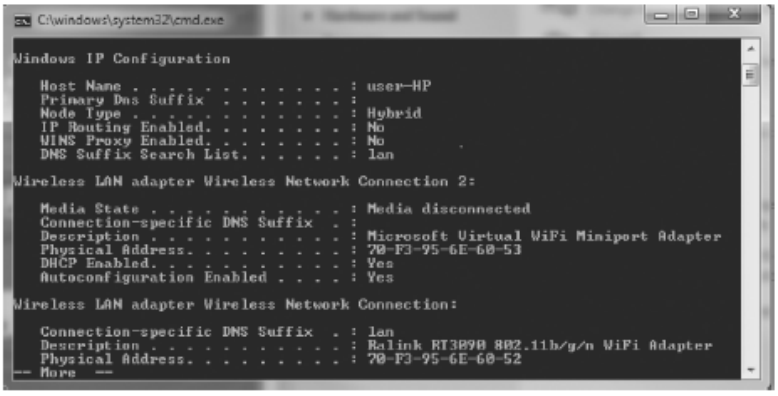
Luki w systemach informatycznych

Cyberprzestrzeń: od terra incognita do terra nullius.

Wprowadzenie

Luka w zabezpieczeniach dowolnego systemu jest wynikiem celowego lub niezamierzonego pominięcia lub nieumyślnego błędu projektowego, który bezpośrednio lub pośrednio prowadzi do kompromisu w zakresie dostępności, integralności lub poufności systemu. W ramach zapewniania informacji luki mogą ukrywać się na każdym poziomie bezpieczeństwa, czy to bezpieczeństwa dostępu do informacji, bezpieczeństwa komputera i pamięci masowej, bezpieczeństwa komunikacji czy bezpieczeństwa operacyjnego i fizycznego. W przypadku systemów informatycznych głównymi komponentami są ludzie, sprzęt i oprogramowanie. Z tego względu należy poszukiwać luk w każdym z tych trzech obszarów.

Ponad pół wieku temu projektanci, inżynierowie i naukowcy z powodzeniem skwantyfikowali pojęcie niezawodności w zakresie projektowania i konserwacji sprzętu i oprogramowania w mniejszym stopniu. Obecnie podejmowane są wysiłki w celu oszacowania abstrakcyjnej koncepcji podatności na zagrożenia, która dotyczy bezpieczeństwa systemów informatycznych. Celem jest wyrażenie postrzeganego poziomu bezpieczeństwa w sposób mierzalny, ustandaryzowany i zrozumiały oraz poprawa „… mierzalności bezpieczeństwa poprzez wyliczenie podstawowych danych bezpieczeństwa, zapewnienie znormalizowanych języków jako środków do dokładnego przekazywania informacji i zachęcanie do udostępnianie informacji użytkownikom poprzez tworzenie repozytoriów ”. Luki w zabezpieczeniach można ukryć w danych, kodzie, a najczęściej w procesach, które przypadkowo umożliwiają nieautoryzowany dostęp. Włamania mogą jednak wystąpić nie tylko w Internecie, ale także w intranetach, w których najczęściej bezpieczeństwo nie jest tak silne. Bezpieczeństwo można wzmocnić dzięki inteligentnym mechanizmom uwierzytelniania stosowanym na obu końcach - po stronie użytkownika, jak i po stronie serwera. Po stronie użytkownika uwierzytelnianie można znacznie wzmocnić dzięki wprowadzeniu dodatkowych mechanizmów, takich jak hasła jednorazowe (OTP), zapewnianych przez kanały wewnątrz- lub dodatkowe. Takimi kanałami mogą być dane biometryczne, kwestionariusze lub dodatkowe przejrzyste parametry związane z numerami identyfikacyjnymi urządzenia użytkownika, takie jak numer seryjny producenta, Media Access Control (MAC) lub International Mobile Equipment Identity (IMEI). MAC, zwany także adresem fizycznym, to 48-bitowa liczba, wyrażona jako 12 cyfr szesnastkowych, która jednoznacznie identyfikuje interfejs sieciowy komputera. Obwód interfejsu sieciowego może być wkładaną kartą sieciową lub może być osadzony w płycie głównej komputera. Rysunek pokazuje, jak można zidentyfikować adres MAC komputera osobistego.



IMEI w podobny sposób jednoznacznie identyfikuje urządzenia korzystające z telefonii komórkowej i jest liczbą, zwykle o długości od 13 do 15 cyfr. Dostawcy telefonii komórkowej przypisują numer telefonu urządzeniom łączącym je z ich identyfikatorem IMEI. Rycina 1.3 ilustruje dostępne numery IMEI wewnątrz telefonów komórkowych.

Oprócz dostępnych numerów MAC i IMEI do uwierzytelnienia można również używać numerów seryjnych urządzenia i parametrów sieci, takich jak adresy intranetowe i internetowe. Powyższe dotyczy uwierzytelniania klienta w stosunku do serwera. Po stronie serwera użycie certyfikatów, ograniczeń IP i enkapsulacji danych może znacznie poprawić uwierzytelnianie i bezpieczeństwo. Podczas transportu dane mogą być chronione kodami skrótu, takimi jak cykliczny kod redundancji (CRC), oraz szyfrowaniem klucza prywatnego / klucza publicznego , mechanizmy Luki w systemach informatycznych mogą wynikać z bardzo różnych przyczyn, od penetracji zapory ogniowej i ataków koni trojańskich po decentralizację i statyczny przydział zasobów. Najczęściej luki są wprowadzane podczas aktualizacji lub dostosowywania systemów do nowych środowisk operacyjnych.

Przyczyny podatności

W kontekście cyberbezpieczeństwa podatność jest brakiem, który może spowodować obniżenie wydajności lub awarię systemu. Taki niedobór może występować w samej aplikacji lub w komputerze hosta, w sieci, a nawet w brakach szkoleniowych użytkownika.

Dlatego aplikacje muszą być stale sprawdzane. Parametry aplikacji, oprócz samego kodu oprogramowania, obejmują interfejsy z systemem hostingu, a także interfejsy z użytkownikami. Dlatego kod należy zastąpić zaktualizowanym, należy wziąć pod uwagę nowe cechy systemu hostingu i poprawić umiejętności użytkownika. Poprawki dostarczone przez programistę należy natychmiast zastosować. Ponadto aplikacje zaprojektowane dla określonej wersji systemu operacyjnego niekoniecznie muszą działać z inną wersją wcześniejszą lub późniejszą. Chociaż sama aplikacja może być bezpieczna, jej zdalna dostępność może mieć słabą kontrolę, taką jak hasła lub inne mechanizmy uwierzytelniania, tworząc w ten sposób lukę w systemie. Często sieć organizacji jest wypełniona aplikacjami, które nieumyślnie i przypadkowo umożliwiają dostęp krzyżowy. Oznacza to, że legalne

wejście do jednej aplikacji umożliwia wejście backdoora do innej. W takim przypadku konieczna jest segmentacja sieci w celu wyeliminowania takiej podatności. Na przykład sieć operacji finansowych i punkty dostępu powinny być fizycznie oddzielone od dostępu użytkowników do informacji o produktach. Należy zdać sobie sprawę, że ochrona, czy to dla kraju, domu czy bazy danych, ma wiele parametrów, z których każdy ma swoją cenę. Tak więc każda tarcza ochronna musi przejść analizę opłacalności, aby zoptymalizować alokację zasobów organizacji. Luki można tworzyć z wnętrza organizacji. Nazywamy to zagrożeniem dla osób z wewnątrz. Takie zagrożenie niekoniecznie musi być złośliwe. Przeważnie takie podatności wynikają z dwóch następujących głównych kategorii:

• Brak szkolenia w zakresie cyberbezpieczeństwa dla personelu

• Niedojrzały osąd, szczególnie w zakresie cyberbezpieczeństwa środków

Wewnętrzne szkolenie w zakresie bezpieczeństwa cybernetycznego dla wszystkich osób uzyskujących dostęp do sieci jest podobne do uzyskiwania prawa jazdy, z tą różnicą, że szkolenie w zakresie bezpieczeństwa cybernetycznego wymaga aktualizacji w miarę ewolucji zagrożeń cybernetycznych.

Pomiar podatności

US National Institute of Standards and Technology (NIST) opracował protokół znormalizowanej klasyfikacji i oceny zawartości zabezpieczeń w systemie oprogramowania w celu „ujednolicenia sposobu identyfikacji i katalogowania podatności na zagrożenia i informacji o konfiguracji". Protokół nosi nazwę Security Content Automation Protocol (S'CAP, wymawia się „es-cap") i składa się z następujących sześciu składników.

1. Typowe luki w zabezpieczeniach i narażenia (CVE). Jest to depozyt znanych zarejestrowanych luk w zabezpieczeniach informacji, w których każde wystąpienie ma swój własny, niepowtarzalny numer identyfikacyjny. Początkowo takie zdarzenie jest definiowane jako potencjalna luka, a jeśli zostanie zaakceptowane, staje się wpisem zarejestrowanym na liście MITER CVE i ostatecznie zarejestrowanym w National Vulnerability Database (NVD). Pod koniec lata 2010 r. NVD zawierało 43 163 luki w zabezpieczeniach CVE, rosnąc w tempie 11 luk dziennie. W tej bazie danych można znaleźć słabe punkty bezpieczeństwa wielu programów, w tym dobrze znanych systemów operacyjnych i przeglądarek internetowych.

2. Common Configuration Enumerator (CCE). Jest to podobny depozyt, ale zawiera luki w zabezpieczeniach i niespójności interfejsu występujące w konfiguracjach systemu. Takie informacje mogą pomóc w zapewnieniu zgodności z przepisami, w określeniu właściwej interoperacyjności, a także w kontrolach audytu. Dostarczone informacje są w formie narracyjnej identyfikującej istniejące problemy i zwykle zalecającej rozwiązania.

3. Common Platform Enumerator (CPE). Ten komponent protokołu dotyczy prawidłowej nazewnictwa oprogramowania i oferuje hierarchiczną strukturę. W ten sposób oprogramowanie jest zdefiniowane jawnie, co znacznie ułatwia zarządzanie zapasami oprogramowania

4. Common System Vulnerability Scoring System (CVSS) Jest to algorytm, który bierze pod uwagę parametry związane z opracowaniem i użyciem przedmiotowego oprogramowania i zapewnia wynik wyrażający poziom obliczonego bezpieczeństwa. Dostarczony algorytm jest dostępny do użytku bez żadnych kosztów i cieszy się powszechnym stosowaniem przez projektantów systemów i analityków bezpieczeństwa wykonujących analizy ryzyka i planowanie systemu. Kalkulator CVSS dostępny online implementuje opracowany algorytm

5. Format opisu rozszerzalnej listy kontrolnej konfiguracji (XCCDF). Jest to szablon XML, który ułatwia przygotowanie znormalizowanych dokumentów zawierających wytyczne bezpieczeństwa, które przedstawiają luki w zabezpieczeniach lub obawy związane z bezpieczeństwem całego oprogramowania lub konkretnych konfiguracji lub zastosowań oprogramowania adresowanego, w znormalizowanym „ zawartość konfiguracyjna za pomocą zautomatyzowanych narzędzi bezpieczeństwa ".

6. Otwarty język luk w zabezpieczeniach i język oceny (OVAL). Służy to jako wspólny wątek „w całym spektrum narzędzi i usług związanych z bezpieczeństwem informacji ... (i)… standaryzuje trzy główne etapy procesu oceny", a mianowicie reprezentację informacji o systemie, wyrażenie konkretnego stany maszyny, a na koniec raportowanie oceny, wszystko w języku wspólnym dla społeczności systemów bezpieczeństwa. Przedsiębiorstwa używają OVAL do szerokiej gamy kluczowych funkcji, w tym oceny podatności, zarządzania konfiguracją, zarządzania poprawkami, zasad zgodności, dokumentacja porównawcza i automatyzacja zawartości bezpieczeństwa. „Protokół Security Content Automation Protocol (S'CAP) to synteza interoperacyjne specyfikacje pochodzące z pomysłów społeczności. " Poza S'CAP inne inicjatywy zapewniają normalizację w dodatkowych obszarach. Należą do nich: Common Weaknesses Enumerator (CWE), Common Malware Enumerator (CME), Common Weaknesses Scoring System (CWSS), Malware Attack Enumeration and Characterization (MAEC), oraz Common Attack Enumeration and Classification (CAPEC)). Łącznie powyższe standardy składają się na bardzo potężną infrastrukturę do oceny podatności systemów informatycznych i raportowania. W związku z tym podatności, słabości i złośliwe oprogramowanie można opisać w dokładny, znormalizowany, ilościowy i wyraźny sposób. Korzystając z technologii S'CAP, systemy informacyjne można klasyfikować pod względem poziomu bezpieczeństwa w sposób, który jest standardowy i ostatecznie akceptowany w całej branży.

Unikanie luk w zabezpieczeniach dzięki bezpiecznemu kodowaniu

W kulturze tworzenia oprogramowania, jeszcze nie tak dawno temu, celem projektowania było tworzenie efektywnych programów z minimalną liczbą linii kodu lub wykonywanie w minimalnym czasie lub kombinacja obu. Odzwierciedlając wysoki koszt pamięci i niską prędkość procesorów, cennymi towarami były przestrzeń pamięci i szybkość wykonywania. Tolerancja błędów dla integralności danych często przychodziła na myśl projektantom, ale nigdy dodatkowego kodu dla bezpieczeństwa, ponieważ wszystkie systemy były autonomiczne i fizycznie odizolowane od siebie. W dużych projektach oprogramowania luki można zminimalizować, dzieląc kod i dane na sekcje rezydentne i przejściowe, zgodnie z zasadami projektowania systemu operacyjnego. Oznacza to, że gdy wywoływana jest aplikacja, procedury i dostęp do danych są wprowadzane tak, jak tego wymaga natychmiastowa potrzeba, zamiast gromadzenia całego spisu aplikacji. W ten sposób, jeśli dojdzie do ingerencji złośliwego oprogramowania, szkody zostaną uwzględnione w pobranej (załadowanej pamięci) części aplikacji. Dzisiaj, ogólnie mówiąc, ani przestrzeń pamięci, ani szybkość przetwarzania nie wydają się już ograniczeniami programowymi. Ta era minęła nieodwracalnie, a jej miejsce zajął świat szybkich połączeń wzajemnych. Internet oferuje tak wysoki poziom użyteczności, że każdy możliwy do podłączenia sprzęt, od telefonów komórkowych po superkomputery, chce zostać podłączony. Podany poziom tego zaawansowanego narzędzia i wygody skutkuje zwiększoną produktywnością, która często przesłania towarzyszące ryzyko bezpieczeństwa. Eksperci otwarcie mówią: „Internet jest wrogim środowiskiem, dlatego musisz ... [być w stanie] wytrzymać atak [s, aby przetrwać]", i jest często określany jako Wild Wild Web, WWW. W związku z tym kod, który będzie używany w sieci, musi zostać zaprojektowany z myślą o możliwości wrogich ataków, dokładnie w taki sam sposób, jak budynek musi być zaprojektowany i zbudowany tak, aby był odporny na trzęsienia ziemi. Kryterium tego, co stanowi dobry kod, zmieniło się teraz z minimalnego kodu na minimalnie

podatny na atak. Istnieje popularne greckie przysłowie, które mówi: „Lepiej jest spędzać czas na zabezpieczaniu osła na drzewie niż na poszukiwaniu zagubionego osła”. Dotyczy to bezpośrednio projektowania oprogramowania z dostępem do Internetu. Lepiej jest spędzać czas na projektowaniu bezpiecznego oprogramowania, niż stawiać czoła konsekwencjom włamań - kosztowny rozwój łatek, zła reklama itp. Innymi słowy, dzisiaj pojęcia jakości oprogramowania i bezpieczeństwa oprogramowania są ze sobą powiązane. Dlatego jeśli specyfikacja oprogramowania wymaga ochrony, musi istnieć odpowiedni mechanizm bezpieczeństwa. Coraz częściej obserwuje się, że aplikacje internetowe mają własne zapory ogniowe zamiast polegać wyłącznie na systemach hostingu. Koszt usunięcia podatności jest zwykle bardzo wysoki, jeśli weźmie się pod uwagę powstające szkody niematerialne. Podczas naprawy zasoby będą musiały zostać odebrane innym zadaniom, aby zająć się tą sprawą w bardzo pilny sposób. Pod względem pieniężnym koszt usunięcia luki w zabezpieczeniach wynosi od pięciu do siedmiu cyfr w dolarach, w zależności od głębokości projektu tej luki. Procedura niezbędna do usunięcia luki zazwyczaj wykonuje następujące kroki:

1. Lokalizacja źródła luki

2. Zaprojektowanie łatki, która wzmocni kod i wyeliminuje luki

3. Zastosowanie i testowanie łatki

4. Potwierdzenie, że nie ma żadnych skutków ubocznych

5. Opracowanie dokumentacji łaty

6. Przygotowanie planu dystrybucji łatek do wszystkich klientów, których dotyczy problem

7. Instalacja poprawki

8. Potwierdzenie skuteczności łatki; kampania public relations w celu zrównoważenia wcześniejszej negatywnej reklamy

O ile źródło luki nie zostanie jednoznacznie zidentyfikowane, każda łatka może obejmować problem bez eliminacji źródła luki.

Najczęstsze luki w zabezpieczeniach spowodowane niepewnym kodem to

• Przepełnienie bufora. Działania w programie, zwłaszcza dane wejściowe, przydzielają pewną ilość skończonej przestrzeni na nowe, utworzone dane do przechowywania. Nadmierna ilość danych zapełnia bufor, a program ulegnie awarii, chyba że program zastosuje środki zapobiegawcze.

• Przepełnienie arytmetyczne. Zwykle ma to miejsce, gdy następuje akumulacja i przekroczona zostaje maksymalna liczba akumulatorów. Następna dodawana ilość przewraca się nad akumulatorem, tworząc fałszywy wynik, chyba że ponownie zostaną zastosowane środki zapobiegawcze.

• Atak sformatowanym łańcuchem. Niepewny kod pozwala, aby dane dostarczone przez użytkownika były traktowane jako polecenie, gdy mogą to być tylko dane. Jeśli jest to dozwolone, osoby atakujące mogą zainstalować własny kod wykonywalny.

• Wstrzyknięcie polecenia. Brak weryfikacji danych wejściowych pozwoli na przyjęcie i wykonanie niedozwolonych poleceń.

• Cross-site scripting (XSS). Jest to wstrzyknięcie złośliwego kodu do oprogramowania klienckiego, zwykle w celu ominięcia kontroli dostępu,

• Zastrzyki SQL. To jest kod SQL, który wprowadza w błąd aplikację do wykonania.

