić testy podstawowych luk w zabezpieczeniach, zaczynając od narzędzi. Co się stanie, jeśli dostawa wody do budynku operacyjnego zostanie przerwana, nastąpi utrata zasilania, usługa telefoniczna, dostęp do Internetu nie będzie możliwy lub transport publiczny zostanie przerwany z jakiegokolwiek powodu? Klienci na całym świecie, przechodząc do Internetu w celu uzyskania dostępu do usług organizacji, przyjmują za pewnik, że tam będą. Nasze życie stało się tak współzależne, że jeśli jedna usługa zawiedzie, powstanie efekt domina niesprzyjających sytuacji. Kiedy jedziemy i widzimy zielone światło, wciskamy benzynę i oczekujemy przed nami wyraźnej drogi. Co się stanie, jeśli przejeżdżający kierowca nie zatrzyma się na czerwonym? Z pewnością takie życie zakłóci życie wielu ludzi. Dlatego w planie ciągłości działania muszą znajdować się szczegółowe instrukcje krok po kroku, zawierające długą listę możliwych niepożądanych zdarzeń, które należy przezwyciężyć, aby zachować ciągłość działania. Co najważniejsze, każde rozwiązanie do odzyskiwania musi zostać przetestowane, a jego ważność potwierdzona. Takie testowanie musi odbywać się regularnie, przy czym słowo regularne musi być określone ilościowo w jednostkach czasu przez Głównego Urzędnika ds. Bezpieczeństwa Informacji (CISO).

Szkolenie z wdrażania planu ciągłości działania.

Faktem jest, że nie można nauczyć się pływania , czytając same książki. Jeśli badacz książek pływackich wskoczy do głębokich wód po ukończeniu studiów, będzie to pierwszy i ostatni skok. W związku z tym właściwego zachowania organizacyjnego w stanie wyjątkowym można się spodziewać tylko pod warunkiem powtarzanego szkolenia, które stale uwzględnia wykrywanie nowych zagrożeń i słabych punktów.

Wskaźniki wydajności planu ciągłości działania

BRP, który obejmuje zarówno przerwy, jak i katastrofy, należy stale oceniać za pomocą wybranych wskaźników, które w sposób zadowalający oznaczają, że w przypadku prawdziwej katastrofy plan będzie skuteczny. Czwórka najbardziej reprezentatywnych wskaźników to

- Wskaźnik pierwszy: raportowanie do kierownictwa
- Wskaźnik drugi: zaangażowanie inżynierii
- Wskaźnik trzeci: testowanie planu
- Wskaźnik czwarty: udoskonalenia planu

Poprzez okresowe składanie sprawozdań zarządowi zostanie podkreślony stan gotowości i poszukiwane będą odpowiednie zasoby. Kierownictwo wyższego szczebla musi być w pełni świadome istnienia ryzyka, które może spowodować przerwy w działalności lub katastrofę biznesową. W tych raportach komitet BCP będzie wymieniał ryzyko w miarę ich ewolucji w czasie, potencjalne straty dla organizacji, koszty odzyskiwania oraz wpływ ,po odzyskaniu, na organizację. Ponieważ każda firma jest zasadniczo oparta na technologii, zaangażowanie kluczowego personelu technicznego jest niezbędne w komitecie BCP, przedstawiając ich stale dostosowywane strategie odzyskiwania, strategie, które są funkcjami ryzyka i technologii obie ewoluują. Testowanie planu może zapewnić niezbędną pewność, że żadna nieciągłość biznesowa nie będzie miała katastrofalnego wpływu. Dzięki suchym uruchomieniom zostanie ustalona odporność planu - zdolność do odzyskiwania - oraz skuteczność usług tworzenia kopii zapasowych. Kluczem do każdego planu jest udział dostawców - z obowiązującymi umowami serwisowymi - oraz dużych klientów. Biorąc pod uwagę szybki rozwój technologii, szczególnie w systemach informatycznych, oczekuje się ulepszeń planu, a osoby odpowiedzialne muszą być zgodne z postępem technologicznym w zakresie z jednej strony i ryzyko z drugiej strony.

Kontrola dostępu do systemu

W kontroli dostępu do systemów podstawowym celem jest zapobieganie nieautoryzowanemu dostępowi, dzięki czemu kontrolowane zasoby są dostępne tylko dla uprawnionych użytkowników. Dodatkowe cele obejmują wykrywanie prób przez nieautoryzowanych użytkowników i ochrona dostępu przed błędnymi wpisami w dobrej wierze. Proces kontroli dostępu do systemu składa się z trzech elementów: poświadczenia, czytnika i procesora. Na każdym etapie należy podjąć środki bezpieczeństwa, aby utrzymać bezpieczny system.

