Bezpieczne systemy informatyczne

Każda firma to biznes cybernetyczny.

Wprowadzenie

Dla wszystkich praktycznych celów każdy system informacyjny jest hostowany przez Internet, a jego stan bezpieczeństwa jest w najlepszym razie taki sam jak w samym Internecie. System informacyjny może zwiększyć swoje bezpieczeństwo poprzez wydostanie się z Internetu, ale to może zerować jego funkcjonalność. Dlatego, chociaż wiele środków bezpieczeństwa można zastosować do pojedynczego systemu informatycznego, jego ogólne bezpieczeństwo jest funkcją cyberbezpieczeństwa. Fizyczny aspekt cyberprzestrzeni, Internetu, to zbiór sieci, które indywidualnie wiernie przekazują sobie nawzajem pakiety, ale łącznie nie posiadają inteligencji, która byłaby w stanie rozpoznać zagrożenie indywidualne lub rozproszone. W związku z tym „Bezpieczeństwo przedsiębiorstwa w przedsiębiorstwie [jest] zagrożone bez globalnej zintegrowanej architektury bezpieczeństwa". Prowadzone są niekończące się badania w celu opracowania skutecznych metodologii cyberobrony, ale są one w większości skierowane na obronę poszczególnych systemów informatycznych. „W ciągu ostatnich 10 lat agencje rządowe USA zwiększyły inwestycje ... [ale] nadal brakuje technologii bezpieczeństwa wystarczającej do ochrony kluczowej infrastruktury [nadal]. Konsorcjum DETER tworzy jednak model cyberfizyczny, w którym można opracowywać i testować technologie cyberobrony. Ostatecznie zbiorowa wiedza o ruchu cybernetycznym, obecnie rezydująca w kawałkach w poszczególnych węzłach internetowych, zostanie zintegrowana i stworzy inteligentny system, który będzie w stanie rozpoznawać i zapobiegać cyberatakom. Bezpieczeństwo systemu informatycznego wymaga strategii obrony na dwóch frontach. Jednym z frontów są granice ze światem zewnętrznym, a innym frontem jest ochrona każdego z zasobów systemowych indywidualnie. Granice to w zasadzie Internet, przez który wnioski przychodzą do systemu informacyjnego, który z kolei może odpowiadać cennymi danymi dla hakera lub może zaakceptować prośbę hakera jako polecenie swojego administratora. Tutaj zdolność rozróżniania między rzetelnymi żądaniami i fałszywymi stanowią udane cyberbezpieczeństwo. Drugim frontem jest wewnętrzna ochrona zasobów, danych i procesów organizacji. ISO / IEC 17799: 2005 „ustanawia wytyczne i ogólne zasady inicjowania, wdrażania, utrzymywania i ulepszania zarządzania bezpieczeństwem informacji w organizacji". Podstawowymi cechami bezpiecznego systemu informacyjnego są jego integralność, dostępność i poufność. Te cechy muszą mieć zastosowanie do każdego elementu tego systemu. Przed opracowaniem strategii bezpieczeństwa cybernetycznego lub kompleksowego planu bezpieczeństwa informacji korporacyjnych konieczne jest, aby najpierw zidentyfikować aktywa, które mają być chronione, i zapisać w bezpiecznej bazie danych.

Identyfikacja aktywów

Zasoby informacyjne w organizacji są identyfikowane według nazwy, lokalizacji, właściciela, opiekuna i parametrów, a ich plikami należy zarządzać zgodnie ze zdefiniowaną polityką korporacyjną.

Nazwa. Zasób informacji korporacyjnej musi mieć nazwę elektroniczną, która definiuje - bezpośrednio lub za pomocą kodu - jego treść i przynależność organizacyjną w przedsiębiorstwie. Na przykład w kontekście firmy ubezpieczeniowej nazwa pliku polisy może mieć nazwę auto / 2008 / miami / 12345 / johnson / 001 .pdf. W ten sposób hierarchiczna klasyfikacja plików może być wyjaśniona i rozpoznawalna przez personel nietechniczny. Oczywiście należy unikać używania znaków innych niż alfanumeryczne lub spacji.