• Niezabezpieczone bezpośrednie odniesienie do obiektu. Dotyczy to wyszukiwania stron internetowych. Zamiast nazwy pliku HTML odwołuje się do niego bezpośrednia definicja obiektu, którą strona ma w bazie danych. Ujawnia to tożsamość bazy danych, a osoba atakująca może użyć jej do pobrania innych plików.

• Niebezpieczne przechowywanie. Jest to przechowywanie krytycznych plików bez szyfrowania lub ochrony przed odczytem / zapisem. Do tej kategorii należą słabe przykłady steganografii.

• Słaba kryptografia. Jest to szyfrowanie plików, które można łatwo odczytać.

• Warunki wyścigu. Dzieje się tak, gdy przyznawany jest jeden zasób drugi użytkownik przed zakończeniem pierwszego.

Bezpieczeństwo oprogramowania musi pochodzić ze specyfikacji produktu. Nie jest to krok w rozwoju oprogramowania, ale jest to rozwiązanie, które należy przeplatać z funkcjonalnym projektem i pisaniem kodu. Oznacza to, że sposób myślenia projektanta oprogramowania musi mieć dwie równoległe ścieżki - funkcjonalność i bezpieczeństwo - przy czym bezpieczeństwo jest mechanizmem, który ujawnia, a następnie blokuje włamania. Taki mechanizm bezpieczeństwa powinien być solidny i dobrze zaprojektowany i nigdy nie powinien być zastępowany przez jakiś schemat zaciemnienia danych, który próbuje przechytrzyć atakującego.

Oprócz myślenia o potencjalnym napastniku, projektant musi również pomyśleć o wygodzie użytkownika i zapewnić mechanizm bezpieczeństwa, który nie przeszkadza w normalnych operacjach, będąc dla użytkownika jak najbardziej przejrzysty.

Błędy mogą być dobre

Bez względu na to, błędy są zawsze postrzegane negatywnie i są identyfikowane jako chwile niepowodzenia. To jest złe podejście. Kiedy Thomasowi Edisonowi powiedziano, że sto razy zawiódł przed udoskonaleniem lampy żarowej, odpowiedział, że skoro nauczył się czegoś nowego z każdego ze stu razy, proces jego sukcesu po prostu zrobił sto kroków. Oczywiście, popełnianie tego samego błędu raz po raz nie jest oznaką mądrości. Chodzi o to, aby nie obawiać się popełniania błędów, o ile popełniane są one w dobrej wierze, nie prowadzą do katastrof i, miejmy nadzieję, dodają trochę nowej wiedzy. Błędem byłoby rozszerzenie aplikacji lub użytkownika o więcej uprawnień bezpieczeństwa niż jest to konieczne do wykonania przypisanego zadania. Podczas instalowania aplikacji należy wymienić wszystkie potrzebne zasoby z wymaganymi uprawnieniami, takimi jak odczyt, zapis, tworzenie, usuwanie. W ten sposób, jeśli złośliwe oprogramowanie zainstaluje się w aplikacji, potencjalne szkody będą minimalne, a złośliwe oprogramowanie nie będzie mogło wędrować wewnątrz systemu. Podobnie, gdy komputer jest pojedynczym użytkownikiem, niekoniecznie powinien działać w trybie administratora, ale w trybie użytkownika. W ten sposób, jeśli złośliwe oprogramowanie przejdzie w trybie użytkownika, nie rozprzestrzeni się do obszarów uprzywilejowanych w trybie administratora. Dzięki posiadaniu uprzywilejowanych warstw - użytkownika, superużytkownika, administratora, superadministratora - złośliwe oprogramowanie jest w pewnym stopniu zawarte.

Klasyfikacja zagrożeń

Zasadniczo istnieją trzy rodzaje zagrożeń, mianowicie nielegalna zmiana danych, nielegalny dostęp do danych i nielegalna blokada dostępu do danych

Badacze bezpieczeństwa informacji w firmie Microsoft ogólnie klasyfikowali wszystkie zagrożenia w sześciu kategoriach, których akronim wygodnie składa się na słowo STRIDE (fałszowanie, modyfikowanie, odrzucanie, ujawnianie informacji, odmowa usługi, podniesienie uprawnień).

Proces modelowania zagrożeń

W systemach informatycznych zagrożenia - potencjalne ataki, które mogą wykorzystać luki w systemie - pochodzą z różnych źródeł i mają różny poziom grawitacji. Istnieje potrzeba ustrukturyzowanego podejścia do definiowania zagrożeń i radzenia sobie z nimi. Poniżej znajduje się sekwencja kroków, które mogą służyć jako mechanizm do tego celu.

1. Zdefiniuj, co stanowi przedmiotowy system informacyjny. To znaczy określ granice funkcjonalne i geograficzne tego, co nazywamy naszym systemem. Poza jakim punktem nie jest to nasza odpowiedzialność?

2. Teraz, gdy skwantyfikowaliśmy nasz system, próbujemy go zidentyfikować co uważamy za zagrożenia oparte na wewnętrznych lub zewnętrznych podatnościach. Wymienione wcześniej kategorie STRIDE mogą służyć jako punkt wyjścia do klasyfikacji zagrożeń.

3. Rozpoznaj, które z zagrożeń, w kontekście operacji, stanowią absolutne niebezpieczeństwo, które może prowadzić do katastrofalnego wpływu na system. Zdefiniuj tryby, w których takie zagrożenia mogą stać się skutecznymi atakami.

4. Opracuj opcje obrony dla każdego rozpoznanego zagrożenia i uszereguj rozważane mechanizmy obrony w oparciu o efektywność i zapotrzebowanie na zasoby.

5. Wybierz optymalne podejścia do eliminacji zagrożeń, skuteczności równoważenia, prawdopodobieństwa wystąpienia, ciężkości wystąpienia i kosztów opracowania rozwiązania.

Jest to iteracyjny proces wymagający udziału wszystkich, którzy są związani z bezpieczną wydajnością systemu, a mianowicie analityków, projektantów, programistów, użytkowników, trenerów, sprzedaży i oceniających. Proces ten należy poddawać przeglądowi w określonych odstępach czasu lub gdy pojawią się nowe zagrożenia.

Bezpieczeństwo zaczyna się w domu

Oczywiście dom to kreatywne fazy cyklu rozwoju oprogramowania (SDLC), zwłaszcza etapy projektowania i kodowania programów. SDLC jest często opisywane jako składające się z siedmiu podstawowych etapów przejściowych. Mianowicie,

1. Od abstrakcyjnych potrzeb do wymagań formalnych - analiza

2. Od wymagań formalnych po ogólny projekt - projektowanie

3. Od ogólnego projektu do kodu programu

4. Od wszystkich powyższych do opracowania dokumentacji

5. Od wszystkich powyższych do testowania systemu

6. Od testowania systemu do wykorzystania systemu (lub do poprzedniego kroku)

7. Od wykorzystania systemu do ulepszeń (krok 1)

W fazie analizy definiowane są wymagania bezpieczeństwa, w fazie projektowania rozwijane są mechanizmy bezpieczeństwa. Później podczas testów luki zostaną odkryte i wyeliminowane. Eliminacja podatności zwykle przyjmuje jedną z dwóch form. Jednym z nich jest usunięcie przyczyn luki, a drugim usunięcie skutków luki. W zależności od panujących uzasadnień zwykle wdrażane jest jedno z dwóch rozwiązań. Jest to obecnie standardowa praktyka i wymóg prawny na wszystkich głównych budowach, aby inżynierowie bezpieczeństwa nadzorowali wszystkie działania na rzecz bezpieczeństwa

pracowników. Podobnie podczas opracowywania systemów informatycznych specjaliści ds. Bezpieczeństwa oprogramowania muszą nadzorować proces rozwoju od a do z i wykonywać następujące czynności:

• Zidentyfikuj typowe błędy programowania, które prowadzą do podatności.

• Ustanowić standardowe praktyki bezpiecznego kodowania.

• Edukuj programistów (/ projektantów).

Ponadto mogą obejmować inicjatywy rozwoju oprogramowania wewnątrz organizacji

• Certyfikacja programistów w zakresie bezpiecznego kodowania

• Certyfikacja oprogramowania w zakresie bezpiecznego kodowania

• Wykorzystanie narzędzi do analizy oprogramowania

Narzędzia programowe są bardzo ważne w rozwoju bezpiecznych i dobrze udokumentowany kod i można go podzielić na następujące cztery kategorie:

• Pokrycie kodu - Śledzi kod i lokalizacje danych, które zostały utworzone, odczytane lub zmodyfikowane.

• Śledzenie instrukcji - rejestruje wyniki każdej instrukcji, udostępniając ją do późniejszej analizy krok po kroku.

• Analiza pamięci - śledzi wykorzystanie miejsca w pamięci, szukając możliwych naruszeń.

• Analiza wydajności - w oparciu o kryteria użytkownika oprogramowanie jest analizowane i dostrajane w celu optymalizacji wydajności.

W ten sposób aplikacje systemu informatycznego będą zarówno bezpieczne, jak i niezawodne. Software Engineering Institute na Carnegie Mellon University jest liderem w opracowywaniu standardów, narzędzi i szkoleń mających na celu projektowanie niezawodnych i bezpiecznych systemów informatycznych. Głównym problemem związanym z tworzeniem oprogramowania jest ekonomia cyklu życia i logistyka, w których bardzo często inwestycja przedpremierowa nie pokrywa się z przychodami po wydaniu. Często czas od wydania pomysłu do produktu jest minimalizowany, co często skutkuje wydaniem niezabezpieczonego oprogramowania. Na ratunek szybkiemu rozwojowi oprogramowania przybyły języki zorientowane obiektowo i ustrukturyzowane koncepcje programowania leżące u podstaw projektowania nowoczesnych systemów informatycznych. Jednak bezpieczne oprogramowanie od samego początku nadal stanowi nową zasadę głoszącą, że bezpieczeństwo musi stanowić integralną część funkcjonalności

Bezpieczeństwo w aplikacjach

Luki w zabezpieczeniach są również dostarczane z niezabezpieczonymi aplikacjami. Microsoft Word jest typowym przykładem. Jego wadą jest to, że po zażądaniu zapisu poprzednio usunięty tekst, choć już nie pojawia się w końcowym dokumencie, nadal pozostaje częścią pliku. Po otwarciu pliku Word w Notatniku usunięty tekst jest wyraźnie widoczny podczas przeglądania .

Dokument Word nie jest częścią końcowego widocznego tekstu. Ta luka narusza prywatność użytkownika i sugeruje poufność, nie oferując żadnej dodatkowej funkcjonalności. W takim przypadku jedynym rozwiązaniem jest wybranie wszystkich, skopiowanie i wklejenie w zupełnie nowym dokumencie pod koniec przygotowywania dokumentu. Jednak przeciętni użytkownicy nie

podejrzewają istnienia luk w zabezpieczeniach, szczególnie w przypadku produktów znanych marek, ani nie dysponują umiejętnościami technicznymi do wykrywania i usuwania wad projektowych oprogramowania. Obowiązkiem pracowników ds. bezpieczeństwa informacji w organizacji jest posiadanie wiedzy o istnieniu wad w oprogramowaniu, które zatwierdzają do użytku, oraz odpowiednie doradzanie użytkownikom. Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (US-DHS) utrzymuje obszerny zespół gotowości na wypadek awarii komputera (US-CERT), który ostrzega opinię publiczną o istnieniu luk w oprogramowaniu, które jest powszechnie używane i które prowadzi online bazę danych notatek o zagrożeniach. Luka w zabezpieczeniach.

Uwaga, na przykład VU # 446012, identyfikuje i opisuje „podatność na uszkodzenie pamięci wskaźnika Microsoft Word". Notatka wskazuje na własny biuletyn zabezpieczeń firmy Microsoft, który stwierdza: „Gdy użytkownik otworzy specjalnie spreparowany dokument Word za pomocą zniekształconego wskaźnika obiektu, może on uszkodzić pamięć systemową w taki sposób, że osoba atakująca może wykonać dowolny kod [złośliwego oprogramowania]". Notatka kontynuuje, że „Dokumenty Office mogą zawierać obiekty osadzone" (które mogą zawierać złośliwe oprogramowanie). Dlatego zaleca się, aby przed użyciem aplikacji odwiedzić tę bazę danych i dowiedzieć się o obecności interesujących luk w zabezpieczeniach. Sortując wyżej wspomnianą bazę danych według poziomu istotności, można rozpoznać, że na górze pojawiają się luki spowodowane przepełnieniem bufora. W związku z tym konieczne jest, aby bufory miały dynamiczny rozmiar, a także samooczyszczanie przestarzałych danych. Najczęstszą bramą przed atakami złośliwego oprogramowania jest przeglądarka internetowa. Z jednej strony musi być otwarty i wydajny, aby ułatwić wyświetlanie danych; z drugiej strony musi być skonfigurowany do ochrony komputera hosta. Eksperci ds. Bezpieczeństwa uważają, że „Wiele przeglądarek internetowych jest skonfigurowanych w celu zapewnienia zwiększonej funkcjonalności kosztem obniżenia bezpieczeństwo." Doskonały przewodnik po zabezpieczaniu przeglądarki internetowej jest dostępny online, z którego mogą korzystać zarówno nowicjusze, jak i eksperci.

Przedstawiamy środki zaradcze

Przeciwdziałanie cyberbezpieczeństwu to działanie, którego celem jest zablokowanie lub zminimalizowanie wpływu ataku cybernetycznego na nasz nasz zasób podłączony do sieci. Takim działaniem może być wykorzystanie określonego procesu, a określonego urządzenia, określonej technologii lub określonego systemu. Jako składnik aktywów uwzględniamy każdą naszą jednostkę podłączoną do Internetu, taką jak komputer, smartfon, urządzenie lub serwer. Podczas gdy podatności nie można całkowicie wyeliminować, można zastosować środki zaradcze, które zminimalizują znaczenie zagrożenia. Obrona przed zagrożeniami zewnętrznymi może przybierać różne formy, takie jak:

• Sprawdzanie adresów URL prób dostępu do systemu online pod kątem listy wstępnie zatwierdzonych.

• Minimalizowanie ryzyka włamania poprzez zmniejszenie uprawnień dostępu wszędzie tam, gdzie nie są absolutnie konieczne. Lub przedłuż je i wycofaj, gdy zajdzie taka potrzeba.

• Minimalizowanie dostępności wrażliwych danych w Internecie, zmniejszając w ten sposób narażenie na ewentualne włamanie.

• Posiadanie haseł odpornych na ataki „słownikowe" poprzez dołączanie liter języków obcych.

• Korzystanie z uwierzytelniania wieloskładnikowego, na przykład otrzymywanie dodatkowych danych parametry dostępu przez telefonię komórkową.

• Projektowanie pod kątem dużego natężenia ruchu, tak aby próby „zalania" portów nie powiodły się.

• Rozwijanie umiejętności rozpoznawania rozproszonego ataku typu „odmowa usługi”, DDoS, ataków za pomocą dynamicznych wskaźników, które stale obserwują wykorzystanie zasobów.

• Korzystanie z zapory ogniowej, oprogramowania antywirusowego oraz aktualizacja oprogramowania (aktualizacji i łatek) urządzeń podłączonych do Internetu.

• Rejestruj i zgłaszaj próby włamań i podejrzane żądania sieciowe.

• Odłącz lub dezaktywuj zasoby dostępne w Internecie, które nie są w tej chwili używane.

• Przeprowadzaj częste (codzienne lub cotygodniowe) audyty. Bądź świadomy rodzaju aplikacji znajdujących się w twoim systemie.

Międzynarodowa świadomość

Podobnie jak US-CERT, inne kraje zajmujące się bezpieczeństwem cyberprzestrzeni utworzyły podobne agencje rządowe w tym celu.

ĆWICZENIA

1. Otwórz program MS Word i utwórz plik zawierający tylko słowa „Dzień dobry”. Usuń wszystko i napisz „Dobranoc”. Zapisz plik pod nazwą Good.doc. Otwórz plik za pomocą Notatnika. Zobacz dolną część kodu. Zobaczysz usunięte słowa „Dzień dobry”. Jakie wyciągasz wnioski?

2. W dwustronicowym raporcie wyjaśnij podatność na przepełnienie bufora. Przywołaj pięć odniesień - komunikaty prasowe - w których zidentyfikowano to jako przyczynę odmowy usługi.

3. Zidentyfikuj preferowane działanie domowych systemów alarmowych i opracuj wymagania formalne (ilościowe).

4. Wybierz dwie przeglądarki internetowe i wykonaj badanie porównawcze ich funkcji bezpieczeństwa.

5. Zbadaj użycie terminów administrator i super administrator.

6. Zbadaj użycie terminów użytkownik i super użytkownik.

Luki w zabezpieczeniach organizacji

Cyberprzestrzeń to infrastruktura współczesnego świata, a cyberbezpieczeństwo to infrastruktura cyberprzestrzeni.

Wprowadzenie

Obecność w Internecie stała się warunkiem działania każdej organizacji, niezależnie od tego, czy jest to agencja rządowa, działalność gospodarcza czy instytucja akademicka. Każda organizacja potrzebuje otwartych drzwi dla społeczeństwa, z możliwością obsługi swojego okręgu wyborczego online i zdolnością do bezpiecznego przechowywania danych. Internet oferuje niespotykane możliwości praktycznie każdej organizacji. Jednak pojawiają się bezprecedensowe niebezpieczeństwa, które mogą prowadzić do kosztownych, często nieodwracalnych szkód. Rozważmy koszt włamania za jeden grosz. Historia mówi, że w pewnym banku system internetowy został przejęty, a jeden grosz został usunięty z konta. Zobaczmy, ile ten grosz będzie kosztował bank. Po odkryciu włamania dotyczącego konta zwołano nadzwyczajne spotkanie dwudziestu dyrektorów, które trwało cztery godziny. Podjęto decyzję o uzgodnieniu wszystkich 250 000 kont banku na podstawie danych z poprzedniego dnia. Działanie to wymagałoby dwóch pełnych dni od pięcioosobowego działu IT banku. Kampania public relations została autoryzowana przez kilka mediów, aby, miejmy nadzieję, zrównoważyć wszelką negatywną reklamę. Niewątpliwie koszt włamania za jeden grosz skończył się znacznie bardziej niż strata za jeden grosz. Operacje organizacyjne nie są już fizycznie wykonywane i monitorowane, ale są wykonywane elektronicznie za pośrednictwem współużytkowanych baz danych oraz intranetów, ekstranetów i Internetu. Oznacza to, że działamy w oparciu o postrzeganie rzeczywistości, a nie z samą rzeczywistością. Menedżer banku patrzy na ekran, aby zobaczyć sytuację finansową banku, i nie liczy rachunków ani monet znajdujących się w setkach lokalizacji banku. Podczas gdy wygoda, wydajność i skuteczność zapewniane przez systemy informacyjne mają niespotykaną dotąd skalę, podobnie są związane z tym zagrożenia. W związku z tym konieczne jest, aby środki bezpieczeństwa organizacji były dostosowane do stale rosnących zagrożeń. W przypadku naruszenia bezpieczeństwa w systemie informatycznym najważniejszym środkiem bezpieczeństwa jest wykrywanie w czasie rzeczywistym, powiadamianie i natychmiastowe przeciwdziałanie. Pewna biała księga stwierdza: „Firma… musi natychmiast wykryć ataki lub słabe punkty i zapewnić skuteczne rozwiązania". Dlatego wykrywanie incydentów jest podstawą każdego planu bezpieczeństwa - planu, który jest wspierany przez zaprojektowanie bezpiecznego systemu, który zapewnia analizę incydentów i procedurę naprawy podatności.