Poświadczenie to zwykle nazwa użytkownika i hasło, przy czym hasła mogą być dostarczane dokładnie na czas i tylko do jednego użytku. Technologia jednorazowego hasła (OTP) stała się teraz niedrogim rozwiązaniem dla większości aplikacji. Czytnik, który może być zaimplementowany w sprzęcie lub oprogramowaniu, musi zawsze prowadzić rejestr użytkowników, którym należy przyznać lub odmówić dostępu ze znacznikami czasu przechowywanymi w bazie danych. Zawartość bazy danych jest sprawdzana przez odpowiednie oprogramowanie w poszukiwaniu nieprawidłowości. Jeśli czytnik jest oprogramowaniem, funkcje biometryczne użytkownika mogą zostać zapisane i przekazane do procesora jako dodatkowy parametr uwierzytelnienia. Procesor jest najważniejszym elementem procesu kontroli dostępu. Sztuczna inteligencja może być wykorzystana do stworzenia profilu użytkownika pod względem kilku parametrów, takich jak pora dnia, miejsce wejścia, jeśli jest kilka, i ewentualnie dane biometryczne. Stopniowo telefon komórkowy staje się również integralną częścią procesu kontroli dostępu, ponieważ staje się względnie nierozerwalnie związany z użytkownikiem. Technologie dostępu fizycznego intensywnie wykorzystują telefonię komórkową do żądań dostępu, w których proces kontroli dostępu ma rezydenta , procesor identyfikowany przez numer telefonu i bazę danych numerów telefonów komórkowych upoważnionych użytkowników, którym przyznano dostęp podczas połączenia. Oprogramowanie udzielające dostępu rejestruje znacznik czasu / daty żądania, a tym samym prowadzi dokładną rejestrację czynności dostępu - żądania, przyznania lub odmowy. Korzystanie z telefonów komórkowych w procesie kontroli dostępu wykracza poza bezosobowe żądanie autoryzacji i staje się żądaniem uwierzytelnienia, w którym żądanie jest dołączone do rzeczywistej osoby. Środkiem komunikacji może być telefonia komórkowa, technologia Bluetooth lub łącze podczerwieni. W kontroli dostępu należy stosować zasadę najmniejszych uprawnień. Oznacza to, że użytkownik ma rozszerzone minimalne prawa dostępu, wystarczające do wypełnienia przypisanych obowiązków. Z czasem bezpieczeństwo infrastruktury stało się niezawodne do tego stopnia, że zajęło drugie miejsce pod względem bezpieczeństwa aplikacji. Najnowsze statystyki wskazują, że trzy na

cztery przypadki naruszenia bezpieczeństwa wynikają z aplikacji. Wpisy aplikacji są zwykle chronione przez nazwy użytkowników, hasła i ewentualnie pytania do tajnej wiedzy. Oprócz wspomnianego wcześniej wprowadzenia OTP, do uwierzytelnienia użytkownika można wykorzystać dodatkowe parametry, takie jak adres IP użytkownika, tam gdzie to możliwe, adres kontroli dostępu do mediów (MAC) lub kod International Mobile Equipment Identity (IMEI) w przypadek telefonii komórkowej. Rozwój i utrzymanie systemu