Lokalizacja. Jest to fizyczna lokalizacja nośnika pamięci. Komputery korporacyjne muszą mieć wyraźnie zidentyfikowane wszystkie obszary pamięci. Wszystkie dyski twarde w licznych komputerach

organizacji są opatrzone identyfikacją na podstawie przypisanego wzorca. Najprościej byłoby po prostu przypisać numer do każdego komputera i wewnętrznie zmienić nazwę dysków, w tym tego numeru. Na przykład, jeśli korporacyjny komputer ma numer 1234, jego dyski zostaną przemianowane na 1234C: lub 1234D: i tak dalej. Ta nazwa wymaga uprawnień administracyjnych, które powinny być zastrzeżone tylko dla personelu bezpieczeństwa IT. W związku z tym użytkownicy nie będą mogli zmienić nazwy urządzeń pamięci. Komplikacje są oczywiście tworzone, gdy zasoby znajdują się w chmurze. Chmura jest zewnętrznym narzędziem usług obliczeniowych dynamicznego adresowania i alokacji przestrzeni, w którym fizyczna lokalizacja danych lub serwerów jest trudna do zidentyfikowania, a przechowywane dane i zasoby komputerowe są identyfikowane tylko poprzez adresowanie logiczne.

Właściciel. Identyfikacja właściciela może składać się z dwóch części. Jedna część to bezosobowy właściciel korporacji. Taki jest tytuł działu lub osoby odpowiedzialnej za kontrolę nad danym aktywem. Na przykład właścicielem może być Departament Kont Specjalnych lub Zastępca Dyrektora ds. Kont Specjalnych. Drugą częścią właściciela zasobu może być osoba fizyczna, która utworzyła / odczytuje / modyfikuje / usuwa prawa do tego zasobu.

Ochroniarz. Identyfikacja ochroniarza będzie podobnie składać się z dwóch części. Jedną z części jest bezosobowa ochrona korporacyjna, czyli tytuł działu lub osoby odpowiedzialnej za bezpieczeństwo danego aktywa. Na przykład wyznaczonym opiekunem może być Departament Bezpieczeństwa IT lub Koordynator Bezpieczeństwa Kont Specjalnych. Drugą częścią ochrony zasobów jest osoba fizyczna, która jest odpowiedzialna za bezpieczeństwo tego konkretnego zasobu.

Parametry .Parametry są operacyjne i związane z bezpieczeństwem. Parametry operacyjne określają nominalne zastosowanie, a parametry bezpieczeństwa określają środki, które zapewnią poufność, integralność i dostępność zasobu. Co ważne, środki muszą odzwierciedlać poziom ryzyka i poziom szkody w przypadku naruszenia bezpieczeństwa aktywów.

Zarządzanie plikami. Istnieją różne filozofie, jak najlepiej organizować pliki w danym obszarze pamięci. Poniższe zasady mogą prowadzić do dobrze zorganizowanej bazy danych.

• Po utworzeniu pliku zdecyduj, czy ma on zostać zaszyfrowany, czy nie. Następnie przypisz poziom bezpieczeństwa. W przypadku niskiego poziomu może wystarczyć ogólne hasło. Dla wysokiego bezpieczeństwa do każdego pliku można przypisać unikalne hasło. Problem może stanowić śledzenie przypisanych haseł i ich lokalizacji oraz ewentualne udostępnianie.

• Utwórz kopię zapasową za pomocą automatycznego mechanizmu tworzenia kopii zapasowych. Obawiaj się o bezpieczeństwo urządzenia do tworzenia kopii zapasowych i dostęp do niego.

• Użyj hierarchicznego schematu nazewnictwa katalogów. W zależności od działań specyficznych dla organizacji, najwyższą nazwą są zwykle lata lub projekty. Staje się więc wielorakimi latami lub projektami wieloletnimi.

• Po tym mogą być podprojekty lub miesiące roku, w zależności od początkowej selekcji.

• Następnie, na najniższym poziomie katalogów, poszczególne pliki można pogrupować według typu w odpowiednich podkatalogach.

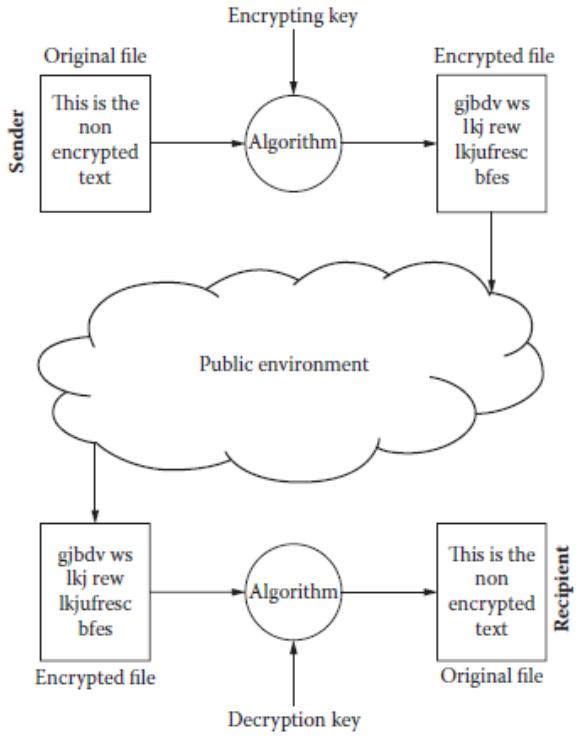
• Wszystkie pliki muszą mieć cykl życia - datę utworzenia, datę modyfikacji i datę wycofania. W pewnym momencie status ich znaczenia może ulec zmianie z aktywnej na usunięty lub do zarchiwizowania.