Typowe luki w zabezpieczeniach organizacyjnych

W definicji organizacyjnego systemu informacyjnego każde wymaganie funkcjonalne musi mieć towarzyszący komponent bezpieczeństwa, reagujący zarówno na ataki zewnętrzne, jak i wewnętrzne. Według statystyk najskuteczniejsze są cyberataki natury hybrydowej. Znawca podatności, znający lukę, pomaga osobie z zewnątrz skutecznie ominąć zabezpieczenia systemu i uzyskać do niej dostęp do zasobów organizacji. Przy projektowaniu i wdrażaniu systemu informatycznego, oprócz oczekiwanej nominalnej wydajności, należy dodać funkcje bezpieczeństwa, które zapobiegną tworzeniu luk w zabezpieczeniach. Większość luk w zabezpieczeniach wynika z jednego lub więcej z poniższych:

* Kopia zapasowa danych: Tworzenie kopii zapasowych danych w odstępach niezgodnych z szybkością działania systemu. Decyzja CIO, czy kopia zapasowa danych ma być wykonywana co godzinę, minutę, sekundę czy milisekundę. Częstotliwość przenoszenia danych z miękkiego magazynu kopii zapasowych na twardy nośnik archiwalny musi być starannie dobrana. Ponadto należy podjąć decyzję co do trwałości danych i ich zasad dostępu. Usunięcie niepotrzebnych danych może być bardzo ważne, ponieważ może podlegać przepisom dotyczącym zgodności. Zależność analiz po wprowadzeniu od

danych z kopii zapasowej jest absolutna, ponieważ ścieżka dostępu do zarchiwizowanych danych może dostarczyć cennych informacji.

* Operacyjne przepełnienie bufora: każdy element wprowadzania danych lub żądania wejścia są tymczasowo przechowywane w buforze podczas obsługi. Łatwe projektowanie oprogramowania wymaga bufora o stałym rozmiarze o szacowanym rozmiarze. Bez względu na rozmiar bufor może się zapełnić, powodując, że dana funkcja nie będzie działać lub będzie niedostępna. Securityminded design software wymaga dynamicznego bufora rozmiaru, który może bez końca rozszerzać się na ogromną dostępną pamięć dyskową. Atakujący przepełniają docelowe bufory, co zwykle powoduje nadpisanie danych lub kodu. Możliwe jest, że atakujący zainstalują złośliwe oprogramowanie, które naiwny bufor może przekazać kodowi wykonywalnemu o katastrofalnych skutkach.

* Nasycenie prędkości operacyjnej: niekończące się i trwałe żądania, choć proste, może przekraczać granice obliczeniowe systemu i praktycznie uniemożliwiać komunikację zewnętrzną z użytkownikami działającymi w dobrej wierze. Ponownie, zorientowane na bezpieczeństwo projektowanie oprogramowania wymaga przepisów, aby ignorować lub blokować trwałe żądania wspólnego pochodzenia.

Autoryzacja i uwierzytelnianie dostępu

Kody i procesy autoryzacji są często wrażliwe z różnych powodów. Najczęstsze to:

• System pozwala użytkownikowi na niekończące się próby wprowadzenia hasła. W takim przypadku atakujący automatyzuje atak, używając generatora haseł, który z czasem wykrywa prawidłowe hasło.

• System nie zezwala użytkownikowi na wiele prób wprowadzenia hasła, a użytkownik zapisuje hasło w miejscach potencjalnie wrażliwych.

• System wymaga zmiany hasła w częstych odstępach czasu, powodując niedogodności dla użytkownika, a użytkownik wprowadza minimalne zmiany, a każda zmiana dodaje luki.

Obecne technologie uwierzytelniania obejmują następujące cztery czynniki:

• Coś, co użytkownik wie (np. hasło, PIN)

• Coś, co użytkownik ma (np. karta bankomatowa, karta inteligentna, urządzenie USB)

• Coś, co użytkownik (np. cecha biometryczna, np. odcisk palca)

• Coś, co użytkownik otrzymuje, np. hasła jednorazowe (OTP) otrzymane przez telefonię komórkową (takie jak usługa krótkich wiadomości, SMS) lub przez Internet (np. e-mail lub inna osobiście dostępna aplikacja)

„Nazwy użytkowników i hasła nie zapewniają już odpowiedniego bezpieczeństwa”.

Udanym rozwiązaniem problemu z hasłem było użycie protokołu OTP, w którym serwer autoryzacji za pośrednictwem alternatywnego kanału wysyła do użytkownika kod OTP za każdym razem, gdy użytkownik potrzebuje dostępu do systemu. Takie hasła mogą być ważne przez krótki okres czasu, jeśli to możliwe alternatywne kanały to ;

• Telefonia komórkowa, w której serwer autoryzacji wysyła OTP na telefon komórkowy użytkownika za pomocą SMS-a, a nawet wypowiada się maszynowo

• Internet, w którym serwer autoryzacji wysyła OTP do użytkownika za pośrednictwem czatu, Skype, MSN lub e-maila

To rozwiązanie należy do kategorii tzw. uwierzytelniania dwuskładnikowego (TFA). TFA oznacza zastosowanie dwóch trybów zezwoleń , aby jak najlepiej uwierzytelnić użytkownika. Pierwszy czynnik jest umowny , taki jak nazwa użytkownika i hasło, a drugim czynnikiem jest tryb niekonwencjonalny, taki jak odpowiedź na określone pytanie lub parametr biometryczny lub parametr parabiometryczny „Dwuskładnikowe rozwiązanie uwierzytelniające wykorzystuje codzienne narzędzie - telefon [komórkowy] [który jest bardzo blisko osoby], aby zabezpieczyć [uwierzytelnianie] logowań i transakcji na kontach". Ten rodzaj uwierzytelnienia należy do kategorii parabiometrycznej. Udział telefonu komórkowego w procesie uwierzytelniania może być tak prosty, jak otrzymanie OTP lub nawet odebranie określonego hasła do uwierzytelnienia drukowania głosowego. Ponadto, nawet jeśli atakujący wprowadzi prawidłową nazwę użytkownika i hasło, autoryzowany użytkownik otrzyma natychmiastowe połączenie z informacją o dostępie. Jeśli dostęp jest próbą włamania, legalny użytkownik „może natychmiast zablokować konto i powiadomić dział oszustwa firmy, [który] może natychmiast podjąć odpowiednie działania". Procedury uwierzytelniania wieloskładnikowego (wielomodowego) są coraz częstsze i są stopniowo wdrażane w aplikacjach o wysokim poziomie bezpieczeństwa. OTP można połączyć z biometrią, gdzie odczyt odcisku palca i OTP są wysyłane do serwera w celu uzyskania dostępu do zasobów.

Czynniki ludzkie

Niesklasyfikowany raport rządu USA ujawnił, że „znaczna większość przeszłych naruszeń dotyczyła osób z zewnątrz, osób posiadających upoważnienie, które mogą ominąć fizyczną barierę bezpieczeństwa, a nie osób postronnych włamujących się do bezpiecznych obszarów". Personel, którego działalność obejmuje Internet lub inne sposoby przetwarzania danych, stanowi krytyczny zasób organizacyjny, który może przekształcić się w słaby link. Ich działalność może polegać na pisaniu kodu, programowaniu baz danych, korzystaniu z urządzenia pamięci USB lub po prostu wysyłaniu wiadomości e-mail. Każda taka czynność musi być wykonywana w określony sposób i zgodnie z polityką. „Sama technologia nie jest odpowiedzią". Ustanowienie, a także egzekwowanie zasad dotyczących wprowadzania, modyfikacji, odczytu lub usuwania danych organizacyjnych stanowi podstawę bezpieczeństwa danych w każdym przedsiębiorstwie. Równie ważna jest funkcja kontroli końcowej w systemie informatycznym, dzięki której zmiany danych można prześledzić według ich pochodzenia. Istnieje wiele sposobów powiadamiania właścicieli danych o dostępie do ich danych. W zależności od krytyczności danych można podjąć odpowiednie środki, od otrzymania wiadomości e-mail po otrzymanie wiadomości SMS na telefon komórkowy. Chociaż technologia może w rozsądny sposób chronić elektroniczne zasoby organizacji, nie może z taką samą łatwością chronić przed zagrożeniami z zewnątrz. Przytłaczające statystyki wskazują, że większość ataków na bazy danych ma charakter wewnętrzny lub zewnętrzny z pomocą wewnętrzną. Wyrażenie brzmi: nie możesz chronić się przed ochroniarzem, kucharzem lub lekarzem. Trudno jest ustalić bariery między danymi organizacyjnymi a tymi, którzy mają bona fide, muszą z nich korzystać. Organizacja nie może również traktować swoich członków jako potencjalnych przestępców. Konieczne są jednak mechanizmy bezpieczeństwa, aby żaden członek organizacji nie mógł samodzielnie spowodować poważnych szkód. Równie ważne jest to, że żaden członek organizacji nie może wpływać na dostęp do danych lub zmiany bez pozostawiania śladu. Studia przypadków i badania ankietowe wskazują, że istnieje podgrupa specjalistów w dziedzinie technologii informatycznych, którzy są szczególnie podatni na stres emocjonalny, rozczarowanie, niezadowolenie i wynikające z tego błędy w ocenie, co może prowadzić do zwiększonego ryzyka szkodliwych działań lub podatności na rekrutację lub manipulację. W ten sam sposób, w jaki poziom podatności jest przypisywany oprogramowaniu, procesom lub procedurom, powinien być również przypisywany personelowi obsługującemu krytyczne dane organizacyjne. Jest to bardzo delikatna kwestia, która, jeśli nie zostanie podana z najwyższym profesjonalizmem, może doprowadzić do powstania wyobcowania w organizacji. Dyrektor ds. Informatyki wraz z szefem działu

HR są odpowiedzialni za ocenę obecności i poziomu potencjalnej podatności na zagrożenia u każdego członka organizacji, który obsługuje krytyczne dane. W związku z tym wszyscy członkowie organizacji muszą przejść specjalne szkolenie i wytyczne dotyczące bezpieczeństwa. W przypadku sektora federalnego National Institute for Standards and Technology (NIST) dostarcza wyraźny dokument. Wytyczne są przeznaczone dla agencji rządowych, ale w równym stopniu dotyczą sektora cywilnego, kładąc nacisk na świadomość potencjalnych negatywnych konsekwencji w przypadku kompromisu w zakresie bezpieczeństwa informacji.

Służby Bezpieczeństwa

Usługi bezpieczeństwa mogą być świadczone przez wewnętrzne talenty, zewnętrzne organizacje zajmujące się bezpieczeństwem danych lub ich połączenie. Tak czy inaczej, wewnętrzny dyrektor ds. Bezpieczeństwa informacji (CISO lub CSO) jest ostatecznie odpowiedzialną osobą i najwyższym organem w zakresie definiowania, projektowania i wdrażania systemu informacyjnego, a także w późniejszych operacjach i zarządzaniu bezpieczeństwem. Znaczne korzyści można uzyskać dzięki wykorzystaniu zewnętrznych organizacji bezpieczeństwa posiadających doświadczenie i wiedzę, które przewyższają talent wewnętrzny. Zasadniczo podatność organizacyjna wzrośnie jednak, gdy zewnętrzni konsultanci ds. Bezpieczeństwa wejdą do organizacji.

Technologie zewnętrzne

Koncepcja architektury informacji przedsiębiorstwa często wykracza poza dane, bazy danych, intranet i cyberprzestrzeń i obejmuje zewnętrzne technologie i zasoby. Jednym z takich przypadków jest wykorzystanie globalnego systemu pozycjonowania (GPS) oferowanego i obsługiwanego przez Departament Obrony USA. GPS, dwadzieścia cztery systemy satelitarne, zapewnia informacje o lokalizacji w postaci długości i szerokości geograficznej, wysokości, kierunku i czasu. Rysunek pokazuje GPS i jego dwadzieścia cztery konstelacje satelitarne.

Technologia ta znajduje zastosowanie w wielu branżach, „takich jak usługi reagowania kryzysowego, egzekwowanie prawa, ochrona ładunków, transport materiałów jądrowych, nawigacja lotnicza oraz standardy czasu krytycznego i synchronizacji dla mediów, telekomunikacji i sieci komputerowych ”. Chociaż system jest bardzo dokładny, niezawodny i wolny od luk w zabezpieczeniach, „sygnały GPS nie są bezpieczne”. Odbiór radiowy dostarczonych danych może być zakłócany przez atakujących, a co gorsza, może zostać sfałszowany, sfabrykowany w celu wprowadzenia użytkownika w błąd. Dlatego błędne dane wprowadzą użytkownika w błąd co do dokładnej lokalizacji śledzonego zasobu. Na szczęście istnieją pewne środki zaradcze, które chociaż nie przywracają prawidłowych sygnałów, wskazują na błąd. W przypadku zakłócania sygnału odbiornik GPS odbiera stosunkowo silny sygnał radiowy, ale nie wytwarza danych, co prowadzi do wniosku, że sygnał jest zakłócany. Jeśli chodzi o fałszowanie, dane potwierdzone przez odebrane sygnały można potwierdzić konwencjonalnymi

środkami, na przykład weryfikując kierunek podróży za pomocą kompasu lub porównując otrzymany czas za pomocą zegara. Również sfałszowany sygnał będzie silniejszy niż oczekiwany, „1×10^{-16} watów"]. Dlatego, chociaż sygnały GPS pochodzą z bardzo wiarygodnego źródła, świadomość możliwego włamania powinna być uwzględniona w równaniu bezpieczeństwa danych organizacji.

Luki w zabezpieczeniach sieci

Sieci są najbardziej wrażliwym i krytycznym elementem w każdej organizacji i właśnie tam musimy skutecznie zapobiegać, wykrywać i reagować na zdarzenia związane z bezpieczeństwem. Cyberobrona sieci wymaga skoordynowanego zaangażowania kompleksowego portfolio narzędzi bezpieczeństwa, które dobrze ze sobą współpracują w sposób inteligentny i zautomatyzowany sposób. Nie tak dawno temu wszystkie dane organizacji, mimo że były połączone w sieć, znajdowały się w fizycznych granicach organizacji. Obecnie dostępność opłacalnego zewnętrznego przechowywania danych za pośrednictwem dostawców usługi Storage-as-a-Service (SaaS), zwanej powszechnie chmurą, stworzyła nowe luki w zabezpieczeniach. Takie opcje przechowywania danych to najlepsze z nieznanych środków bezpieczeństwa. Oznacza to, że wszelkie dane przechowywane przez organizację, przynajmniej poza jej absolutnym nadzorem, muszą być niezawodnie szyfrowane. Trendem zewnętrznego wsparcia IT, który osiągnął już poziom dostępności, jest infrastruktura jako usługa (IaaS). Oznacza to, że organizacja potrzebuje tylko komputerów z przeglądarkami internetowymi i dostępem do sieci. Niewątpliwie IaaS może zapewnić ogromne korzyści ekonomiczne organizacji, ale poziom podatności na zagrożenia jest nieznany. Sieci są głównym punktem wejścia dla cyberprzestępców, dlatego w punktach cyberprzestrzeni organizacji należy zastosować maksymalną ochronę. Praktyka polegała na stosowaniu narzędzi i technik w celu zatrzymania takich prób włamań. Takie próby muszą zostać rozpoznane i zablokowane. W tym celu dostępne są narzędzia komercyjne, określane jako Network Intrusion Prevention Systems (NIPS lub IPS), zwykle instalowane w punkcie wejścia do organizacji. NIPS służy jako cyber-policjant przy wjeździe i wyjeździe, badający każdy pakiet danych wchodzących lub wychodzących z sieci organizacji i decyduje, na podstawie zasad, czy zablokować, czy pozwolić na przejście do pakietów. Oprogramowanie IPS może odgrywać aktywną rolę, jak opisano powyżej, lub rolę pasywną, rejestrując jedynie aktywność punktu wejścia-wyjścia i opracowując statystyki, które mogą być analizowane i mogą tworzyć inteligencję.

Sieci bezprzewodowe

Sieć organizacyjna i związane z nią zasoby są również zagrożone przez luki w wewnętrznej lub zewnętrznej komunikacji bezprzewodowej. Chociaż trzy znormalizowane technologie bezprzewodowe - Bluetooth, Wi-Fi i WiMAX - mają funkcje bezpiecznej komunikacji, istnieją luki w zabezpieczeniach, które muszą być znane i odpowiednio usuwane przez użytkowników. Dzięki temu, że są bezprzewodowe i działają w zakresie częstotliwości radiowych (RF), takie sieci są narażone na niektóre zagrożenia, przed którymi trudno się obronić. To są:

• Podsłuchiwanie. Dostępność analizatorów ruchu umożliwia bardzo łatwe odbieranie i przechwytywanie wymienianych danych. Następnie dane, mimo że są zaszyfrowane, mogą być gromadzone i ewentualnie odszyfrowane w późniejszym czasie.

• Wstrzykiwanie szumu. Jest to przerywany zastrzyk impulsów szumowych RF mających na celu uszkodzenie normalnej komunikacji.

• Zagłuszanie. Potężne źródło RF nadające w pobliżu jednostek organizacji i w spektrum operacji może obezwładnić sieć. Oczywiście lokalizację źródła można łatwo zidentyfikować, chyba że źródło jest mobilne.

• man-in-the-middle. Jest to przypadek, w którym przeciwnik o podobnej łączności bezprzewodowej udaje legalną stację bazową, stację mobilną lub stację abonencką.