Cyberbezpieczeństwo nie może praktycznie zostać doposażone w system informacyjny. Nie jest ogrodzeniem zabezpieczającym, które należy umieścić wokół systemu, ale są to środki, które są osadzone w systemie informatycznym podczas jego procesu rozwoju. Rozwój rozpoczyna się od mapowania celów systemu na specyfikacje techniczne, specyfikacje techniczne na technologie, technologie na projekty, projekty na produkt końcowy i produkt końcowy na jego planie konserwacji. Poza celami systemowymi wszystko jest transformacją - nie ma nic oryginalnego, nic dowodzącego, wszystkie implementacje. Cele systemu muszą więc zawierać funkcje bezpieczeństwa przewidziane dla tego produktu lub usługi, a kolejne transformacje po prostu zrealizują te cele w najlepszy możliwy sposób i na ile pozwala na to obecna technologia. We wszystkich przypadkach przewidywane funkcje obejmują bezpieczeństwo oprogramowania i danych, ochronę przed utratą lub nieuprawnionym dostępem oraz ochronę autentyczności, integralności i poufności informacji. W fazie rozwoju systemu faza wymagań jest etapem, w którym interesariusz indywidualnie powołuje się na odpowiednią podstawę do włączenia cechy będące przedmiotem zainteresowania, podczas gdy wspólnie interesariusze wymagają mechanizmów bezpieczeństwa, które maksymalizują poufność, integralność i dostępność systemu. Na etapie wymagań uwzględnione zostaną środki bezpieczeństwa, które będą eskortować dane podczas ich podróży od wprowadzenia danych, przetwarzania, przechowywania i transmisji do następnego miejsca docelowego. Później w fazach analizy i projektowania zostaną wybrane technologie obrony; podpisy cyfrowe, certyfikaty cyfrowe, szyfrowanie i tym podobne, w których zapewnione zostaną kluczowe funkcje, takie jak niezaprzeczalność, uwierzytelnianie i integralność informacji. Pod koniec rozwoju produkcja - korzystanie z systemu - powinna rozpocząć się wraz z wymaganą konserwacją. Utrzymanie, w kontekście bezpieczeństwa, oznacza ciągłe badanie podatności systemu, szczególnie w odniesieniu do nowych zagrożeń, oraz wierną instalację poprawek bezpieczeństwa oprogramowania, gdy tylko zostaną udostępnione. Last but not least, ćwiczenia i ćwiczenia ratownicze.

Bezpieczeństwo fizyczne i środowiskowe

Bezpieczeństwo fizyczne dotyczy przede wszystkim bezpieczeństwa ludzi, co musi być głównym przedmiotem zainteresowania Głównego Urzędnika ds. Bezpieczeństwa Informacji. CISO najpierw określają fizyczny obwód swojego terytorium, a następnie określają środki, które należy zastosować, aby zapewnić niezbędny poziom bezpieczeństwa. Bardzo ważne jest, aby poziom bezpieczeństwa był proporcjonalny do poziomu zagrożeń i wartości chronionych zasobów. W sensie fizycznym i środowiskowym zagrożenia można ogólnie podzielić na pierwszą, nieupoważnioną osobę próbującą przedostać się do obszarów o ograniczonym dostępie, oraz drugą, niepożądaną sytuację środowiskową. Pierwsze zagrożenie eliminuje się poprzez prowadzenie dziennika dostępu, w którym rejestrowane są wszystkie działania wejścia / wyjścia. Odwiedzający powinni nosić odpowiednią plakietkę wskazującą na potrzebę lub nie autoryzowanej eskorty i pozwolenia lub nie posiadania aktywnego telefonu komórkowego. Kamery wideo mogą rejestrować działania w obszarach krytycznych w trybie 24/7/365. Warto powtórzyć, że środki bezpieczeństwa powinny być zgodne z wartością chronionych danych. Drugie zagrożenie może obejmować pożar, dym, opary, chemikalia, wodę, niedopuszczalną temperaturę lub wilgotność otoczenia lub utratę mediów. Oznacza to warunki środowiskowe, które niekorzystnie wpłynęłyby na ludzi, sprzęt lub dane. Każdemu z tych zagrożeń

można zaradzić za pomocą odpowiednich technologii, takich jak czujniki, systemy gaszenia pożarów, niezawodna klimatyzacja i regulatory napięcia z zasilaczami bezprzerwowymi. Jeśli to możliwe, praktyczne i konieczne, niech firma energetyczna zapewni dwa źródła zasilania z różnych stacji elektroenergetycznych.

Dla każdego z powyższych zagrożeń CISO muszą mieć plan, który musi być weryfikowany i testowany przynajmniej raz w roku. W rzeczywistości organizacja może mieć tydzień bezpieczeństwa, podczas którego testowane są wszystkie plany, z udziałem każdego pracownika w pewnym stopniu.