• Usunięte pliki powinny być elektronicznie niszczone. Niszczenie elektroniczne to proces wielokrotnego nadpisywania plików, których zawartość ma zostać wymazana nie do poznania. Istnieją różne podejścia do tego celu.

Komunikacja aktywów

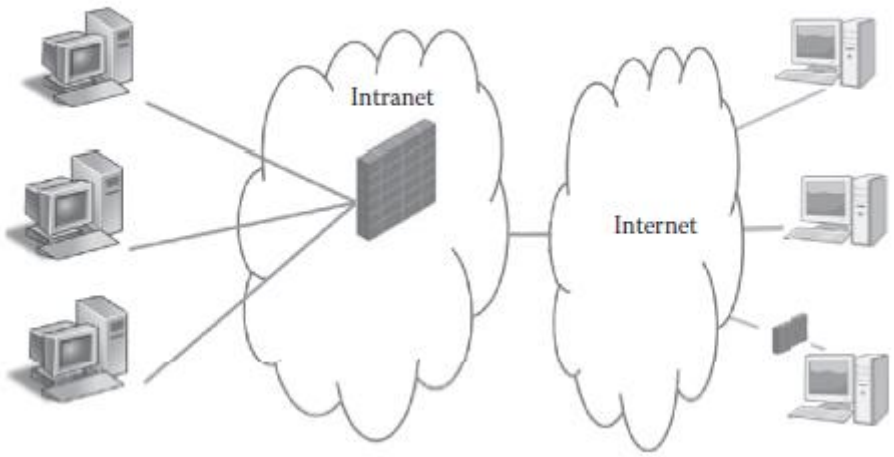
Dostęp lub transfer informacji cyfrowych stanowi lukę, narażając informacje na ryzyko. Takie ryzyko można jednak zminimalizować jeśli zastosowane zostaną odpowiednie środki ostrożności. Te środki ostrożności obejmują szyfrowanie, zapory ogniowe, certyfikaty cyfrowe, podpisy cyfrowe i kontrolę logowania.

Szyfrowanie: „Metody szyfrowania mają na celu zapewnienie poufności, integralności i niezaprzeczalności informacji". Kryptografia jest w praktyce od tysiącleci; jednak użycie potężnych komputerów sprawiło, że odszyfrowanie nie jest tak trudne, jak kiedyś. Istnieje wiele znanych algorytmów szyfrowania, których główną obroną jest nadmierny czas na złamanie. Większość aplikacji do przetwarzania dokumentów zawiera łatwe w użyciu i trudne do złamania opcje szyfrowania, w których osobne hasła mogą być stosowane do ochrony tylko do odczytu i do modyfikacji modyfikacji. Algorytmy szyfrowania są podzielone na symetryczne i asymetryczne. Algorytmy szyfrowania symetrycznego używają tego samego klucza do szyfrowania i deszyfrowania pliku. Taka praktyka, chociaż chroni przesyłane pliki, bardzo utrudnia uwierzytelnianie plików, ponieważ obie strony mogą utworzyć zaszyfrowany plik. Z drugiej strony algorytmy szyfrowania asymetrycznego mają dwa klucze, jeden do szyfrowania plików, a drugi do deszyfrowania plików. W takim przypadku twórca zaszyfrowanego pliku używa tak zwanego klucza prywatnego, a różni odbiorcy przechowują klucz publiczny. Plik zaszyfrowany kluczem prywatnym strony X można odszyfrować tylko za pomocą klucza publicznego tej samej strony X. W ten sposób zagwarantowana jest zarówno autentyczność, jak i poufność. Rysunek ilustruje zasadę szyfrowania plików.

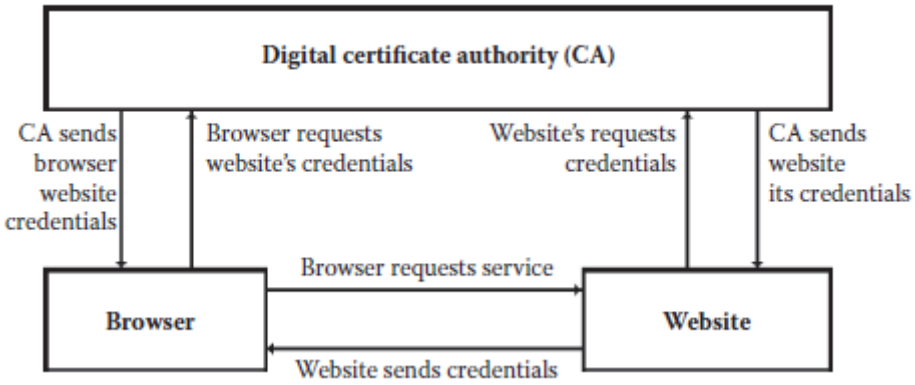


Zapory ogniowe: Zapory ogniowe są podstawą bezpieczeństwa danych. Ich fizyczną postacią może być oprogramowanie lub oprogramowanie zainstalowane na dedykowanym sprzęcie. Zapory ogniowe