Najczęściej używane standardowe sieci bezprzewodowe to Bluetooth (BT), Wireless Fidelity (Wi-Fi) oraz Worldwide Interoperability Microwave Access (WiMAX).

Bluetooth

Bluetooth (BT) to nazwa handlowa transmisji danych, protokołu certyfikowanego przez IEEE (Institute of Electrical and Electronics) znany jako IEEE 802.15.1–1 Mb / s

Protokół WPAN (Wireless Personal Area Network)

Protokół którego celem jest zapewnienie „standardów łączności bezprzewodowej o niskim stopniu złożoności i niskim zużyciu energii". Pomimo obszernych środków bezpieczeństwa, które zostały wprowadzone w specyfikacjach BT, wydaje się, że konstrukcja systemu operacyjnego BT nieumyślnie pozostawiła kilka luk w zabezpieczeniach. Jednak fakt, że większość kodu BT znajduje się w oprogramowaniu wewnętrznym, sprawia, że technologia bezprzewodowa BT jest odporna na „złośliwy kod". Rysunek ilustruje BT WPAN, który służy jako zamiennik kabla o zasięgu do 30 stóp, 10 metrów.

Aby być narażonym na ryzyko włamania, urządzenie mobilne lub komputer osobisty wyposażone w BT musi mieć włączoną funkcję BT. Oznacza to, że urządzenie musi znajdować się w trybie wykrywalnym. Ponadto we wszystkich komunikatach BT - działających w dobrej wierze lub złośliwych - ofiary i atakujący urządzenia - muszą znajdować się w odległości 10 metrów od siebie, aby komunikacja mogła się odbyć. Jednak dostępność bardzo wrażliwych odbiorników umożliwia podsłuch BT z znacznie większych odległości. Luki w zabezpieczeniach urządzeń wyposażonych w BT można uznać za pasywne lub aktywne. W pasywnych intruzi szpiegują lub stwarzają niedogodności, podczas gdy w aktywnych intruzi powodują straty w bazach danych urządzeń ofiary.

Luki w zabezpieczeniach pasywnych

Obecność docelowego urządzenia można rozpoznać po pingowaniu. Powtarzające się pingowanie może renderować funkcje BT ofiary ,że urządzenie nie działa. Podczas gdy urządzenie wyposażone w BT komunikuje się, intruz może określić adres urządzenia i użyć go do komunikacji z nim, uniemożliwiając w ten sposób prawidłowe komunikowanie się z innymi urządzeniami. Ulepszenia specyfikacji BT ostatecznie wyeliminowałyby penetrację urządzeń w trybie nieodkrytym.

Bezprzewodowa technologia BT działa w nielicencjonowanym paśmie, gdzie wiele innych aplikacji uważa za równie wygodne w obsłudze. Dostępna jest technologia bezprzewodowej sieci LAN Wi-Fi, wykorzystująca to samo pasmo, podobnie jak kuchenki mikrofalowe i wiele telefonów bezprzewodowych. w związku z tym urządzenia wyposażone w BT znajdujące się w obszarze promieniowania jednego z takich produktów mogą być niezamierzone

Aktywne podatności

Za pośrednictwem komunikacji BT intruz może przejąć pełną kontrolę nad poleceniami urządzenia-ofiary - mianowicie Poleceniami AT, które sterują telefonem komórkowym - w żaden sposób nie przyciągając uwagi właściciela urządzenia-ofiary. W tej luce intruz może korzystać z urządzenia ofiary tak, jakby znajdowało się w zasięgu ręki. Dane mogą być zmieniane, połączenia i wiadomości mogą być wysyłane i odbierane, dostęp do Internetu, a nawet rozmowy mogą być słuchane przez telefon intruza Dzięki specjalnemu oprogramowaniu intruz może nie tylko uzyskać dostęp do wszystkich danych w urządzeniu ofiary, ale także może nawet odczytać unikalną identyfikację sprzętową telefonu, tzw. International Mobile Equipment Identity (IMEI)

Środki ostrożności

W specyfikacjach protokołu BT osadzono różne mechanizmy bezpieczeństwa. Jednak oprócz ustanowienia zasad bezpieczeństwa , przedsiębiorstwa mogą również wdrażać oprogramowanie BT, które skanuje środowisko i monitoruje pasmo BT

• Zidentyfikuj różne typy aktywnych urządzeń BT

• Podaj wszystkie możliwe do odzyskania atrybuty zidentyfikowanych urządzeń (klasa, nazwa i producent)

• Podaj informacje o połączeniu (parowanie)

• Zidentyfikuj dostępne usługi (faks, drukarka)

Poziom ryzyka związanego z użyciem technologii bezprzewodowej BT jest bezpośrednio związany bardziej z konkretną aplikacją, a mniej z nieodłączną architekturą BT. Biorąc pod uwagę liczne ograniczenia, na podstawie których działa technologia BT - niska moc RF, odległość, szerokość pasma - żadna wysoce wrażliwa lub krytyczna aplikacja nie zwróci się do BT o wsparcie. W zakresie tego, co oferuje, a mianowicie wymiany kabli i tak długo, jak przestrzegane są podstawowe środki ostrożności, bezprzewodowa technologia BT będzie tak bezpieczna, jak powinna być, a mianowicie w przypadku aplikacji wewnątrz biura o minimalnym bezpieczeństwie.

Wireless Fidelity

Wireless Fidelity (Wi-Fi) to nazwa handlowa protokołu transmisji danych certyfikowanego przez IEEE, technicznie zwanego IEEE 802.11 — Multi-Rate DSSS. Wi-Fi to bezprzewodowy odpowiednik przewodowego protokołu Ethernet IEEE 802.3

Główni programiści i firmy OEM utworzyły Wireless Ethernet Compatibility Alliance (WECA), aby wspierać certyfikację sprzętu Wi-Fi. WECA została założona przez branżową sieć gigantów i mikroprocesorów, w tym 3Com, Cisco, Sony, Intel, Motorola, Nokia i Toshiba, i obecnie działa jako izba rozliczeniowa urządzeń Wi-Fi z obecnym członkostwem ponad 250 producentów . Protokół 802.11 zapewnia uniwersalny standard infrastruktury bezprzewodowej sieci LAN (WLAN), dzięki któremu zagwarantowana jest interoperacyjność między „certyfikowanymi produktami Wi-Fi". Przed ustanowieniem standardu WLAN i przez dziesięciolecia aplikacje WLAN ulegały stagnacji, ponieważ

każdy z głównych producentów telekomunikacyjnych miał własne projekty. Wraz z ustanowieniem standardu Wi-Fi sieci WLAN stały się standardowym urządzeniem intranetowym. Funkcje zabezpieczeń Wi-Fi zostały pierwotnie ustanowione przez WEP, a następnie WPA i są obecnie zdefiniowane przez WPA2, a ochrona dostępu nowej generacji objęta jest standardem 802.11w. Istnieją obecnie trzy wersje standardu Wi-Fi, a mianowicie 802.11a, 802.11b i 802.11g. Wersje „a" i „g" oferują szybkość przesyłania danych 54 Mb / s, wykorzystując odpowiednio pasmo 5 GHz i 2,4 GHz. Wersja „b", najstarszy standard, ma przepływność 11 Mb / s pracującą w paśmie 2,4 GHz. nie posiadając licencji, pasmo 5,0 GHz jest bardzo zajęte. Jednak zastosowanie standardu 802.11h, który obsługuje dynamiczny wybór częstotliwości i kontrolę mocy transmisji, zapewnia „współistnienie Wi-Fi z innymi typami urządzeń częstotliwości radiowych", takich jak BT. Następna wersja Wi-Fi to 802.11n. Standard „n" nie tylko czterokrotnie zwiększa przepływ danych, osiągając zakres 200–600 Mb / s, ale jest również wstecznie kompatybilny ze starszymi wersjami „a", „b" i „g". Wersja „n" korzysta z dostępności wystarczającej przepustowości, a „dzięki wielu antenom [i] bardziej inteligentnemu kodowaniu ... [dąży] do uzyskania surowych prędkości transmisji danych do 600 Mb / s". W bezprzewodowym systemie Wi-Fi, z wyjątkiem oprogramowania, istnieją dwa fizyczne komponenty: punkt dostępowy (AP) i moduł interfejsu bezprzewodowego, który jest kartą wkładaną, układem wbudowanym lub urządzeniem USB. Centralnym elementem systemu jest punkt dostępowy, który łączy świat „bezprzewodowy" z przewodowym, zwanym infrastrukturą. Zatem AP z jednej strony komunikuje się z siecią organizacji, tzw. Infrastrukturą, a z drugiej strony komunikuje się z klientami bezprzewodowymi i służy jako router spełniający potrzeby sieciowe stacji bezprzewodowych. AP zapewnia wspólny dostęp do sieci LAN / Internet za pomocą translacji adresów sieciowych (NAT). W niechronionym środowisku Wi-Fi strażnik (WD) może wykorzystać przepustowość ofiary, aby uzyskać dostęp do wszystkiego, co jest dostępne. WD może co najmniej uzyskać dostęp do Internetu lub intranetu ofiary, a maksymalnie WD może uzyskać dostęp do wszystkich plików na komputerze ofiary i przeniknąć do dowolnego innego miejsca, które jest dostępne dla komputera ofiary. Innymi słowy, w niezabezpieczonym środowisku Wi-Fi, WD może przejąć pełną kontrolę nad komputerem ofiary. Warto wspomnieć, że każda wizyta WD w Internecie będzie oznaczać tożsamość routera ofiary, co może sugerować, że ofiara nie jest łatwym dowodem na przejęcie Wi-Fi. W mediach pojawiło się wiele przypadków porwania Wi-Fi, które są zbyt smutne, by o nich wspominać. Poniżej znajduje się lista środków ostrożności, których należy przestrzegać podczas korzystania z Wi-Fi w środowisku domowym.

* Jeden: Wyłącz tryb IBSS. W tym trybie jednostka mobilna jest otwarta na komunikację bez żadnych ograniczeń. Hakerzy mogą łączyć i dyskretnie uzyskiwać dostęp do poufnych informacji. Takie ryzyko można wyeliminować, jeśli IBSS zostanie wyłączony. Wyłącz także połączenie Wi-Fi, gdy tylko nie będzie już potrzebne.

* Dwa: Wyłącz tryb infrastruktury. Tryb infrastruktury umożliwia klientom Wi-Fi dostęp do zasobów po drugiej stronie punktu dostępu (drukarki, serwery itp.).

* Trzy: Wyłącz nadawanie SSID. Ponieważ w środowisku domowym nie przewiduje się nieoczekiwanych urządzeń Wi-Fi, punkt dostępu nie musi transmitować swojej tożsamości SSID na cały świat. Zwykle ten identyfikator jest wprowadzany ręcznie i tylko raz podczas logowania do laptopa, a następnie zapamiętywany

* Cztery: Zmień dostęp routera. Router, znajdujący się w punkcie dostępowym, jest dostępny poprzez nazwę i hasło. Są one ustawiane przy pierwszej instalacji, ale można je ponownie skonfigurować w dowolnym momencie. Te dwa parametry należy zmieniać w odstępach czasu. Ponadto domyślny fikcyjny lokalny, intranetowy adres IP, który mógł mieć postać 192.168.1.1, można zmienić na dowolny inny, o ile liczby w czterech polach mieszczą się w zakresie od 0 do 224, bez zer wiodących. Ponadto „nie ma potrzeby zachowania domyślnej nazwy routera". Przeciwnie, każda zmiana w stosunku do

wartości domyślnych przyczyni się do poprawy bezpieczeństwa. Zazwyczaj wartości domyślne są takie same dla wszystkich punktów dostępu danego producenta i są zwykle znane intruzom.

* Pięć: Włącz szyfrowanie. Specyfikacja Wi-Fi obejmuje tak zwaną ochronę przewodową (WEP). Algorytm szyfrowania występuje w 40 i 64 bitach. Późniejsza wersja, WPA2, ma 128 bitów. Za każdym razem, gdy jednostka mobilna loguje się do punktu dostępowego Wi-Fi, nazwa użytkownika i hasło mogą być łatwo przechwycone przez „sniffera". Jednym ze sposobów, aby temu zapobiec, jest użycie PKI, gdzie każda strona zna klucz publiczny drugiej strony i „klucz dostępu" można ustanowić w ramach szyfrowania bez ujawniania żadnych niezaszyfrowanych informacji. Najnowsza wersja protokołu bezpieczeństwa Wi-Fi, WPA2, zapewnia PKI. Należy zauważyć, że szyfrowanie rozpuszcza się, gdy dane dotrą do miejsca docelowego. Oznacza to, że WPA2 służy wyłącznie do transportu powietrznego. Ponadto „podstawowy algorytm [szyfrowania] jest wadliwy i podlega stosunkowo łatwemu łamaniu." Istnieją nawet strony internetowe, które zapewniają kroki do złamania WEP.

* Sześć: Włącz filtrowanie adresów MAC. Zwykle punkty dostępu Wi-Fi zawierają bramę z funkcją filtrowania Media Access Control (MAC). Można zezwolić filtrowi na przekazywanie ruchu tylko z urządzeń o znanych adresach MAC. Urządzenia te mogą znajdować się w infrastrukturze (tzn. Po przewodowej stronie punktu dostępu), mogą być drukarkami lub innymi komputerami lub mogą znajdować się w przestrzeni bezprzewodowej - na karcie Wi-Fi laptopa, Wi- Fi PDA i tym podobne. W sieci bezprzewodowej znany jest identyfikator SSID, a następnie „bez filtrowania adresu MAC, każdy klient bezprzewodowy może dołączyć ". Nie powstrzyma to jednak zaawansowanego hakera, który wie, jak przechwytywać pakiety i wyciągać z nich adresy SSID i MAC.

* Soedem: Zbadaj fale radiowe. Korzystając ze specjalistycznego oprogramowania, takiego jak darmowy sniffer pakietów Ethereal, trzeba często szukać fal radiowych w poszukiwaniu nieoczekiwanych punktów dostępu Wi-Fi lub klientów Wi-Fi. Takie narzędzia, jak Ethereal, mogą przechwytywać dane „bezpośrednio z połączeń sieciowych na żywo ... mogą odczytywać przechwycone pliki ... rozpakowywać je w locie… [i mogą obecnie analizować] ... 759 protokołów"

Środki ostrożności dotyczące Wi-Fi w hotspocie

Dla wygody klientów publiczne hotspoty nie używają żadnej z możliwych funkcji bezpieczeństwa Wi-Fi (szyfrowanie WEP lub WPA) lub sieci (filtrowanie MAC). Aby ułatwić połączenia klientów, punkty dostępu Wi-Fi faktycznie nadają swój identyfikator SSID. W hotspocie klienci zaczynają od włączenia opcji Wi-Fi, połączenia z punktem dostępu, przesłania prawidłowego numeru karty kredytowej i połączenie zostaje nawiązane. Aby jednostka mobilna mogła komunikować się z punktem dostępowym, znajomość identyfikatora SSID punktu dostępu jest konieczny. Aby włamać się do klienta Wi-Fi, jednostka mobilna nie musi komunikować się z żadnym punktem dostępu. Sam fakt włączenia funkcji Wi-Fi jest wystarczający do ustalenia podatności. Klienci Wi-Fi w publicznych lub korporacyjnych hotspotach muszą podjąć szereg środków ostrożności, aby zmaksymalizować ochronę swoich poufnych informacji przed intruzami. Poniżej znajduje się kilka środków ostrożności, które należy podjąć podczas pobytu w hotspocie.

* Jeden: Hotspot Legitimacy. Hakerzy często tworzą fałszywy punkt dostępu w pobliżu legalnego publicznego punktu dostępu i próbują zwabić osoby poszukujące połączenia. Dzięki takim połączeniom hakerzy przechwytują poufne informacje (nazwy użytkowników, hasła, numery kart kredytowych itp.), Dokonując później nielegalnego wykorzystania. Klienci Wi-Fi muszą absolutnie upewnić się, że hotspot, z którym próbują się połączyć, jest uzasadniony. Zazwyczaj w obiekcie powiązanym z usługą hotspot (poczekalnie, kawiarnie itp.) umieszczane są odpowiednie znaki. Istnieje kilka stron internetowych, które wymieniają znane legalne hotspoty na całym świecie.

* Dwa: szyfrowanie plików. Pliki, w tym wiadomości e-mail, powinny zostać zaszyfrowane przed przesłaniem. Istnieje wiele opcji szyfrowania przy użyciu dedykowanego oprogramowania lub funkcji wbudowanych w aplikacje, takie jak edytory tekstu i klienci poczty e-mail. Można zainstalować aplikację szyfrującą, która „automatycznie szyfruje cały ... przychodzący i wychodzący ruch internetowy".

* Trzy: udostępnianie plików. Będąc w punkcie aktywnym, wyłącz opcję udostępniania plików, aby zapobiec niepożądanemu transferowi plików.

* Cztery: Włącz VPN . W ten sposób przechwycone dane są renderowane i bezużyteczne z powodu szyfrowania.

* Pięć: użycie zapory. Hotspot najprawdopodobniej używa jednego statycznego adresu IP do obsługi 200 klientów. Oznacza to, że wszyscy klienci znajdują się w tej samej podsieci, co ułatwia intruzowi-klientowi węszenie na innych klientach. Problem ten można zminimalizować za pomocą „osobistej zapory ogniowej". Można kupić zaporę ogniową lub skorzystać z zapory dostarczonej przez system Windows. Za pośrednictwem zapory można ograniczyć ruch i zablokować lub zezwolić na „komunikację, która może… być niebezpieczna".

* Sześć: praktyczne zasady. Niezależnie od tego, czy ktoś ma dostęp do zewnętrznego świata przewodowo lub bezprzewodowo, obowiązują również pewne dodatkowe środki ostrożności: korzystanie z najnowszego oprogramowania antywirusowego, korzystanie z najnowszej wersji systemu operacyjnego, korzystanie z bezpiecznej poczty e-mail opartej na Internecie (https), indywidualna ochrona hasłem dla poufnych pliki, a także mechanizm haseł komputerowych, który blokuje komputer, jeśli przez X minut nie ma aktywności klawiatury ani myszy

Środki ostrożności dotyczące Wi-Fi w przedsiębiorstwie

Korporacyjne zabezpieczenia Wi-Fi wymagają znacznie poważniejszego wyeliminowania luk w Wi-Fi. W takich przypadkach zaawansowane protokoły i sieci VPN są w porządku. W środowisku korporacyjnym bezpieczeństwo Wi-Fi i środki ostrożności mogą obejmować wszystkie wyżej opisane, a także te poniżej.