Spełnienie

Zgodność spełnia zestaw standardów. Nowe standardy kontroli jakości są stale ustanawiane w każdym sektorze. Te normy przyznają organizacji prawo do działania lub przynależności do specjalnej grupy w swojej kategorii. Wzrost liczby takich standardów z jednej strony i zależności organizacyjne związane z uznaniem ich za zgodne, z drugiej strony stworzyły obciążenie dla organizacji, które są przekazywane do Biura Zgodności kierowanego przez Inspektora ds. Zgodności. Zadaniem Specjalisty ds. Zgodności jest upewnienie się, że spełnione są prawne, techniczne, a nawet społeczne wymagania organizacyjne, do których organizacja jest zobowiązana lub zobowiązana się stosować. Rząd federalny USA ma federalną ustawę o zarządzaniu bezpieczeństwem informacji (FISMA), która jest ustawą nakładającą na agencje rządowe obowiązek przedstawienia corocznego znormalizowanego raportu wykazującego zgodność z wytycznymi ustawy. Inne wytyczne odnoszą się do fizycznej ochrony i przechowywania dokumentów. Ten został wydany przez National Fire Protection Association. Zgodność z tym standardem jest czynnikiem obliczającym składki na ubezpieczenie przeciwpożarowe. W dziedzinie bezpieczeństwa informacji Międzynarodowa Organizacja Normalizacyjna (ISO) wydała różne normy zawierające ważne wytyczne. Bardzo ważny jest ISO27002 na temat zarządzania bezpieczeństwem informacji, skierowany głównie do dyrektorów IT. Specjalista ds. Zgodności nadzoruje również zgodność organizacyjną z własnymi politykami, zwłaszcza jeśli dotyczą one prywatności, ochrony praw intelektualnych, praw pracowniczych, nękania i relacji międzyludzkich w ogóle. Na przykład w różnych stanach istnieją normy wymagające od firm powiadamiania klientów w przypadku utraty danych osobowych znajdujących się pod ich opieką. Jednak w kilku przypadkach, jeśli utracone dane były w postaci zaszyfrowanej, powiadomienie nie jest wymagane. Wreszcie, specjaliści ds. Zgodności są odpowiedzialni za przeglądanie zapisów dotyczących pozyskiwania oprogramowania, upewniając się, że całe oprogramowanie w organizacji jest odpowiednio licencjonowane.

Bezpieczeństwo personelu

Podstawową cechą bezpiecznej organizacji jest istnienie dwóch rodzajów środków: środki, które chronią personel przed uszkodzonym sprzętem lub nadużyciami oraz środki, które chronią organizację przed działaniami personelu, które mogą spowodować szkody. Podczas gdy bezpieczeństwo fizyczne musi być przedmiotem troski wszystkich, odpowiedzialność za nie spoczywa na konkretnej osobie - oficerze bezpieczeństwa. Ta osoba będzie szukała niewłaściwego wykorzystania urządzeń, oszustwa, kradzieży i działań sprzecznych z Podręcznikiem Polityki Bezpieczeństwa Korporacyjnego.

Organizacja bezpieczeństwa

Struktura organizacyjna personelu bezpieczeństwa informacji powinna być kierowana przez kierownika wyższego szczebla z doświadczeniem w zakresie bezpieczeństwa informacji kierującego zespołem doświadczonych i stale przeszkolonych specjalistów. „Role i obowiązki powinny być zdefiniowane dla [każdej] funkcji bezpieczeństwa informacji" i powinny być wyraźnie określone w Podręczniku polityki bezpieczeństwa korporacji organizacji. Należy uwzględnić osobną sekcję

dotyczącą wymiany informacji między stronami zewnętrznymi - klientami, partnerami i organami nadzoru. Outsourcing zawsze był relacją krytyczną dla bezpieczeństwa.

Zarządzanie komputerem i siecią

Komputery, w szczególności sieciowe, stanowią najbardziej podstawową infrastrukturę każdego systemu informatycznego. W związku z tym ich niezawodność i interoperacyjność muszą być zagwarantowane przez cały czas dzięki dostępności odpowiednio przeszkolonych specjalistów z obowiązkami określonymi w ISO17799.

Klasyfikacja i kontrola aktywów

W szerokim znaczeniu wszystko w organizacji jest atutem. Aktywa mogą być materialne, takie jak oprogramowanie, sprzęt i personel, lub niematerialne, takie jak relacje, reputacja i wiedza specjalistyczna. Jednak ogólne postrzeganie aktywów skłania się bardziej ku temu pierwszemu. Aktywa należy podzielić na odpowiednie kategorie, których poziom znaczenia dla organizacji jest wyraźnie określony. Równolegle do tego poziomu działa poziom bezpieczeństwa wymagany do ochrony zasobu. Przez kontrolę aktywów rozumiemy, że należy przechowywać zapisy dotyczące cyklu życia każdego zasobu. Cykl życia rozpoczyna się od decyzji o ich przejęciu, po której następuje przejęcie zgodnie z ustalonymi procedurami, ich właściwe użytkowanie i utrzymanie, a na koniec wycofanie lub zmiana przeznaczenia. Organizacje prowadzą bazy danych zasobów fizycznych i oprogramowania oraz powiązane zasady. Należy jednak zwrócić uwagę na wartości niematerialne, ponieważ są one tymi, które skutecznie gwarantują ciągłość działalności.