służą jako strażnicy podłączeni do procesora komunikacyjnego systemu, badając ruch zewnętrzny zgodnie z określonymi kryteriami bezpieczeństwa. Badany ruch to zwykle ruch przychodzący, chociaż zapory ogniowe mogą być również wykorzystywane do badania ruchu wychodzącego. W przypadku kontroli ruchu przychodzącego zapory ogniowe analizują parametry przychodzących pakietów, korelując żądaną usługę z pochodzeniem pakietów. W zależności od chronionych zasobów zapory zezwalają na ruch na podstawie określonych kryteriów „tylko zezwolenie" lub „zezwolenie na wszystko, chyba że". Rysunek 4.2 ilustruje opcje zapory sieciowej, a mianowicie zapory sieciowej i prywatnej zapory zainstalowanej na komputerze osobistym.

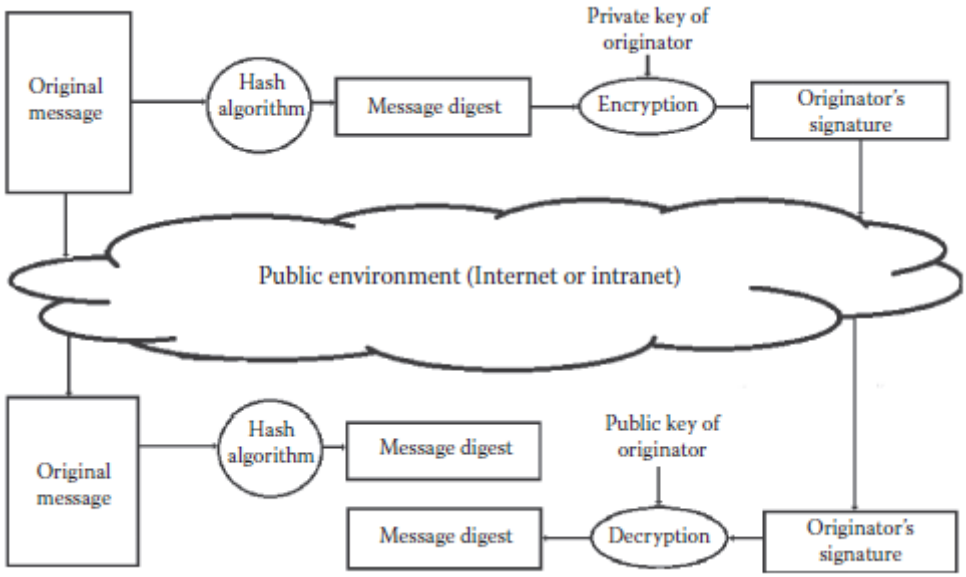


Certyfikaty cyfrowe : Certyfikat cyfrowy, znany również jako certyfikat klucza publicznego lub certyfikat tożsamości, służy do cyberprzestrzeni, czym jest karta kredytowa do handlu. W przypadku karty kredytowej strona trzecia, czyli firma wydająca kartę kredytową, potwierdza jakość karty. Na tej podstawie kupiec oferuje kupującemu produkt. Podobnie, gdy nasza przeglądarka pobiera dla nas stronę internetową, certyfikat cyfrowy potwierdza swoją ważność, komunikując się z urzędem certyfikacji, który udzielił tej stronie wiarygodności. Przeglądarki z cyfrowymi certyfikatami mogą uzyskiwać dostęp do serwerów zaprogramowanych do reagowania tylko na autoryzowane przeglądarki. Rysunek ilustruje zasadę cyfrowego certyfikatu



Podpisy cyfrowe : Podpisy cyfrowe towarzyszą plikom, które są zaszyfrowane, a także plikom, które nie są szyfrowane. Podpis cyfrowy pliku jest generowany przez splot plików nad określoną funkcją, tworząc unikalny klucz. Oznacza to, że plik jest przekazywany przez algorytm matematyczny, zwykle