* Jeden: ogrodzenie obwodowe. Obecnie dostępne są rozwiązania, w których pozycjonowanie czujników RF może geometrycznie określić, czy klient znajduje się w autoryzowanym obszarze fizycznym. Takie technologie, które wymagają szkolenia w terenie i dokładnego dostrojenia, zapewniają 100% bezpieczeństwa podczas testów. Za pomocą ogrodzenia obwodowego „Środowiska Wi-Fi można chronić w przestrzeni powietrznej 3D [z dokładnością] ... około 5 stóp".

* Dwa: zaawansowane uwierzytelnianie. Zamiast polegać na nominalnych funkcjach bezpieczeństwa Wi-Fi, przedsiębiorstwo może korzystać z zaawansowanych protokołów autoryzacji / uwierzytelniania, takich jak DIAMETER.

Wi-Fi stało się obecnie podstawową technologią w lokalnej komunikacji bezprzewodowej. Jego główne luki w zabezpieczeniach - przechwytywanie sesji, man-in-the-middle i denial-of-service - są stale ograniczane poprzez postępy w technologiach bezpieczeństwa i zwiększoną świadomość bezpieczeństwa po stronie użytkowników. Wraz ze wzrostem efektywnej prędkości transmisji danych przekraczającej 200 Mb / s, będzie dużo przepustowości dla zaawansowanych technik szyfrowania i zaawansowanych protokołów autoryzacji / uwierzytelniania. Oczekuje się, że standard bezpieczeństwa 802.11w, z kluczem szyfrowania dla pakietu i dodatkowymi zaawansowanymi funkcjami, znacznie zwiększy bezpieczeństwo Wi-Fi i zmniejszy liczbę udanych ataków intruzów

Dostęp do mikrofali na całym świecie

Ogólnoświatowy interoperacyjny dostęp mikrofalowy (WiMAX) to IEEE Wireless Networking Standard 802.16, który został wydany w 2004 roku. Jego specyfikacje są stale ulepszane, wprowadzając poprawki mające na celu uczynienie z niego realnej bezprzewodowej wymiany technologii kablowej, ADSL i T1 . WiMAX działający jako stacjonarna lub mobilna sieć LAN lub Metropolitan Area Networks (MAN) wykorzystuje licencjonowane i nielicencjonowane pasma częstotliwości odpowiednio dla transmisji o wysokiej i niskiej mocy, aby zapewnić Broadband Wireless Access (BWA).

Funkcje WiMAX

Nielicencjonowane pasma w widmie 2–10 GHz ograniczają zasięg do zasięgu Wi-Fi, który wynosi około 10 do 50 metrów, a moc nadawania jest zwykle ograniczona do 200 mW. Licencjonowane pasma w zakresie widzenia w linii 10–66 GHz, w których transmitowana moc może osiągnąć 20 watów, mogą oferować zasięg w promieniu 50 km od pojedynczej stacji bazowej. Ponadto standardowa szybkość transmisji danych WiMAX wynosi 70 Mb / s. Kilku sprzedawców laptopów oferuje jednostki „gotowe do WiMAX", dostępne są również adaptery USB WiMAX. Technologia WiMAX jest również wykorzystywana do połączeń na duże odległości punkt-punkt za pośrednictwem repeaterów za pomocą anten kierunkowych. Funkcje WiMAX obejmują

• Roaming - zapewnia mobilność klienta (802.16e)

• Forward error error - wykorzystuje algorytmy tolerancji błędów

• Modulacja adaptacyjna - zmienia zakres przepustowości

• Uwierzytelnianie użytkownika i urządzenia

• Poufność przesyłanych wiadomości danych

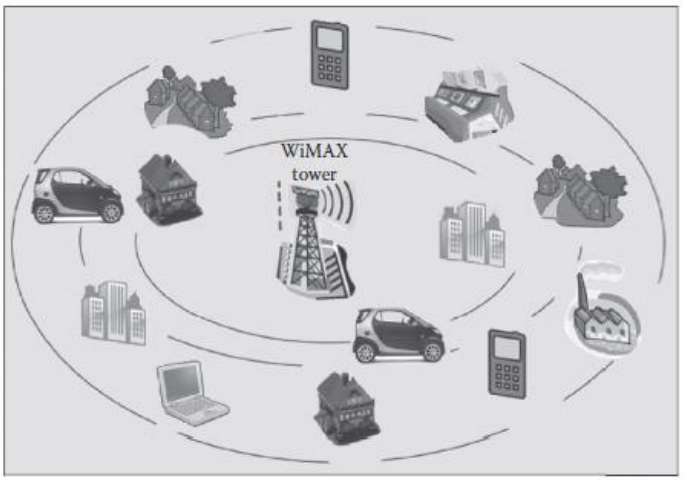
• Wysoka przepustowość danych - osiąga 75 Mb / s

• Szyfrowanie Triple-DES - do uwierzytelniania i transmisji

• AAS — wykorzystuje zaawansowane techniki antenowe (802.16e)

• Prędkość do 1 Gb / s i 100 Mb / s odpowiednio dla operacji stacjonarnych i mobilnych (802.16m)

Rysunek 2.9 ilustruje możliwe środowisko WiMAX, w którym Internet jest świadczony w promieniu 50 km dla całej populacji.



W tym scenariuszu Internet jest zapewniany jednemu użytkownikowi za pomocą telefonu komórkowego, laptopa lub komputera stacjonarnego, a także organizacjom wielu użytkowników, takim jak budynki biurowe, budynki mieszkalne lub parki przemysłowe. W przeciwieństwie do dostawców produktów i usług WiMAX badacze twierdzą, że istnieje kilka luk w technologii WiMAX. Po wprowadzeniu specyfikacji 802.16e większość domniemanych luk została usunięta. Pozostają jednak następujące luki, jak wskazano w raporcie NIST.

• Kompleksowe bezpieczeństwo (tj. urządzenie z urządzeniem) nie jest możliwe bez zastosowania dodatkowych środków kontroli bezpieczeństwa, które nie są określone w standardach IEEE.

• Dane SA (Security Associations) nie mogą być stosowane do wiadomości zarządzania, które nigdy nie są szyfrowane.

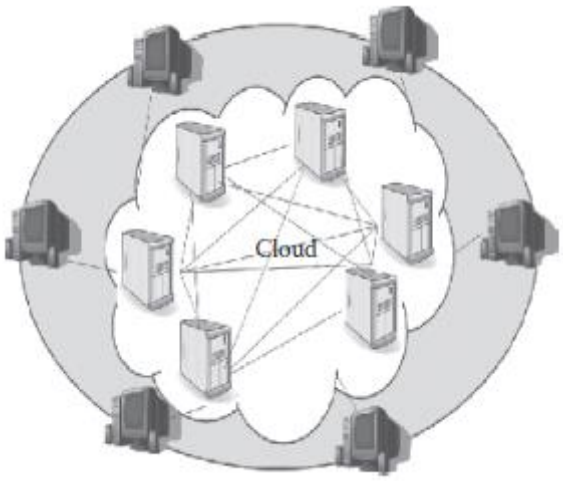
• Brak wzajemnego uwierzytelnienia może pozwolić podstępnej BS (stacji bazowej) na podszywanie się pod legalną BS, przez co SS / MS (stacja abonencka / stacja mobilna) nie będzie w stanie zweryfikować autentyczności wiadomości protokołu odebranych od BS.

Dlatego w celu zachowania poufności komunikatów zarządzania użytkownicy WiMAX muszą udoskonalić swój własny system bezpieczeństwa. W takim przypadku można również użyć standardowej umowy Diffie – Hellmana, która jest często stosowana w przypadkach, gdy poufna komunikacja musi rozpocząć się bez uprzedniej wymiany kluczy. Lista środków zaradczych, które mogą zmniejszyć ryzyko w sieciach bezprzewodowych, jest opisana w dokumentach przygotowanych przez NIST

Chmura obliczeniowa

Skutkiem tego jest coraz niższy koszt sprzętu komputerowego i telekomunikacyjnego w połączeniu ze standaryzacją oprogramowania.

Chmura obliczeniowa. Termin „przetwarzanie w chmurze” odnosi się do nowej koncepcji pozyskiwania mocy obliczeniowej jako usługi. Ta usługa jest świadczona z połączonych zasobów, w których użytkownik nie ma wiedzy o fizycznym pochodzeniu takiej usługi. Rysunek ilustruje koncepcję przetwarzania w chmurze, w której użytkownicy potrzebują tylko dostępu do Internetu.



Dostawcy takich usług mogą nawet współdzielić zasoby, tworząc usługę, która może być równoległa do dystrybucji energii elektrycznej. W tym kontekście moc obliczeniowa obejmuje oprogramowanie, sprzęt wirtualny, przechowywanie danych i dostęp do danych. W pewnym sensie jest podobny do

koncepcji dzielenie czasu w latach siedemdziesiątych, ale jest ono znacznie bardziej wydajne i dostępne za pośrednictwem Internetu, a nie modemów telefonicznych. Obecnie w przypadku przetwarzania w chmurze organizacja nie potrzebuje centrum komputerowego, ponieważ wszystkie potrzeby obliczeniowe są realizowane i świadczone jako usługa przez Internet. Przetwarzanie w chmurze należy do czterech podstawowych definicji.

Chmura publiczna: komercyjne centrum ogromnych zasobów obliczeniowych, które są udostępniane społeczeństwu na żądanie w sposób dozowany.

Prywatna chmura: prywatne centrum współdzielonych zasobów obliczeniowych, które są dostarczane członkom społeczności na żądanie w sposób dozowany. Środki bezpieczeństwa i prywatności są dostosowane do potrzeb właścicieli.

Chmura społecznościowa: będące własnością społeczności centrum ogromnych zasobów obliczeniowych, które są dostarczane członkom społeczności na żądanie w sposób dozowany. Środki bezpieczeństwa i prywatności są dostosowane do potrzeb społeczności.

Chmura hybrydowa: połączenie powyższych opcji

Dostawcy usług przetwarzania w chmurze oferują infrastrukturę, platformę i oprogramowanie jako usługę (odpowiednio w skrócie IaaS, PaaS i SaaS). Użytkownicy subskrybują takie usługi i konfigurują własne wirtualne centrum komputerowe z serwerami i bazami danych, tak jakby kupowali sprzęt fizyczny w tym celu. W takim trybie operacyjnym organizacja może w dowolnym momencie zmienić konfigurację i skalować potrzeby obliczeniowe i być obciążana opłatami według zużycia. Motto tej nowej branży brzmi: „kup dokładnie taką pojemność, jakiej potrzebujesz, kiedy jej potrzebujesz, na godzinę lub w ramach abonamentu miesięcznego. Aplikacje i dane użytkowników dostarczane przez współdzielone centra danych mogą znajdować się w zróżnicowanych geograficznie lokalizacjach, a nawet mogą zmieniać lokalizacje w sposób przejrzysty dla użytkownika. Jednak wszystko jest dostępne w Internecie za pośrednictwem tych samych adresów logicznych. Dzięki udostępnianiu ekranu, a także udostępnianiu aplikacji w chmurze, przetwarzanie w chmurze stało się jeszcze bardziej atrakcyjne dla interakcji przez Internet. Przetwarzanie w chmurze zyskuje coraz większe wsparcie jako praktyczne rozwiązanie do budowy korporacyjnego centrum danych w sposób zwirtualizowany i bez alokacji fizycznej przestrzeni. Poniżej mamy listę najbardziej uznanych zalet przetwarzania w chmurze.

1. Rekonfiguracja Użytkownicy mogą przeprojektować swoją infrastrukturę obliczeniową jednym kliknięciem myszy, wybierając i usuwając zasoby (serwery, pamięć masową, aplikacje, sieci i usługi) w zależności od potrzeb.

2. Obsługa interfejsu API Interfejs programowania aplikacji jest możliwy do interakcji oprogramowania w chmurze z maszynami lub ludźmi.

3. Niższe koszty Przetwarzanie w chmurze zmniejsza bariery wejścia na rynek, ułatwiając tworzenie centrów danych organizacji z odmierzonych zasobów za pomocą modelu biznesowego „na żądanie”.

4. Ograniczone umiejętności Niezbędne umiejętności konfigurowania i utrzymywania zwirtualizowanego centrum danych w chmurze są znacznie mniej wymagające niż umiejętności utrzymania centrum fizycznego.

5. Łączność Usługi łączności w chmurze obejmują dostęp do Internetu oraz telefon komórkowy.

6. Niezawodność Korzystanie z wielu zbędnych witryn może zapewnić ciągłość biznesową i odzyskiwanie po awarii.

7. Skalowalność Przetwarzanie w chmurze zapewnia skalowalność na żądanie w trybie samoobsługowym, umożliwiając rekonfigurację systemu w celu zwiększenia lub zmniejszenia wielkości lub zużycia zasobów.

8. Bezpieczeństwo Zapewnione są funkcje bezpieczeństwa, które zwykle są zbyt drogie, na które stać poszczególnych użytkowników.

9. Konserwacja Dostawcy usług przetwarzania w chmurze

Nie ma wątpliwości, że przetwarzanie w chmurze jest bardzo silnym nieodwracalnym trendem, ale wraz z nim pojawiają się wyzwania związane z bezpieczeństwem i prywatnością, które przekładają się na podatności na zagrożenia, które należy dokładnie rozważyć przed wejściem do tego ogrodu różanego. „Wyzwania związane z bezpieczeństwem przetwarzania w chmurze są jednak ogromne, szczególnie w przypadku chmur publicznych, których infrastruktura i zasoby obliczeniowe są własnością podmiotu zewnętrznego, który sprzedaje te usługi ogółowi społeczeństwa". Powyższe oświadczenie, pochodzące od bardzo autorytatywnego organu, takiego jak NIST, może sprawić, że CIO i CSO zatrzymają się. Istnieje silna obawa, że powierzona opieka powierzona fizycznemu przechowywaniu wrażliwych danych organizacyjnych stanowi sama w sobie poważną lukę. Dla wielu i z definicji przetwarzanie w chmurze jest niezabezpieczonym środowiskiem. Jednak dla rosnącej liczby, przetwarzanie w chmurze jest właściwą drogą i pozostanie. Jeśli chodzi o bezpieczeństwo i prywatność, można podjąć dodatkowe środki w celu dostosowania tego nowego trybu do tradycyjnych wewnętrznych centrów danych w tym zakresie. Przed przystąpieniem do przejścia na przetwarzanie w chmurze należy uzyskać weryfikowalne gwarancje, że wymogi bezpieczeństwa i prywatności w organizacji są w pełni spełnione. Dostawcy usług w chmurze często oferują umowy usługowe, które nie podlegają negocjacji. Nie jest to jednak absolutne i można je wynegocjować. Należy podkreślić, że system przetwarzania w chmurze obejmuje oprogramowanie klienckie oraz jego oprogramowanie i urządzenia dostępowe, a także po tej stronie należy zabezpieczyć zasady bezpieczeństwa i prywatności. W razie potrzeby dostawca usług przetwarzania w chmurze powinien być w stanie wykazać skuteczność oferowanych usług, zwłaszcza tych związanych z bezpieczeństwem i prywatnością. Często kontrolerzy zewnętrzni są przyprowadzani w celu potwierdzenia ważności żądanych usług. Przetwarzanie w chmurze należy do ogólnej kategorii outsourcingu, ze wszystkimi związanymi z tym zagrożeniami. Dlatego przed przystąpieniem do takich umów wymagana jest dokładna analiza ryzyka. Główne dostrzegane wady subskrypcji środowiska przetwarzania w chmurze wymieniono poniżej.

• Złożoność systemu	• Z powodu platform chmurowych, zwłaszcza publicznych ich rozmiar i zwiększona funkcjonalność są otwarte na błędy i podatności.
• Wiele dzierżawców	• Obawy dotyczą środowiska współdzielonego przez wielu dzierżawców zasoby, brak silnego podziału na kategorie może skutkować problemy z bezpieczeństwem lub prywatnością.
• Internet vs.intranet	• Przetwarzanie w chmurze jest dostępne w Internecie i z definicji mniej bezpieczne niż izolowany intranet organizacyjny.
• Personel	• Personel chmury publicznej może nie mieć wymaganych wymagań poziom poświadczenia bezpieczeństwa.
• Forensics	• W środowisku chmurowym, w zależności od poziomu wewnętrznego w przypadku audytu może nie być możliwe powiązanie wykonanych usług powiązany sprzęt. Ponadto poprzednie ciągi komputerów i działania

	generowane przez ludzi mogą być trudne do prześledzenia i udokumentowania do akceptowalnego przez sąd poziomu i może być niemożliwe do powielenia.
• Zasady chmurowe	• Zasady bezpieczeństwa i prywatności dostawców usług przetwarzania w chmurze oraz praktyki mogą, ale nie muszą być zgodne z praktykami wymagającymi prywatnych lub lokatorzy rządowi.
• Przejęcie konta	• Chociaż przykłady nie są dostępne, istnieje duże zaniepokojenie w Internecie możliwość włamania poświadczeń i późniejszej strony internetowej kompromis.
• Przerwa w świadczeniu usług	• Istnieje wiele przykładów, w których przyczyny są poza kontrolą dostawcy usług w chmurze spowodowali przerwy w pracy na kilka godzin w najmniej oczekiwane czasy. Jest to problem, który można dobrze sformułować w umowa serwisowa, ale piorun nie przeczyta jej przed uderzeniem.
• Reakcja na incydent	• Takie zdarzenie będzie wymagało skoordynowanego wysiłku służby subskrybent i usługodawca w ogromnym zadaniu audytu śledzenie, które może obejmować wcześniejsze użycie wspólnego sprzętu.

Podczas gdy „przejście do outsourcingu publicznego środowiska przetwarzania w chmurze jest pod wieloma względami ćwiczeniem w zakresie zarządzania ryzykiem", przetwarzanie w chmurze, które jest obecnie w powijakach, ostatecznie stanie się głównym hostem centrum danych ze względu na swoją opłacalność, która poprawi się w porównaniu z czasem.