Polityka bezpieczeństwa

Polityka bezpieczeństwa organizacji jest udokumentowana w podręczniku udostępnianym wszystkim członkom.

Zarządzanie kluczami szyfrującymi

Wraz ze spadkiem kosztów przechowywania i sieci nastąpił gwałtowny wzrost ilości danych, które muszą być bezpiecznie przechowywane, oraz wzrost liczby łączy komunikacyjnych, które należy zabezpieczyć. W związku z tym liczba nazw użytkowników i haseł, które może mieć organizacja, może z łatwością wzrosnąć do setek. Równolegle do dużej liczby parametrów szyfrowania pojawia się potrzeba spełnienia wymagań regulacyjnych i innych wymagań dotyczących zgodności. Ta potrzeba stworzyła przemysł zarządzania kluczami szyfrującymi (EKM), oferujący szeroki zakres usług, od tworzenia i kontroli kluczy szyfrowania po moduły sprzętowe w celu bezpiecznej ochrony kluczy.

Funkcje EKM

Usługi EKM oferują szeroki zakres funkcji, które obejmują

• Tworzenie, dystrybucja i niszczenie kluczy (haseł).

Dla

• Użytkowników zewnętrznych (klienci, współpracownicy itp.)

• Użytkowników wewnętrznych

• Personel zajmujący się przetwarzaniem danych

• Administratorów danych

• Egzekwowanie kluczowych zasad użytkowania

• Utrzymania dzienników użytkowania

• Wymiany kluczy po wygaśnięciu

• Tworzenia i rozpowszechniania raportu użycia kluczy

• Obsługi aplikacji kryptograficznych

• Generowania liczb losowych

• Zautomatyzowania operacji kryptograficznych

• Szyfrowania kopert

• Szyfrowania kluczy szyfrujących

• Szyfrowania przy użyciu wielu kluczy. Oznacza to, że jeśli obiekt, który ma zostać zaszyfrowany, jest duży, można go podzielić na segmenty z każdym kluczem.

• Wyboru najbardziej odpowiedniego algorytmu szyfrowania, w zależności od kontekstu danych.

Wybór klucza

Wybór kluczy szyfrowania uwzględnia warunki aplikacji, w których dane muszą być bezpieczne. Takie warunki obejmują

• Bezpieczeństwo danych w spoczynku

• Bezpieczeństwo danych w transporcie

• Tworzenie danych w miejscu pochodzenia

• Dostęp do danych w miejscu docelowym

• Konieczność szyfrowania kluczy szyfrujących

W każdych okolicznościach, oprócz bezpieczeństwa i poufności danych, chodzi również o integralność danych. Na przykład hałaśliwe medium spowoduje uszkodzenie danych niezależnie od zastosowanego poziomu poufności.

Algorytmy

Istnieją zasadniczo dwa rodzaje schematów szyfrowania-deszyfrowania. Jednym z nich jest szyfrowanie symetryczne, w którym ten sam klucz jest używany do szyfrowania danych, a także do deszyfrowania danych. Drugim jest szyfrowanie asymetryczne, w którym klucz szyfrowania danych różni się od klucza deszyfrowania danych. Mogą istnieć nieskończone projekty takich schematów kryptograficznych. Bardzo popularnym i powszechnie akceptowanym schematem szyfrowania asymetrycznego jest algorytm RSA. Projekt tego algorytmu wykorzystuje liczby pierwsze i jest znany publicznie. Deweloper twierdzi, że złamanie kodów będzie wymagało bardzo mocnych komputerów obliczających przez długi czas. Jednak dokładne badanie † przygotowane przez SANS Institute opublikowało następujące trzy wnioski:

Po pierwsze: „... istnieje backdoor do RSA (system kryptograficzny) i można go otworzyć, biorąc pod uwagę moduł. ”

Po drugie: „Nie ma znanej metody szybkiego i jednoznacznego testowania danej liczby pod kątem pierwszeństwa”.

Po trzecie: „... dochodzenia mogą pewnego dnia dostarczyć wydajnego algorytmu uwzględniającego bardzo duże liczby w ich głównych czynnikach, przełom (lub nie, zależnie od tego, jak się na to spojrzy), który sprawiłby, że większość współczesnych systemów kryptograficznych z kluczem nie byłaby użyteczna”.