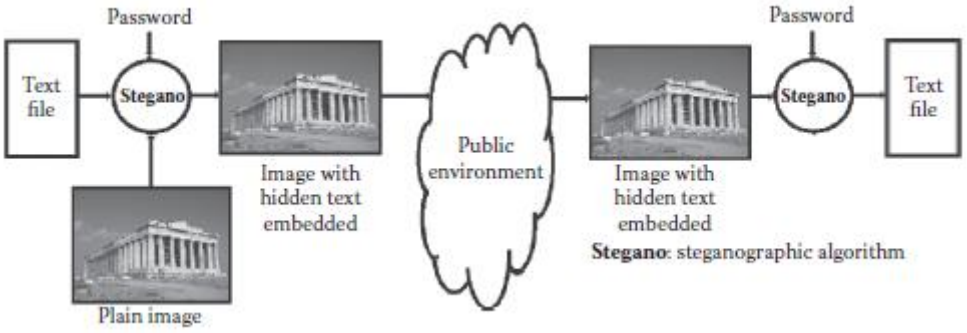
binarny, a na końcu tworzona jest krótka sekwencja liczbowa - ciąg znaków. Ze względów praktycznych ciąg ten jest unikalny dla tego pliku w kontekście tego algorytmu. Sekwencja, która może różnić się długością od 32 do 512 bitów, służy jako weryfikator autentyczności dołączonego pliku. Rysunek ilustruje zasadę podpisu cyfrowego.



Kontrola logowania : Ogólny dostęp do zasobów, a w szczególności dostęp do zasobów informacyjnych, wymagają konkretnych kontroli, które są weryfikowalne i kontrolowane. W tym drugim przypadku nazwy użytkownika i hasła są najczęstszymi środkami kontroli dostępu. Istnieje wiele punktów widzenia na wybór nazw użytkowników i haseł, wszystkie mające na celu zrównoważenie prostoty i skuteczności. W dalszej części tego rozdziału omówiono parametry hasła.

Przechowywanie aktywów

Wszystko w cyfrowym świecie to pliki. Pliki mogą zawierać tekst, arkusze kalkulacyjne, obrazy, filmy, muzykę itp. Ciągle tworzone są nowe typy plików, które wymagają specjalnych aplikacji do ich otwierania. Ich wymagania bezpieczeństwa pozostają jednak takie same. W razie potrzeby zawartość plików musi być niedostępna dla nieautoryzowanego użytkownika. Do użytku wewnętrznego organizacja może opracować własne mechanizmy bezpieczeństwa, algorytmy i kody, ale aby bezpiecznie komunikować się z partnerami, należy zastosować ogólnie przyjęte mechanizmy bezpieczeństwa. Podstawową zasadą zabezpieczenia plików przed nieautoryzowanym dostępem jest kryptografia, czyli poprzez pewien schemat, w którym pliki stają się niedostępne dla nieautoryzowanych użytkowników. Zasadniczo istnieją dwa takie schematy, steganografia i szyfrowanie. W steganografii pliki są bezpieczne, ponieważ są niewidoczne. Oznacza to, że pliki są umieszczane w katalogach, które prawdopodobnie nikt nie może wymyślić lub pliki mają nazwy lub rozszerzenia, które wprowadzają w błąd. Pliki można również ukryć w innych plikach. Na przykład plik tekstowy może ukryć się w pliku dźwiękowym lub obraz może ukryć się w innym obrazie. Rysunek ilustruje zasadę steganografii, w której plik tekstowy jest ukryty w znacznie większym pliku obrazu.



Istnieje wiele algorytmów steganograficznych. W przypadku obrazu zawierającego krótki plik tekstowy najmniej znaczące bity definicji koloru piksela łącznie przechowują krótką wiadomość. Oczywiście rozdzielczość kolorów obrazu jest zmniejszona, ale ta redukcja jest niewidoczna. Steganografia polega na bezpieczeństwie poprzez niejasność, która jest pogwałceniem podstawowej zasady bezpieczeństwa danych, która obejmuje bezpieczeństwo tylko poprzez szyfrowanie - inaczej mówiąc, bezpieczeństwo pliku poprzez odwracalne zatarcie pliku. W szyfrowaniu plik jest zabezpieczony przez przekazanie go przez algorytm matematyczny, który szyfruje bity i bajty pliku do punktu, w którym tylko algorytm będący odpowiednikiem może przywrócić plik do oryginalnej wersji. Narzędzie kontroli dostępu do zasobów

Resource Access Control Facility (RACF) to oprogramowanie, które przyznaje i kontroluje parametry kontroli dostępu. W biurze obsługi placówka wydaje nazwy użytkowników i hasła, natomiast w biurze obsługi rejestruje i kontroluje każdą czynność związaną z dostępem.