Internet przedmiotów

Pierwsza era cyberprzestrzeni miała miejsce, gdy jej jedynymi mieszkańcami były komputery. Ogromnym osiągnięciem było posiadanie jednej sieci - Internetu obejmującej cały świat, a także możliwość wysyłania i odbierania tekstu, audio i wideo w czasie rzeczywistym. Druga era cyberprzestrzeni miała miejsce, gdy zalały ją smartfony, znacznie przewyższając liczbę podłączonych komputerów. Wkroczyliśmy w trzecią erę cyberprzestrzeni, w której zostanie zalana rzeczami, dzięki czemu stanie się Internetem Rzeczy (IoT). Oczekuje się, że do roku 2020 będzie 24 miliardów urządzeń IoT obsługujących świat w praktycznie każdym aspekcie życia. Wraz z napływem urządzeń IoT pojemność protokołu IPv4, który może pomieścić do $4{,}3 \times 10^9$ adresów IP, będzie wymagać uaktualnienia do protokołu Ipv6, który pomieści ponad 340×10^{36} adresów IP - astronomiczny 39- cyfra Uważa się jednak, że protokół IPv4 będzie wystarczający w najbliższej przyszłości. Są to znormalizowane urządzenia dostępne w Internecie z możliwością komunikacji z czujnikami i urządzeniami wykonawczymi, umożliwiając nam interakcję w czasie rzeczywistym w praktycznie dowolnym środowisku. W skrócie, przez Internet lub Bluetooth, urządzenia IoT bez ograniczeń wykrywają, komunikują się, analizują i działają. Urządzenia IoT mogą służyć jako autonomiczne inteligentne czynniki, usprawniające operacje w celu zwiększenia skuteczności, bezpieczeństwa i wydajności. Poziom innowacji osiągnie niespotykane wyżyny. Ogólnie oczekujemy, że zobaczymy:

• Nieograniczona i wszechobecna łączność

• Redukcja kosztów produktów i usług

• Miniaturyzacja

• Postępy w analizie danych

• Wzrost w chmurze obliczeniowej

• Zmniejszenie zużycia energii dzięki inteligentnemu sterowaniu oświetleniem i temperaturą

• Lepsza opieka zdrowotna dzięki cichemu monitorowaniu 24/7

• Zwiększa produktywność

• Nie do pomyślenia produkt i usługi

Rzeczywiście, dzięki wykorzystaniu urządzeń IoT społeczeństwo będzie czerpać znaczne korzyści. Konkretne zastosowania Internetu Rzeczy obejmują następujące przykłady:

• Śledzenie zwierząt gospodarskich, upewniając się, że każda jest odpowiednio karmiony.

• Śledzenie drzew, upewniając się, że nie ma nielegalnych działań związanych z wylesianiem.

• Wyczuwanie wilgoci w glebie w celu optymalnego nawadniania działek w miarę potrzeby.

• Wykorzystanie urządzeń monitorujących zdrowie do monitorowania wartości parametrów zdrowotnych, takich jak oddychanie, bicie serca, temperatura, ciśnienie krwi itp., Przy jednoczesnym natychmiastowym powiadamianiu o odchyleniach od oczekiwanych wartości.

• Zdalne rejestrowanie zużycia energii elektrycznej, które poprzednio wymagało od osoby odczytania każdego licznika elektrycznego w mieście, deszczu lub świecenia.

• Automatyczny wykrywacz awarii i dyspozytor pomocy awaryjnej.

• Reporter miejsca parkingowego, w którym strona internetowa wyświetla lokalizację dostępnego parkingu.

• Parametry śledzenia pojazdów flotowych, takie jak lokalizacja, prędkość, poziom paliwa, temperatura silnika itp.

Biorąc pod uwagę, że urządzenia IoT wykorzystują mikrokontrolery - komputery jednoukładowe - o ograniczonej mocy obliczeniowej i pojemności pamięci, równolegle z powyższymi oczekiwaniami budzą wiele obaw, podobnych do tych zgłaszanych podczas wprowadzania smartfonów, takich jak:

• Co stanowi dobrą praktykę projektową?

• Jaki jest poziom tolerancji na uszkodzenia?

• Czy jest nadmiarowość?

• Czy usterki są wykrywalne i usuwalne?

• Czy istnieją wystarczające zasoby edukacyjne, aby wyprodukować tak dużą liczbę inżynierów Internetu Rzeczy?

• Czy gromadzone dane są odpowiednio oznaczone datą?

• W jaki sposób monitorowana jest wydajność?

• W jaki sposób ocenia się i ocenia ryzyko bezpieczeństwa?

• W jaki sposób chroniona jest poufność danych, uwierzytelnianie i kontrola dostępu?

• W jaki sposób nastąpi modernizacja?

• Jak długo potrwa, zanim zostaną ustanowione standardy branżowe urządzeń IoT?

• Jak długo potrwa, zanim zostanie ustanowiona legalna infrastruktura IoT?

• Jak będą obsługiwane awarie bezpieczeństwa lub wydajności?

• Czy urządzenia IoT powinny mieć wymuszone wygaśnięcie, wyłączając je w określonym momencie?

Przy tak wielu oczach i uszach na całym świecie jest rzeczą naturalną, że poruszone zostaną kwestie prywatności. W wielu przypadkach będzie to niezapowiedziane naruszenie prywatności bez zgody, a nawet świadomości. Przykład podniesionych już problemów związanych z prywatnością urządzeń IoT jest następujący:

• Gromadzenie danych: tryb, wykorzystanie i usuwanie.

• Preferencje prywatności: wyrażenie, egzekwowanie, przejrzystość.

• De-personalizacja danych „statystycznych" gromadzonych za pośrednictwem urządzeń IoT.

• Równowaga między prywatnością a bezpieczeństwem.

• Prywatność od samego początku.

• Problemy z odpowiedzialnością i zaufaniem.

Prawdą jest, że jeśli czujniki są wszędzie, praca organów ścigania będzie łatwiejsza. Na przykład kamery w miejscach publicznych mogą, miejmy nadzieję, powstrzymać przestępczość, a urządzenie IoT w każdym samochodzie ułatwi odzyskanie, jeśli zostanie skradzione, ale takie aplikacje, jeśli zostaną wykorzystane, mogą spowodować poważne naruszenia wolności obywatelskich. Niezależnie od zastosowania lub potencjalnego nadużycia, urządzenia IoT powinny być tak zaprojektowane aby :

• Poziom wbudowanych zabezpieczeń jest proporcjonalny do zastosowania urządzenia.

• Choć bezpieczny, szanuje prywatność gromadzonych danych.

• Domniemana prywatność jest weryfikowalna.

• Osobiste identyfikatory są usuwalne.

• Klucze szyfrujące są bezpieczne i zarządzane.

Zgodnie z oczekiwaniami istnieje wiele przykładów problemów z bezpieczeństwem lub nadużyć w stosowaniu urządzeń IoT, przy czym bezpieczeństwo fizyczne urządzeń jest najmniejsze. Typowe przypadki to gdzie

• Jeden z głównych producentów samochodów musiał wycofać ponad milion samochodów, aby naprawić usterkę, która umożliwi ingerencję bezprzewodową w samochody.

• W kraju Europy Wschodniej cyberprzestępcy zamknęli całą sieć energetyczną, pogrążając się w ciemnościach i zimnych milionach mieszkańców.

• W innym kraju europejskim cyber-szpiedzy, z powietrza, nie chcieli wybierać kanałów telewizyjnych, aby udowodnić swoje zdolności hakerskie.

Podsumowując, niewątpliwie technologia Internetu przedmiotów jest bardzo obiecująca dla producentów urządzeń, dla przedsiębiorstw, które je zintegrują, oraz dla konsumentów, którzy będą z

nich korzystać. Przed nami jednak wyzwania, szczególnie na dwóch frontach, a mianowicie: stać się prywatnymi i bezpiecznymi oraz przekonać świat, że są prywatne i bezpieczne.

Cyberbezpieczeństwo motoryzacyjne

Cyberprzestrzeń rozwija się i obejmuje całkowicie nienaruszone dziedziny, takie jak przemysł motoryzacyjny i kierowca. To kwestia czasu, kiedy producenci samochodów będą oferować „Internet w samochodzie" jako standardową funkcję. Kierowca po prostu włoży kartę SIM telefonu komórkowego, a pojazd „zapełni" się Wi-Fi. Wi-Fi będzie dostarczane z urządzeniem Pandora oferującym niespotykane funkcje:

• Wsparcie nawigacji

• Doradztwo drogowe w czasie rzeczywistym

• Przybycie wybranego e-maila

• Wykrywanie awaryjne i wezwanie pomocy

• Raportowanie wydajności pojazdu

• Raportowanie wydajności kierowcy

• Nieograniczone opcje rozrywki

• Rozpoznawanie głosu dla tożsamości i kontroli

• Zdalny dostęp i wykrywanie

Zasadniczo komfort salonu i wydajność biura zostaną połączone w fotelu kierowcy, czyli w centrum dowodzenia i kontroli kierowcy. Wraz z bogactwem funkcji - zwiększonym bezpieczeństwem, wydajnością i rozrywką - powstaje „szeroki obszar cyberataków", ku radości hakerów i cyberprzestępców. Z definicji wszystko w sieci, przewodowo lub bezprzewodowo podlega hakowaniu. Ingerencja w lokalną sieć kontrolowanego obszaru pojazdu (CAN) może wstrzykiwać polecenia ze zdalnej lokalizacji, zdolnej do przejęcia danych i funkcji krytycznych z punktu widzenia bezpieczeństwa i innych niż bezpieczeństwo, co może mieć wpływ na zdolność kierowcy do kontrolowania pojazdu. Rządy przewidujące nadchodzącą integrację pojazdu z Internetem przygotowały szeroko zakrojone badania, wskazujące na ryzyko, które towarzyszy wraz z szybkim przyjęciem technologii. Na szczęście opracowano standardy cyberbezpieczeństwa dla „Cyber-fizycznych pojazdów samochodowych". Zdarzały się przypadki zdalnego dostępu do elementów sterujących pojazdu, które potencjalnie mogły stworzyć niebezpieczną sytuację. Podsumowując, we wszystkich sektorach cyberbezpieczeństwo pozostaje mieszanym błogosławieństwem, wymagającym dokładnych słabych punktów i oceny ryzyka. Takie badania wymagają profesjonalnej znajomości branży motoryzacyjnej, a także cyberbezpieczeństwa. W końcu każdy pojazd musi być postrzegany jako wielofunkcyjne „urządzenie" Internetu Rzeczy, które należy chronić przed możliwymi cyberprzestępstwami

Narzędzia oceny podatności

Dzisiejsze korzystanie z Internetu przypomina pływanie w wodach wypełnionych rekinami. Wirusy internetowe zwykle po cichu wykonują swoje własne zadania kopiowania lub niszczenia plików lub instalowania kodu, który spowoduje jeszcze więcej szkód. Często aktywne wirusy spowalniają komputer lub działają dziwnie.

Na szczęście dostępnych jest wiele narzędzi antywirusowych, które mogą zminimalizować takie ryzyko, jeśli nie wyeliminować je. Należy podkreślić, że ciągłe infekowanie Internetu nowymi i potężniejszymi

wirusami uniemożliwia absolutne poleganie na narzędziach antywirusowych. Zazwyczaj działania wykonywane przez takie narzędzia antywirusowe obejmują:

• Zbieranie adresów IP ruchu przychodzącego i wychodzącego

• Śledzenie zgodności użytkownika z zasadami organizacji

• Wykrywanie wzorców ataku

• Wykrywanie nietypowych działań użytkownika

• Ocena integralności transferów plików

• Analizy zebranych danych pod kątem kryteriów bezpieczeństwa cybernetycznego

Jednak zainstalowanie bieżącego narzędzia antywirusowego w systemie jest rozsądne i utrzymanie go w trybie automatycznym jest koniecznością. W przypadku braku trybu automatycznego codzienne skanowanie jest niezbędne.

Zagrożenia w infrastrukturze systemów informatycznych

Wprowadzenie

Być może nie zdawaliśmy sobie sprawy, że każdy aspekt życia wiąże się z ryzykiem, przy czym ryzyko to niekorzystna szansa, że oczekiwany cel nie zostanie spełniony. Analiza ryzyka ocenia takie nieszczęścia pod kątem prawdopodobieństwa ich wystąpienia oraz wagi konsekwencji, jeśli tak się stanie. Należy zauważyć, że nie może istnieć złożony system, który byłby w 100% doskonały lub bezpieczny. Każdy projekt jest zbliżony do ideału. Przy tworzeniu produktu końcowego lub usługi należy wyważyć wiele parametrów według wybranych kryteriów. Najważniejsze parametry to pieniężny koszt przedsprzedażny, czas trwania procesu opracowywania lub wprowadzenia produktu na rynek, okres życia produktu po sprzedaży oraz bezpieczeństwo i dostępność tego produktu lub usługi w tym okresie. Rozwój i wykorzystanie systemów informatycznych odbywa się zgodnie z tą ogólną ścieżką, w ramach której w procesie równoważenia parametrów powstają luki, które prowadzą do ryzyka. W życiu nie ma działalności całkowicie wolnej od ryzyka, a tam, gdzie to możliwe, kupowane jest ubezpieczenie lub podejmowane są środki w celu zminimalizowania ryzyka. Dlatego motto to minimalizacja ryzyka, a nie eliminacja ryzyka. Obecnie każda organizacja działa na infrastrukturze systemów informatycznych, zarówno wewnętrznej, jak i zewnętrznej. W obu przypadkach istnieje ryzyko. Istnieją dwa czynniki oceny wartości operacyjnej infrastruktury systemów informatycznych: identyfikacja nieodłącznego ryzyka i dostępność odpowiednich pozycji rezerwowych. Infrastrukturą zewnętrznych systemów informatycznych jest w zasadzie Internet. Jeśli chodzi o zależność organizacyjną od Internetu - niestety - jest ona prawie absolutna. W rezultacie bezpieczeństwo Internetu, cyberbezpieczeństwo, jest sprawą najwyższej wagi dla wszystkich sektorów społeczeństwa. Internet zawiera luki, które stanowią zagrożenie dla tych, którzy z niego korzystają, ale ponieważ nie ma wyboru, z Internetu należy korzystać z jego wadami. Użytkownicy powinni jednak rozpoznawać i oceniać zagrożenia, dzięki czemu są one przystępne cenowo dzięki środkom ostrożności, dzięki którym systemy są stosunkowo dostępne, niezawodne i bezpieczne.

Ryzyko sprzętowe

W systemie każdy element sprzętu odgrywa rolę w misji organizacji. W oparciu o znaczenie tej roli należy podjąć odpowiednie środki bezpieczeństwa. Aby zminimalizować ryzyko związane z bezpieczeństwem, organizacje ustanawiają oficjalne zasady bezpieczeństwa, które muszą obejmować co najmniej następujące dwanaście zasad.

Zasada pierwsza: identyfikacja połączeń. Każdy element sprzętu, uważany za jednostkę sprzętową, musi mieć jasno określone, uzasadnione i chronione połączenia za pomocą określonych środków bezpieczeństwa, niezależnie od tego, czy połączenia te są fizyczne czy bezprzewodowe. Parametry operacyjne urządzenia muszą być wyraźnie udokumentowane. Na przykład hasła muszą zidentyfikować ich właścicieli, a także administratorów, przy czym administratorzy przypisują hasła, a także zasady odnowienia, które muszą być znane wszystkim znającym się pracownikom. Niepotrzebne połączenia muszą zostać usunięte, a niezbędne muszą zostać połączone, gdy zajdzie taka potrzeba. W stosownych przypadkach należy prowadzić dzienniki połączeń, szczególnie w przypadku połączeń z Internetem, intranetem i dowolnymi ekstranetami.

Zasada druga: ocena bezpieczeństwa. Środki bezpieczeństwa należy oceniać w odstępach czasu związanych z rozwojem technologii i zaawansowaniem ataków. Ocena powinna obejmować analizę podatności na zagrożenia, a także testy penetracyjne. Środki bezpieczeństwa muszą obejmować dwukierunkowe zapory ogniowe we wszystkich punktach wejścia-wyjścia, a także system wykrywania i zapobiegania włamaniom. Dostęp do urządzenia musi odbywać się na zasadzie dostępu, bez żadnych haseł. Oznacza to, że użytkownicy otrzymują hasła, które uzyskują dostęp tylko do funkcji, do których

są autoryzowane. Przez cały czas, 24 godziny na dobę, przez 7 dni w tygodniu, każda jednostka sprzętowa ma członka organizacji odpowiedzialnego za jej bezpieczeństwo. Jednostka sprzętowa w żadnym momencie nie może być uważana za nienadzorowaną.

Zasada trzecia: parametry dostawcy. Wszystkie parametry operacyjne muszą zostać wprowadzone przez personel rozpoznający i nie można pozostawić sprzętu z parametrami domyślnymi, zwłaszcza nazwami użytkowników, hasłami i ustawieniami zapory. Istnienie jakichkolwiek backdoorów, zapadni lub specjalnych punktów wejścia lub interfejsów dostawców musi być znane i zaplombowane, jeśli to możliwe. Dostawcy muszą być stale dostępni w celu wyjaśnienia słabych punktów, wsparcia operacyjnego, konserwacji i napraw.

Zasada czwarta: środki bezpieczeństwa. Podczas gdy większość głównych deweloperów sprzętu zapewnia własne środki bezpieczeństwa, najczęściej opierają się one na zastrzeżonych protokołach, zgadzając się z filozofią, że niejasność jest wbudowanym zabezpieczeniem. Jest to sprzeczne z podstawową zasadą bezpieczeństwa, że dostęp musi być chroniony, a nie ukryty, przed wzrokiem. Biorąc pod uwagę, jak krytyczna jest jednostka w działaniu, należy zaprojektować środki w celu spełnienia polityki bezpieczeństwa i prywatności organizacji. W stosownych przypadkach dostęp przychodzący należy zastąpić informacją „nie dzwoń do nas" podejście. Oznacza to, że dzwoniący składa żądanie danych, a system wysyła dane do dzwoniącego, a nie dzwoniącego bezpośrednio uzyskującego dostęp do baz danych.

Zasada piąta: Wykrywanie włamań i zapobieganie im. Wbudowany powinien być system wykrywania i zapobiegania włamaniom 24/7 (IDPS), który monitoruje zarówno zewnętrzne, jak i wewnętrzne włamania oraz zgłasza personelowi rozpoznającemu różne tryby; takich jak dźwięki dźwiękowe i / lub migające obrazy na terminalu monitorującym, wiadomości e-mail lub w wiadomości SMS Integralną częścią IDPS jest predefiniowana sekwencja kroków w celu obsługi włamania. W każdym działaniu związanym z bezpieczeństwem musi być zaangażowanych więcej niż jeden członek IT. Jest bardzo ważne i z różnych punktów widzenia, aby raporty z oceny włamań były wynikiem pracy zespołowej, a nie pojedynczego badacza.

Zasada szósta: audyty. Częste audyty techniczne są podstawą każdej polityki bezpieczeństwa. Korzystając z gotowych narzędzi bezpieczeństwa, transpirowane operacje mogą być rejestrowane i przeglądane w kolejności identyfikować trendy i ewentualnie rozpoznawać aberracje. Audyty powinny obejmować wizyty w środowisku fizycznym danej jednostki sprzętowej w celu ewentualnego wykrycia nieautoryzowanych możliwych punktów stukowych, fizycznych lub bezprzewodowych oraz w celu potwierdzenia egzekwowania zasad dostępu fizycznego.

Zasada siódma: „Niebieska drużyna". Powstaje niebieski zespół odpowiedzialny za ocenę podatności, zagrożeń i ryzyka. Zespół jest stałym komitetem złożonym z członków IT i nie-IT, którzy identyfikują scenariusze ataków oraz sugerują obronę i środki zaradcze. Niebieskie zespoły często ustawiają doniczki z miodem w oczekiwaniu na włamanie.

Zasada ósma: opisy stanowisk. Wyraźne opisy zadań określają obowiązki i uprawnienia każdego członka struktury bezpieczeństwa cybernetycznego organizacji. Opublikowano schemat blokowy ilustrujący kroki, jakie należy podjąć w przypadku cyberataku. Najważniejsze jest, aby uznać, że aby skutecznie wypełniać obowiązki, należy rozszerzyć wystarczające uprawnienia.

Zasada dziewiąta: funkcje krytyczne. W każdym systemie, chociaż wszystkie funkcje są ważne, niektóre funkcje są bardziej krytyczne lub wrażliwe niż inne. Z tego powodu należy narysować hierarchiczną tabelę ilustrującą różne funkcje, ponieważ obejmują one misję systemu. Pokazany powinien być również ich poziom względnego znaczenia wraz z odpowiednimi zagrożeniami i powiązanymi środkami

zaradczymi. Biorąc pod uwagę, że nowe zagrożenia pojawiają się stale, wykres ten musi być stale poddawany ponownej ocenie przez komitet ds. Bezpieczeństwa cybernetycznego organizacji. Ten proces samooceny utrzyma organizację w ryzach wobec rosnących zagrożeń dla bezpieczeństwa cybernetycznego.

Zasada dziesiąta: ciągłość działania. Awaria systemu nigdy nie może zostać wykluczona przez dojrzałego stratega. W związku z tym konieczne jest przyjęcie przepisów i wdrożenie procedur umożliwiających wyleczenie po wyłączającym cyberataku z ograniczeniem strat do absolutnego minimum. Wymaga to ciągłej i wielowarstwowej archiwizacji danych, nadmiarowości funkcjonalnej oraz znajomości niezbędnych procedur przez personel. Taki kryzys niekoniecznie musi być spowodowany cyberatakiem. Może to być praca wewnętrzna lub akt natury.

Zasada jedenasta: zarządzanie konfiguracją. Konfiguracja dowolnego systemu, a nawet więcej dowolnego systemu informatycznego, nigdy nie może być statyczna. Nowy sprzęt, nowe oprogramowanie, nowe zagrożenia, nowe rynki, nowe technologie i nowe pomysły wymagają od strategów IT zmiany konfiguracji systemów w sposób ewolucyjny. Jednak moda może być czasami rewolucyjna. W rezultacie zarządzanie konfiguracją obejmuje całe spektrum elementów systemu, w tym sprzęt, oprogramowanie i umiejętności personelu, a także aktualizacje zasad bezpieczeństwa.

Zasada dwunasta: Głęboka obrona. Jest to bardzo stara koncepcja obrony, która została przeszczepiona do systemów informatycznych. Jego podstawowe zasady to dwa: obrona warstwowa i brak pojedynczego punktu awarii. Pomyślne wdrożenie tej koncepcji wymaga zastosowania odpowiednich środków podczas całego procesu rozwoju systemu. Takie środki stworzyłyby wiele warstw obrony między uczestnikiem a poszukiwanym zasobem i zablokowałyby dostęp uczestnika do nieautoryzowanych obszarów

Zagrożenia w oprogramowaniu

Chociaż oprogramowanie i sprzęt idą w parze, ich potrzeby w zakresie rozwoju, konserwacji i bezpieczeństwa są zupełnie inne. Główną różnicą jest to, że programistom brakuje skończonej metodologii oraz wskaźniki generowane przez rozwój sprzętu na przestrzeni lat. Oprogramowanie nigdy nie osiągnie poziomu sprzętowego wskaźników, ponieważ tworzenie oprogramowania jest procesem w 100% intelektualnym i jako takie podlega ludzkim parametrom. Wytwarzanie produktu sprzętowego, na przykład komputera osobistego, można podzielić na skończone procesy za pomocą skończonych kroków, co skutkuje podobnie ograniczonymi wymaganiami umiejętności i roboczogodzin. Z drugiej strony, tworzenie oprogramowania silnie zależy od doświadczenia, wiedzy i dostępnych narzędzi programistów - analityków i programistów - a jego kosztów, szczególnie na czas, nie można ustalić tak łatwo, jak w przypadku sprzętu. „Badania niepowodzenia projektów ... sugerują, że 75% wszystkich projektów IT w USA uważa się za niepowodzenia", ponieważ nie spełniają oczekiwań sponsorów. Istnieją trzy podstawowe oczekiwania: czas dostawy, budżet i wydajność funkcjonalna. Aby zminimalizować ryzyko awarii podczas tworzenia oprogramowania, należy przestrzegać następujących siedmiu zasad.

Zasada pierwsza: zintegrowane zabezpieczenia. Opracowywanie systemu obejmuje kilka etapów, poczynając od koncepcji, a kończąc na opracowaniu instrukcji obsługi, przy czym każda faza zawiera niezbędne środki bezpieczeństwa. Miary te są początkowo zdefiniowane w sposób abstrakcyjny, ale stopniowo są mapowane między fazami podczas procesu rozwoju, co kończy się na konkretnych krokach, które zapewnią bezpieczeństwo systemu.

Zasada druga: rozwój strukturalny. Należy przestrzegać ustrukturyzowanego rozwoju oprogramowania, które wymaga hierarchicznej organizacji modułów oprogramowania, w których

maksymalna autonomia modułów jest większa niż wielkość kodu. W ten sposób moduł można łatwo opisać i przetestować. Może nie mieć kodu najbardziej wydajnego przestrzennie, ale jego testowanie i rozwiązywanie problemów będzie łatwe i bezpośrednie.

Zasada trzecia: zarządzanie projektem. Projekt musi mieć wykwalifikowanego profesjonalnego kierownika projektu. Istnieje błędne przekonanie, że dobry analityk lub dobry programista może być dobrym menedżerem projektu rozwoju oprogramowania. Prowadzi to do problemów, w których niewykwalifikowani i nieprofesjonalni liderzy projektów nie przestrzegają standardowych zasad zarządzania projektami, zarządzając intuicyjnie.

Zasada czwarta: specyfikacje projektu. Specyfikacje muszą być wyraźnie zdefiniowane, umożliwiając nie więcej niż jedną interpretację. Z tego powodu większość opracowań oprogramowania napotyka problemy. Bardzo częstym nieodłącznym ryzykiem związanym z oprogramowaniem jest brak nietolerancji błędów, który został zaakceptowany, aby produkt mógł szybko i konkurencyjnie wejść na rynek. Ponadto po pewnym czasie i przed rozpoczęciem projektowania specyfikacje muszą zostać zamrożone. W przeciwnym razie rozwój staje się bajką tysiąca i jednej nocy. „Błędy projektowe systemu są znacznie ważniejsze i bardziej kosztowne niż błędy kodowe; są również subtelniejsze i trudniejsze do wykrycia i poprawienia ”.

Zasada piąta: Planowanie projektu. Harmonogram rozwoju projektu musi uwzględniać nieoczekiwane zdarzenia - zawsze pojawiają się tajemnicze błędy. Ponieważ metryk oprogramowania nie można ściśle stosować, a ponieważ tworzenie oprogramowania jest procesem mentalnym wysoce zależnym od doświadczenia, wiedzy specjalistycznej i dostępnych narzędzi, nie można dokładnie przewidzieć wymagań czasowych zadania programowego. Czynniki takie jak wcześniejsze doświadczenie w danej dziedzinie lub konkretny język, złożoność funkcjonalna i przydzielony czas wprowadzenia produktu na rynek mogą znacząco wpłynąć na wynik rozwoju. Obszary niedoceniania w planowaniu obejmują czas, siłę roboczą, złożoność, poziom wymaganych umiejętności i kapitał. Najczęściej zapotrzebowanie rynku, wsparcie korporacyjne i własny poziom umiejętności są przeszacowane.

Zasada szósta: Testowanie projektu. Na testowanie oprogramowania należy przeznaczyć 25% wysiłku programistycznego w stosunku do 5% normalnie przeznaczonego na sprzęt. Testy muszą być optymalnie zgodne z filozofią TQM , która polega na testowaniu w trakcie pracy, a nie na końcu na testowaniu. Przez optymalne testowanie mamy na myśli niezbyt częste testy ani zbyt mało testów i odstępy między nimi.

Zasada siódma: stosowanie OOL. Należy użyć języka obiektowego (OOL). W ten sposób rozwój oprogramowania może skorzystać z dostępnych modułów, które zostały już opracowane i dokładnie przetestowane.

Oprócz poprzednich zagrożeń, które wpływają na funkcjonalną wydajność oprogramowania, istnieją również zagrożenia bezpieczeństwa, które mogą przechodzić przez testy nominalne. „Wszystkie typy oprogramowania mogą zawierać błędy i konsekwencje bezpieczeństwa ”. Poniższe pięć zasad może pomóc w zminimalizowaniu ryzyka związanego z bezpieczeństwem oprogramowania, zwłaszcza ryzyka cyberbezpieczeństwa.

Zasada ósma: łatki Waluta. Aby zminimalizować czas wprowadzenia produktu na rynek, programiści często wypuszczają oprogramowanie przedwcześnie, a następnie udostępniają łaty, które - miejmy nadzieję - eliminują znane już luki w zabezpieczeniach. Użytkownicy oprogramowania muszą upewnić się, że znajdują się na liście zarejestrowanych dostawców, aby otrzymywali powiadomienia, gdy tylko zostanie wydana nowa poprawka. Zwykle łaty są dostarczane regularnie, ponieważ twórcy produktu odkrywają luki w zabezpieczeniach, a złośliwe oprogramowanie staje się coraz bardziej wyrafinowane.

Reguła dziewiąta: Walidacja danych. Dane i ich autor muszą zostać zatwierdzone przed ich zaakceptowaniem. Ponadto dane i ich odbiorcy muszą zostać podobnie sprawdzone przed wysłaniem. Ponadto dane muszą zostać sprawdzone pod kątem zgodności z kryteriami akceptacji przed ich zapisaniem. Ponadto dane muszą być szyfrowane podczas przechowywania, a także podczas przesyłania do odbiorców w dobrej wierze.

Zasada dziesiąta: Niepowodzenie walidacji. Niepowodzenie sprawdzania poprawności danych w którejkolwiek z powyższych trzech faz musi spowodować wygenerowanie ostrzeżenia o błędzie na potrzeby dalszego badania. Alert musi być multimodalny, w tym wpisywać do dziennika błędów, alertu dźwiękowego, wiadomości e-mail i ewentualnie powiadomienia SMS do osób rozpoznających. Zawsze musi być więcej niż jedna osoba otrzymująca powiadomienia utworzone przez możliwe próby włamania.

Reguła jedenasta: Kontrola dostępu. Użytkownikom oprogramowania należy zapewnić poziom bezpieczeństwa dostępu, który spełnia - i nie przekracza - ich autoryzowanych potrzeb.

Zasada dwunasta: oprogramowanie antymalware. W celu uzyskania najnowszych informacji o atakach złośliwego oprogramowania należy często konsultować się z krajową bazą danych podatności. Oprogramowanie antymalware musi być zainstalowane zarówno na serwerze, jak i po stronie klienta. Na serwerze istnieją zasadniczo dwa rodzaje ataków. Pierwszym z nich jest atak Denial-of-Service, w którym serwer jest zalewany fałszywymi żądaniami mającymi na celu nasycenie jego pojemności i uniemożliwianie prawidłowego odwiedzania. Drugi to wstrzyknięcie SQL, w którym dostęp do serwera został naruszony, a baza danych serwera zawiera złośliwe oprogramowanie, które powoduje nielegalne działania. „Korzystając z tej metody, haker może przekazać dane wejściowe do aplikacji z nadzieją na uzyskanie nieautoryzowanego dostępu do bazy danych”.

Poniżej wymieniono dwa zestawy zasad, których celem jest zminimalizowanie ryzyka związanego ze sprzętem i oprogramowaniem systemów informatycznych

Reguły mające na celu minimalizację ryzyka w sprzęcie i oprogramowaniu systemów informatycznych

SPRZĘT : OPROGRAMOWANIE

1. Identyfikacje połączeń : 1. Zintegrowane zabezpieczenia

2. Ocena bezpieczeństwa : 2. Zorganizowany rozwój

3. Parametry dostawcy: 3. Zarządzanie projektem

4. Środki bezpieczeństwa : 4. Specyfikacje projektu

5. Wykrywanie włamań : 5. Planowanie projektu

6. Audyty : 6. Testowanie projektu

7. Blue Team : 7. Korzystanie z OOL

8. Opisy stanowisk : 8. Łata walutowa

9. Funkcje krytyczne : 9. Walidacja danych

10. Ciągłość działania : 10. Niepowodzenie walidacji

11. Zarządzanie konfiguracją : 11. Kontrola dostępu

12. Dogłębna obrona : 12. Antimalware

Ryzyko u ludzi

Aby skutecznie zacieśnić współpracę międzywydziałową, międzyorganizacyjną lub międzynarodową, dane muszą być dostępne dla różnych osób z różnych organizacji. Jednak według statystyk największym zagrożeniem dla bezpieczeństwa danych jest osoba upoważniona do dostępu do danych. Osoby z dostępem do wrażliwych danych lub wrażliwych usług z definicji stanowią luki w zabezpieczeniach. Takie luki w zabezpieczeniach wewnętrznych można podzielić na dwa typy. Pierwszy typ to osoby, które choć mają dostęp do poufnych informacji, zachowują się w sposób niedbały, ujawniając takie informacje osobom nieupoważnionym. Najczęściej dzieje się tak w postaci zagubionych telefonów komórkowych, zagubionych laptopów, odsłoniętych haseł, bezobsługowych terminali lub luźnych ust. Dzięki zastosowaniu technologii i odpowiednim szkoleniom podnoszącym świadomość w zakresie bezpieczeństwa cybernetycznego można zminimalizować ten rodzaj ryzyka. Drugi typ to ludzi, którzy choć mają dostęp do poufnych informacji, zdradzają to zaufanie i nadużywają przyznanego im autorytetu. Większość takich ingerencji jest wysoce skoncentrowana i ma na celu znaczne korzyści finansowe. Ponownie istnieją zasady, które można zastosować, które zminimalizują ryzyko związane z ludźmi. Sześć takich zasad może wyglądać następująco:

Zasada pierwsza: przyznawanie hasła. Autoryzacja dostępu za pomocą haseł lub innych mechanizmów bezpieczeństwa musi być udzielana tylko w razie potrzeby i przy minimalnej ilości danych i odstępie czasu. Podwyższone uprawnienia powinny mieć blokadę czasową, po której powinny zostać obniżone do poziomu nominalnego.

Zasada druga: utrzymanie hasła. Hasła muszą być ważne przez określony czas; ich odnowienie musi być bardzo odmienne od poprzednich i musi mieć złożoność proporcjonalną do znaczenia danych, które chroni.

Zasada trzecia: dostęp do dzienników. W zależności od poziomu ważności chronionych danych należy automatycznie utworzyć dzienniki z listą pieczęci dostępu (czas, terminal, użytkownik itp.). Alerty w czasie rzeczywistym muszą być generowane w przypadku nieautoryzowanych prób wykorzystania luk w zabezpieczeniach, nienormalnych działań oraz działań poza charakterem lub podejrzanych.

Zasada czwarta: technologia. Biorąc pod uwagę, że hasła mogą zostać utracone, co stwarza ryzyko i niedogodności, można stosować zaawansowane technologie, takie jak hasło jednorazowe. W jednym trybie tej technologii po otrzymaniu nazwy użytkownika serwer wysyła hasło do autoryzowanego telefonu komórkowego w postaci wiadomości SMS. Kod hasła dotyczy tylko komputera, który wysłał nazwę użytkownika i tylko przez skończoną liczbę sekund.

Zasada piąta: Monitorowanie odporne na manipulacje. Zabezpieczenia są tak dobre, jak integralność systemu monitorowania. Często intruzi neutralizują system monitorowania bezpieczeństwa przed przystąpieniem do ataku hakerskiego. Najlepiej byłoby, gdyby systemy nadzoru bezpieczeństwa były zautomatyzowane, generując alarmy o zagrożeniach w czasie rzeczywistym do natychmiastowego rozpatrzenia i podjęcia działań.

Zasada szósta: separacja. Wiele incydentów wewnętrznych szkód ma miejsce w przedziale czasowym między początkiem plotek o możliwym zwolnieniu pracownika a faktyczną datą takiego rozwiązania. Był czas, kiedy firmy przekazywałyby dwutygodniowe lub miesięczne wypowiedzenie. Jednak w latach siedemdziesiątych pojawiły się pierwsze niekorzystne konsekwencje. Zachowanie pracowników uległo zmianie. Było wiele incydentów, w których po powiadomieniu o wypowiedzeniu pracownik dosłownie zniszczył majątek firmy, zanim ostatecznie wyszedł. Zwolnienie pracownika z powodu, z podejrzenia o

przyczynę, z jakiegokolwiek powodu lub z jakiejkolwiek wymówki wymaga uczciwości, poufności, niepodważalnych faktów, profesjonalizmu, zdecydowania i uczciwości.

Ryzyko w laptopach

Biorąc pod uwagę, że liczba kradzieży laptopów rośnie, należy zawsze używać środków zaradczych. Laptopy i notebooki stały się stałymi towarzyszami, a ich ekspozycja lub utrata w większości przypadków mogą być katastrofalne. Jako minimalną ochronę można zainstalować pełne szyfrowanie dysku, które normalnie szyfruje wszystko na dysku twardym oprócz Master Boot Record (MBR). Szyfrowanie całego dysku może być obsługiwane przy użyciu odpowiednich zewnętrznych urządzeń sprzętowych. Szyfrowanie całego dysku nie może chronić, gdy komputer zostanie pozostawiony bez nadzoru po uruchomieniu. Jednak technologie zbliżeniowe mogą ci pomóc, a urządzenie w kieszeni ostrzega cię, jeśli jesteś oddzielony od chronionej jednostki na pewną niewielką odległość. Tabela przedstawia niewyłączną listę porad, które mogą zminimalizować naruszenia bezpieczeństwa związane z laptopami.