Obiekt znajduje się pod pełną kontrolą wyznaczonego urzędnika ds. bezpieczeństwa informacji w przedsiębiorstwie i służy jako wydawca początkowej nazwy użytkownika i hasła, które pozwolą nowemu użytkownikowi zalogować się do systemu po raz pierwszy. Istnieje wiele różnych zasad i filozofii dotyczących wyboru hasła. Bez wątpienia hasła powodują niedogodności dla użytkowników, którzy mogą skłaniać się w kierunku łatwego do zapamiętania i szybkiego wprowadzenia hasła. Złożoność hasła musi być wprost proporcjonalna do wielkości negatywnego wpływu, jaki może mieć kompromis. W interfejsie użytkownika, który wchodzi w interakcję z użytkownikiem, obiekt wymusza reguły hasła zaprogramowane przez wyznaczonego pracownika ds. Bezpieczeństwa informacji w przedsiębiorstwie. Znaki specjalne i spacje są albo odradzane, albo odradzane, w zależności od możliwości analizatora haseł. Proces wyboru nowego hasła może obejmować ocenę siły hasła , w której należy osiągnąć określony poziom siły hasła przed zaakceptowaniem nowego hasła. Dostępne mierniki siły hasła online mogą służyć do wskazywania siły danego hasła. W przypadkach, gdy wybór nowego hasła zależy wyłącznie od użytkownika, zaleca się losową kombinację cyfr i liter. „Organizacje powinny okresowo sprawdzać swoje zasady dotyczące haseł, szczególnie w przypadku poważnych zmian technologicznych (np. nowy system operacyjny), które mogą mieć wpływ na zarządzanie hasłami”. W biurze administracyjnym, które jest przezroczyste dla użytkownika, oprócz umożliwienia lub odmowy dostępu śledzi zachowanie każdej nazwy użytkownika i utrzymuje dziennik ze znacznikami czasu i dostępnymi zasobami. Analizy statystyczne uzyskanych danych mogą ujawnić próby kompromisu. Takie monitorowanie w czasie rzeczywistym we współpracy z korporacyjnym systemem wykrywania włamań może wywoływać alerty w czasie rzeczywistym. Przedsiębiorstwo z dużą siecią rozległej komunikacji zewnętrznej i cennych danych do ochrony musi mieć Pokój Operacji Bezpieczeństwa (SOR). W SOR wszystkie działania korporacyjnego systemu informacyjnego są monitorowane i kontrolowane, i właśnie tam kierowane są raporty z wykrywania włamań do oceny

Zabezpieczanie komunikacji e-mail

Jednym ze składników bezpiecznego przedsiębiorstwa jest system poczty elektronicznej organizacji, w którym reguły bezpieczeństwa mogą obejmować następujące elementy.

Strona serwera e-mail

• Zachowaj wszystkie kontrole administracyjne za zaporą ogniową.

• Zainstaluj rygorystyczny mechanizm uwierzytelniania administratora. Najlepiej zastosować schemat jednorazowego hasła (OTP). „Wygenerowane wcześniej hasła jednorazowe, zwane„ pobieraniem wstępnym ". Można je wydrukować lub wysłać pocztą e-mail, czatem lub SMS-em. Świetnie mieć, gdy masz ograniczony dostęp do sieci GSM lub podczas podróży ".

• Obsługuj oprogramowanie serwera e-mail z niezależnego sprzętu, który nie ma niepowiązanych wrażliwych plików.

• Utrzymaj zaktualizowane oprogramowanie wykrywające złośliwe oprogramowanie i przetestuj wszystkie przychodzące i wychodzące pliki pod kątem złośliwego oprogramowania.

• Utrzymuj zaktualizowaną listę spamowych serwerów e-mail i oflaguj spam dla wyznaczonego odbiorcy.

• Oprócz załącznika przetestuj treść wiadomości e-mail pod kątem aktywnego kodu, który może zawierać złośliwe oprogramowanie.

• Zachowaj listę słów, które, jeśli znajdują się w tekście wiadomości e-mail, podnieś flagę f do odbiorcy lub administratora.

• Zachowaj zgodność ze wszystkimi powszechnie używanymi klientami e-mail i przeglądarkami poczty internetowej.

• Zapewnij obsługę szyfrowania SSL / TLS [protokół Transport Layer Security (TLS), protokół Secure Sockets Layer (SSL)]. Są to protokoły kryptograficzne, które zapewniają bezpieczeństwo w komunikacji internetowej.

Po stronie klienta e-mail

• Oprogramowanie klienta poczty e-mail nie powinno być instalowane na sprzęcie komputerowym lub stacjach roboczych - które są używane jako serwery lub zawierają poufne informacje.

• Należy używać zaktualizowanych wersji systemu operacyjnego i klientów poczty e-mail.

• Używany sprzęt musi mieć zaktualizowane, samoaktualizujące się oprogramowanie antymalware, które monitoruje pliki w czasie rzeczywistym.

• Oprogramowanie poczty e-mail powinno działać w trybie użytkownika, w przeciwieństwie do trybu administratora, aby zapobiec narażeniu na cyberprzestrzeń uprawnień administracyjnych.

• Oprogramowanie poczty elektronicznej powinno być skonfigurowane do funkcji bezpieczeństwa zgodnie z zasadami organizacyjnymi. Polityka musi zapobiegać

• Automatyczny podgląd wiadomości

• Automatyczne otwieranie wiadomości

• Automatyczne ładowanie zdjęć w wiadomościach

• Automatyczne pobieranie aktywnych treści

• Automatyczne przetwarzanie aktywnych treści

• Przechowywanie nazw użytkowników i haseł

• Klient pozostanie aktywny po X minutach bezczynności

• Unikaj odczytu potwierdzenia i potwierdzenia odbioru, ponieważ są one wykonywalne i mogą łączyć się ze złośliwym oprogramowaniem.

• Wiadomości e-mail z podejrzanych lub nieznanych źródeł powinny być usuwane bez otwierania.

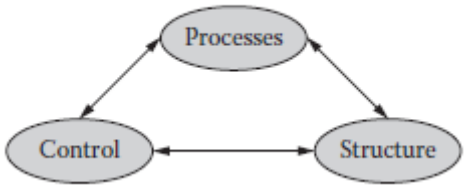
• Spamowa wiadomość e-mail może zawierać aktywne złośliwe oprogramowanie w opcji anulowania subskrypcji.

• Najlepiej, aby wiadomości e-mail były wyświetlane jako zwykły tekst. Zaawansowane formatowanie, takie jak HTML i RTF, może pozwolić złośliwemu oprogramowaniu na ukrywanie się w skryptach.

• Poufne wiadomości powinny być raczej wysyłane w postaci zaszyfrowanej jako załączone pliki niż w treści wiadomości e-mail.

Zarządzanie bezpieczeństwem informacji

Trzy filary bezpieczeństwa informacji to poufność, integralność i dostępność danych. Aby te właściwości były trwałe, potrzebne są zasoby, w związku z czym niezbędne jest wsparcie wyższej kadry zarządzającej. Podobnie, trzema filarami zarządzania są kontrole, procesy i struktury. Rysunek podkreśla trzy filary zarządzania.



Kontrola. Pod kontrolą znajdują się zasady organizacyjne dotyczące bezpieczeństwa, klasyfikacji i dostępności danych. Bezpieczeństwo to kosztowne przedsięwzięcie; w związku z tym poziomy bezpieczeństwa muszą być proporcjonalne do wartości organizacyjnej chronionego zasobu danych. W tym kontekście klasyfikacja danych odbywa się z myślą o bezpieczeństwie, dzięki czemu zasoby bezpieczeństwa są przydzielane w najbardziej odpowiedni i opłacalny sposób. Uwierzytelnienia użytkowników zawsze będą najważniejszym problemem w zakresie bezpieczeństwa, kierowanym potrzebą dostępu i wydajnością technologii.

Procesy. Zarządzanie z definicji polega na ustanawianiu procesów. W tym kontekście trzema podstawowymi procesami są zgodność, szyfrowanie i integralność danych. Istnieje wiele przepisów prawnych, które wymagają zgodności w zakresie bezpieczeństwa danych i prywatności danych, podczas gdy inne wymagają archiwizacji danych w celu ewentualnej kontroli w przyszłości. Szyfrowanie danych stanowi infrastrukturę bezpieczeństwa danych. Jednak skuteczność i kompatybilność determinują poziomy szyfrowania, technologie i standardy. Oprócz bezpieczeństwa dane muszą być poprawne dzięki zastosowaniu zaktualizowanego oprogramowania, weryfikacji i odporności na awarie.

Struktury. Niezależnie od poziomu automatyzacji obecność człowieka jest nieunikniona. Struktura bezpieczeństwa jest kierowana przez dyrektora ds. bezpieczeństwa informacji w organizacji, którego misją jest wdrażanie polityki bezpieczeństwa danych organizacji. To zadanie wymaga zespołu ekspertów z ciągle doskonalonymi umiejętnościami do obrony danych organizacyjnych w sposób wydajny i opłacalny. Logiczna struktura systemu informatycznego również musi zostać zaprojektowana z myślą o bezpieczeństwie, wdrożona przez zapory ogniowe i sieci VPN. Koncepcja przetwarzania w chmurze, stanowi nowe wyzwanie dla projektantów systemów informatycznych, ponieważ zależność od usług zlecanych na zewnątrz staje się absolutna. Z czasem zwiększone możliwości biznesowe spowodowały zapotrzebowanie na systemy informatyczne o niespotykanej dotąd złożoności, wymagające wymagania dotyczące interfejsu międzysystemowego i surowe wymagania dotyczące interoperacyjności. Stała się rasą wieczystą i nieprzerwaną. Technologia rośnie, a nowe możliwości biznesowe ze snów stają się rzeczywistością. Jednak ich wdrożenie nie jest proste, ale zależy od współpracy wielosystemowej, co w konsekwencji prowadzi do trudności w kontrolowaniu wzajemnych zależności. W tym stanie, zarówno z punktu widzenia biznesu, jak i możliwości technologicznych niepowodzenia, główne przyczyny to:

• Eskalacja technologii z późniejszym brakiem masy krytycznej specjalistów posiadających doświadczenie i wiedzę specjalistyczną.

• Współdziałanie technologii z licznymi standardami interfejsu i komunikacji.

• Technologie wirtualne z łatwością w montażu systemu, ukryte złożoności i często nieprzewidziane zachowanie.

• Nowe trendy hamujące dojrzałość i zwrot z inwestycji istniejących udanych technologii.

• Szybkość zmian jest większa, niż zarządzanie zmianą może śledzić.

• Złośliwe oprogramowanie, które jest zawsze od trzech do sześciu miesięcy przed oprogramowaniem zabezpieczającym.

Przy powyższych wyzwaniach utrzymanie bezpiecznego systemu informatycznego jest trudnym, ale nie niemożliwym zadaniem wymagającym całościowego uczestnictwa wizjonerów, programistów i użytkowników. „Przetrwanie organizacji zależy od możliwości ludzi, działań i technologii które składają się na proces operacyjny, który ma na celu wspólną pracę wydajność operacyjna" .

Opcje szyfrowania w wiadomościach e-mail

Gdy wiadomość e-mail opuszcza swój początek i zanim dotrze do miejsca docelowego, istnieje wiele transmisji i hubów, które niekoniecznie są bezpieczne. Wiadomość e-mail bez zabezpieczeń przypomina pocztówkę. Dlatego wiadomość e-mail musi być zaszyfrowana u źródła i odszyfrowana w miejscu docelowym. Typowe aplikacje pocztowe oferują opcję szyfrowania wiadomości e-mail u źródła hasłem i odszyfrowują ją w miejscu docelowym. Dla przedsiębiorstw istnieje więcej rozbudowanych portali e-mail, które oferują zaawansowane funkcje, takie jak

• Bezpieczny podpis elektroniczny, czyli cyfrowe podpisywanie zaszyfrowanych plików. W tym miejscu kod jest tworzony przez klucz prywatny nadawcy i jest weryfikowalny przez każdego z kluczem publicznym nadawcy, zapewniając w ten sposób autentyczność.

• Automatyczne szyfrowanie wiadomości e-mail i załączników, gdy nadawca używa klucza publicznego odbiorcy, zapewniając w ten sposób poufność.

• Obsługa urządzeń mobilnych, umożliwiająca pełne wykorzystanie aplikacji za pośrednictwem smartfonów.

• Zgodność z przepisami ustawowymi dotyczącymi ochrony danych, takimi jak HIPAA, HITECH, CFPB itp. Pełny opis aktów znajduje się w rozdziale dziewiątym.

• Załączanie dużych plików.

• Kompatybilność z innymi aplikacjami e-mail.

• Scentralizowane zarządzanie, umożliwiające pełny audyt.

• Ochrona antywirusowa i antyspamowa.

• Wykorzystanie PGP (Pretty Good Protection) * i szyfrowanie nośników wymiennych.

• Duża przestrzeń do przechowywania.

Aby zwiększyć bezpieczeństwo poczty e-mail, przedsiębiorstwa mogą mieć własny serwer e-mail, zamiast liczyć na obsługiwany serwer w chmurze (fizycznie poza lokalem przedsiębiorstwa)

Steganografia

Oprócz szyfrowania plik może być ukryty w znacznie większym pliku bez zauważalnego wpływu na efektywność dużego pliku. Zazwyczaj tak duże pliki to pliki obrazów, audio lub wideo. W tych plikach, zasób i jego jakość są reprezentowane numerycznie. W przypadku obrazów są próbki kolorowych kropek - piksele natomiast w przypadku audio są próbki dźwięku. Tak czy inaczej, próbki te są reprezentowane przez odpowiadające im liczby binarne do jakości próbki. Najprostszym sposobem jest poświęcenie najmniej znaczącego bitu liczb binarnych do wprowadzenia i ukrycia danych, które mają być ukryte. Wpływ tego działania na ludzkie postrzeganie obrazu, dźwięku lub wideo jest znikomy. Bardzo popularnym narzędziem steganografii jest S-Tools z licznymi plikami do pobrania