Środki zaradcze dotyczące bezpieczeństwa laptopa

1. Filtry ekranu prywatności. Takie filtry umożliwiają tylko bezpośrednie oglądanie, blokując widzów bocznych.

2. Śledzenie i odzyskiwanie laptopa. Jest to usługa świadczona w połączeniu z oprogramowaniem wbudowanym.

3. Blokada zbliżeniowa Bluetooth. Ta metoda zabezpieczenia danych laptopa blokuje laptopa, jeśli powiązane urządzenie Bluetooth pozostawi określoną odległość od laptopa.

4. Alarm zbliżeniowy RFID. Para urządzeń RFID wyemituje alarm, jeśli odległość między nimi przekroczy ustaloną wartość.

5. Szyfrowanie plików. Szyfruj poufne pliki, najlepiej wszystkie pliki.

6. Testowanie siły hasła. Użyj silnego hasła, aby zabezpieczyć laptopa. Sprawdź swoją siłę, korzystając z dostępnych stron testowych.

7. Kopia zapasowa na żywo. Pliki z laptopów są archiwizowane na bieżąco.

Ryzyko w cyberprzestrzeni

Przy zagrożeniach pochodzących z cyberprzestrzeni komputer osobisty stanowi pierwszą linię obrony. Dlatego konieczne są rygorystyczne środki bezpieczeństwa utrzymywane w celu skutecznej ochrony zasobów cyfrowych. Poniższe zasady mogą służyć jako minimalna ochrona przed złośliwym oprogramowaniem.

Zasada pierwsza: zaktualizowane oprogramowanie. Twórcy oprogramowania zapewniają na bieżąco aktualizowane wersje swojego oprogramowania, które zawierają silniejszą ochronę przed złośliwym oprogramowaniem. Dotyczy to zarówno systemów operacyjnych, jak i aplikacji. Może to być dodatkowy wydatek, ale utrzymanie najnowszej wersji zainstalowanego oprogramowania jest opłacalne na dłuższą metę.

Zasada druga: minimalizuj treść. Zminimalizuj ilość wrażliwych treści przechowywanych na laptopie lub notebooku, przechowując wrażliwe pliki na serwerze dostępnym w Internecie i zaszyfrowane.

Zasada trzecia: konto administratora. Ponieważ jesteś jedynym użytkownikiem, nie bądź jednocześnie administratorem. Komputer nienadzorowany w trybie administratora jest całkowicie niechroniony.

„Uprzywilejowanego konta administratora należy używać wyłącznie do instalowania aktualizacji lub oprogramowania oraz do ponownej konfiguracji hosta w razie potrzeby.

Zasada czwarta: zgodność. Przestrzeganie przepisów lub zasad zgodności, takich jak FISMA dla agencji federalnych, jest obowiązkowym i minimalnym zadaniem w zakresie ochrony danych

Zagrożenia w starszej infrastrukturze

Przejście na nową technologię może być bardzo kosztowne, zwłaszcza gdy obecnie stosowana technologia nie jest jeszcze zamortyzowana. Tak więc organizacje trzymają się starej infrastruktury IT, wahając się przed umieszczeniem ciężko zarobionej gotówki w najnowocześniejszej technologii. W tym momencie można zapytać, co jest „stare"? Niestety w świecie IT zwykle pięć lat to emerytury. Utrzymanie i utrzymanie starszej infrastruktury IT może być bardzo kosztowne, jak wskazano w ostatnim raporcie Urzędu ds. Odpowiedzialności Rządu Stanów Zjednoczonych (GAO). Sytuacja w sektorze prywatnym nie jest lepsza, jak wskazuje inny raport , w którym prowadzi bankowość. Zazwyczaj starsza infrastruktura IT ma sprzęt którego:

• Nie można łatać

• Dla którego nie ma aktualizacji

• Które są nadmiernie dostosowane

• Brakuje wykwalifikowanych techników

• Wymaga to wyższych składek na ubezpieczenia cybernetyczne

W skrócie: „… starsza technologia jest zarówno kwestią bezpieczeństwa, jak i przeszkodą dla innowacji…", jak stwierdził urzędnik FCC . Przeciwko temu na tle mroku znajdują się nowoczesne technologie informatyczne, które zapewniają bezpieczeństwo, elastyczność, automatyzację i inteligencję. Technologie te obejmują przechowywanie w chmurze i, co najważniejsze, przetwarzanie w chmurze, urządzenia mobilne z mocą komputera stacjonarnego oraz nadchodzący Internet-of-Things (IoT). Te nowe technologie z wieloma wbudowanymi funkcjami, takimi jak uwierzytelnianie, szyfrowanie, zgodność z mechanizmami polityki i raportowanie, są zdecydowanie najbardziej opłacalne i mają do pomocy wielu wykwalifikowanych specjalistów.

Zagrożenia w telefonii komórkowej

W ciągu kilku krótkich lat bałagan na biurku zmieścił się w naszej dłoni. Nie potrzebujemy już komputera z procesorem, monitorem, klawiaturą i myszą. Nie wymagamy też urządzeń pomocniczych, takich jak telefon, książka adresowa, kalendarz czy przypomnienia wysyłane wszędzie. Nawet zdjęcie naszej ulubionej osoby nie jest już oprawione. Dziś wszystkie powyższe funkcje są uporządkowane i wygodnie umieszczone w bardzo ergonomicznym urządzeniu zwanym smartfonem, które stało się integralną częścią naszego istnienia. Funkcje smartfonów zazwyczaj obejmują

• Telefonia GSM

• Sieć osobista — Bluetooth

• Sieć lokalna — WiFi

• Sieć rozległa - Internet

• Dodatkowy interfejs bezprzewodowy - podczerwień

• Liczne interfejsy fizyczne - karty SD, USB, HDMI itp.

Ponadto urządzenia te są praktycznie bezpłatne, biorąc pod uwagę ich ofertę. Smartfon to nowoczesna skrzynia skarbów, którą należy chronić przed cyberprzestępczością, która rozwija się równolegle z ewolucją Internetu. Można wymienić następujące filary bezpieczeństwa smartfonów

• Dostępność - smartfon musi być dostępny 24/7, ponieważ w rzeczywistości jest integralną częścią nas, podobnie jak nasz mózg.

• Integralność - musi dostarczać poprawnych i dokładnych informacji w oparciu o liczne stale instalowane aplikacje.

• Poufność - smartfon musi chronić naszą prywatność za pomocą niezawodnych środków bezpieczeństwa.

• Autentyczność - w przypadku korzystania z naszych transakcji musimy być niezawodnie rozpoznawani.

• Niezaprzeczalność - I wreszcie, jesteśmy zobowiązani do pewnych działań, za pośrednictwem komunikacji ze smartfonem, żadna ze stron nie powinna później zaprzeczyć takiemu zobowiązaniu.

Aby zabezpieczyć powyższe pięć filarów bezpieczeństwa smartfonów, należy wprowadzić odpowiednie środki i je zastosować. Niektóre z tych środków są

• Instalacja oprogramowania antywirusowego

Na szczęście istnieje wiele niezawodnych programów anty-malware, które mogą zapewnić ochronę do pewnego stopnia. Należy je jednak zaktualizować w miarę udostępniania nowych wersji. To samo dotyczy wszystkich instalacji. Aktualizacje oferują więcej funkcji, często w tym środki bezpieczeństwa.

• Opcja zdalnego czyszczenia

Jest to możliwość całkowitego lub selektywnego czyszczenia przez Internet plików lub fragmentów danych znajdujących się w smartfonie.

• Korzystanie z bezpiecznych haseł

Konieczne jest, aby w przypadku zgubienia smartfona jego zawartość będzie niedostępna.

• Enterprise Mobile Device Management (MDM)

Biorąc pod uwagę, że organizacje wydają członkom smartfony do użytku biznesowego, musi istnieć polityka użytkowania, w tym monitorowanie aplikacji zainstalowanych na każdym urządzeniu.

• Magazyn zdalny

Cała zawartość smartfona musi być regularnie powielana w pamięci innej niż mobilna. W ten sposób w żadnym wypadku nie grozi katastrofa.

• Korzystanie z wirtualnej sieci prywatnej (VPN)

VPN to technologia sieciowa, w której ruch internetowy urządzenia przechodzi przez węzeł, który służy jako bufor między urządzeniem a resztą Internetu.

• Użyj szyfrowania wiadomości e-mail

Wszystkie aplikacje e-mail zawierają szyfrowanie wiadomości e-mail, dzięki czemu błędny adresat nie będzie mógł odczytać treści wiadomości e-mail.

• Zgłoś utratę lub kradzież

W przypadku utraty lub kradzieży urządzenia z dostępem do Internetu, natychmiast zgłoś to swojemu usługodawcy. Upewnij się, że istnieje baza danych zagubionych lub skradzionych urządzeń z dostępem do Internetu, która uniemożliwia ich późniejsze użycie.

• Minimalizuj ekspozycję

Wyłącz aplikację i / lub opcję, której nie używasz, i usuń niepotrzebne pliki. Ponadto, gdy nie jest to potrzebne, wyłącz funkcje bezprzewodowe, takie jak Bluetooth i podczerwień (IR).

• Ufaj ale sprawdzaj

W Internecie dostępnych jest wiele aplikacji na smartfony. Niektóre aplikacje są nawet darmowe, oferując „fantastyczne" funkcje. Przed ich użyciem przeprowadź je przez niezawodne oprogramowanie antywirusowe. Niektóre rzeczywiście mogą być świetne w tej cenie, ale być może zbierają autoryzacje kart kredytowych w celu późniejszego nadużycia.

• Bez łamania więzienia

W żargonie internetowym oznacza to, że nie należy manipulować fabrycznymi ustawieniami zabezpieczeń urządzenia mobilnego.

• Użyj funkcji automatycznego blokowania

Gdy urządzenie mobilne jest nieaktywne przez X minut, ponowna aktywacja musi wymagać ponownego wprowadzenia hasła. W ten sposób unika się szpiegowania przez oprogramowanie szpiegujące.

• Unikaj fałszowania

Korzystając z niezabezpieczonej publicznej sieci Wi-Fi, możliwe jest, że Twoje dane zostaną skopiowane z powietrza. Przeprowadzaj poufne transakcje tylko w bezpiecznych środowiskach Wi-Fi.

• Smartfony są prywatne

Prawdą jest, że celem smartfona jest, abyśmy byli osiągalni. Jednak numery telefonów smartfonów muszą być prywatne, aby uniknąć „zeskanowania" i nielegalnego dostępu do zawartości telefonu. Nie ma więc publicznego publikowania numerów smartfonów. W razie potrzeby przygotuj niezbyt inteligentny system komunikacji publicznej.

• Last but not least - szkolenie

Użytkownicy smartfonów muszą skorzystać z każdej okazji, aby zapoznać się z najnowszymi środkami cyberobrony i najnowszymi typami cyberataków. Z czasem smartfony wejdą w każdy aspekt naszego życia prywatnego i zawodowego, wymagając uczenia się przez całe życie w zakresie cyberbezpieczeństwa.

Ubezpieczenie ryzyka w cyberprzestrzeni

Podobnie jak w przypadku zagrożeń w świecie fizycznym, ryzyko w cyberprzestrzeni może być podobnie przeniesione na firmy ubezpieczeniowe, których wyłączną działalnością jest kupowanie ryzyka. Od 1995 r., kiedy Internet został zaakceptowany jako platforma rynku elektronicznego, pojawiły się obawy dotyczące zabezpieczenia potencjalnych strat spowodowanych niekorzystnymi zdarzeniami w cyberprzestrzeni, takimi jak kradzież informacji, wandalizm i odmowa usługi. Przedsiębiorstwa inwestujące w handel elektroniczny są zaniepokojone możliwymi stratami, jeśli ich

strona internetowa przestanie działać z jakiegokolwiek powodu, na który nie mają wpływu. Witryna może zostać wyłączona z wielu powodów, a mimowolne przerwy w działalności biznesowej są tradycyjnie problemem ubezpieczalnym. Przedsiębiorstwa często wolą kupować ubezpieczenie od ryzyka niż wdrażać kosztowne środki ochrony. Coraz większe możliwości przestoju z powodu problemów technicznych lub bezpieczeństwa sprawiają, że cyberbezpieczeństwo stanowi dla cyberprzestrzeni opcję zabezpieczenia się przed ryzykiem. Organizacja może, dzięki wykorzystaniu ubezpieczenia cybernetycznego, zminimalizować straty spowodowane niekorzystnymi incydentami cybernetycznymi. Cyberataki mogą powodować przestoje systemu, uszkodzenie danych, utratę działalności, a także utratę reputacji. Składki na ubezpieczenie cybernetyczne opierają się nie tyle na oczekiwanych odszkodowaniach, co na postawie cyberobrony organizacji. Oznacza to, że składki na ubezpieczenia cybernetyczne są oparte na środkach i praktykach cyberbezpieczeństwa organizacji. Zazwyczaj polisy ubezpieczeniowe cyberbezpieczeństwa obejmują

• Utrata aktywów cyfrowych

• Koszty przerwania działalności

• Zagrożenie wymuszeniem cybernetycznym

• Koszty zdarzeń związanych z bezpieczeństwem

• Bezpieczeństwo sieci i ochrona prywatności

• Ochrona prywatności pracownika

• Zakres odpowiedzialności za media elektroniczne

• Ochrona przed cyberterroryzmem

Nowością w ubezpieczeniach od ryzyka cybernetycznego jest to, że nie ma sprawdzonej metodologii obliczania ryzyka w celu późniejszego oszacowania odszkodowania, a na koniec obliczenia odpowiedniej składki ubezpieczeniowej. Oznacza to, że rynek cyberbezpieczeństwa nie ma historii, z której można czerpać statystyki, a „firmy ubezpieczeniowe zdają sobie sprawę z potrzeby wdrożenia większych możliwości oceny ,podczas rozpatrywania wniosku organizacji o objęcie ubezpieczeniem". Jednak wiele firm ubezpieczeniowych oferuje polisy ubezpieczeniowe w zakresie dziewięciu cyfr. Firmy ubezpieczeniowe podjęły wysiłki w celu określenia skończonych parametrów, które można określić ilościowo, aby służyły jako współczynniki w ocenie ryzyka cybernetycznego. Zazwyczaj równanie ubezpieczenia od ryzyka cybernetycznego obejmuje następujące parametry:

• Możliwość niekorzystnej selekcji.

• Silne środki bezpieczeństwa na miejscu

• Kwalifikacje personelu ds. Bezpieczeństwa danych

• Wartość pieniężna chronionych aktywów

• Poziom pokusy nadużycia.

Niekorzystny wybór to termin w terminologii ubezpieczeniowej, który opisuje istnienie ukrytych niekorzystnych warunków wstępnych znanych tylko ubezpieczonemu. Są to warunki wstępne, które nie są ujawniane firmie ubezpieczeniowej. Aby przeciwdziałać temu ryzyku, firmy ubezpieczeniowe chcą, aby polisa miała określony początkowy okres bezskuteczny i / lub znaczny koszt uzyskania przychodu. Moralne zagrożenie jest terminem również w terminologii ubezpieczeniowej, która opisuje obojętność ubezpieczonego na ryzyko. Aby przeciwdziałać temu ryzyku, firmy ubezpieczeniowe chcą

włączyć odliczenie, które zmotywuje ubezpieczonego do podjęcia niezbędnych środków ostrożności w stosunku do ryzyka. Firmy ubezpieczeniowe próbują oszacować związane z tym ryzyko, szkicując profil firmy wnioskodawcy poprzez ocenę różnych powiązanych dokumentów wewnętrznych. Tabela zawiera listę niektórych wymaganych dokumentów. Bez wątpienia przegląd powyższej listy dokumentów może dać bardzo wyraźny obraz postawy podatności firmy na zagrożenia. Wskazuje również wymagane dokumenty do samooceny bezpieczeństwa w firmie. Firmy narażone na cyberprzestrzeń mogą obniżyć poziom ryzyka cybernetycznego do akceptowalnego, stosując własne środki wraz z cyberbezpieczeństwem. Poniższe kroki pokazują związek niechronionego surowego ryzyka z chronionym dopuszczalnym ryzykiem.

Możliwe załączniki do wniosku o ubezpieczenie cybernetyczne

1. Dowód zgodności z ISO 17799 [19]

2. Życiorys dyrektora ds. bezpieczeństwa informacji

3. Plan ochrony antywirusowej

4. Konfiguracja infrastruktury zapory

5. Plan wykrywania i reagowania na incydenty

6. Plan aktualizacji oprogramowania

7. Biznesowy plan naprawy

8. Polityka prywatności firmy

9. Korporacyjna polityka zgodności

10. Polityka bezpieczeństwa danych korporacyjnych

11. Podręcznik bezpieczeństwa korporacyjnego

12. Korporacyjna siatka dostępu do danych pracowników

13. Certyfikaty bezpieczeństwa i prywatności

14. Skargi przeciwko firmie

15. Raporty o przeszłych naruszeniach bezpieczeństwa

16. Umowy z partnerami dotyczące przetwarzania danych osobowych

Krok pierwszy: ocena surowego ryzyka, RR. Jest to ryzyko organizacji która jest narażona, gdy nie ma żadnych środków zaradczych.

Krok drugi: ocena chronionego ryzyka, PR = RR × CM. Jest to nowe ryzyko, które zostało zmniejszone dzięki zastosowaniu wewnętrznych środków zaradczych, CM.

Krok trzeci: Ocena polis ubezpieczenia cybernetycznego i planów ochrony.

Krok czwarty: wybór odpowiedniego cyberbezpieczeństwa, IK, polisy i planu.

Krok piąty: dopuszczalne ryzyko, AR = CI × PR. Jest to ryzyko, na jakie narażona jest organizacja po wykupieniu wybranej polisy i planu cyberbezpieczeństwa.

Ubezpieczenie od ryzyka cybernetycznego jest zwykle kompleksową polisą korporacyjną obejmującą szeroki zakres ubezpieczeń, w tym pozycje wymienione poniżej

Kompleksowa polisa ubezpieczenia korporacyjnego - typowy zakres ubezpieczenia

1. Przerwanie działalności gospodarczej
2. Odpowiedzialność zawodowa
3. Odpowiedzialność za praktyki zatrudnienia
4. Odpowiedzialność dyrektorów i funkcjonariuszy
5. Ubezpieczenie na życie kluczowej osoby
6. Przemoc w miejscu pracy
7. Własność intelektualna

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.

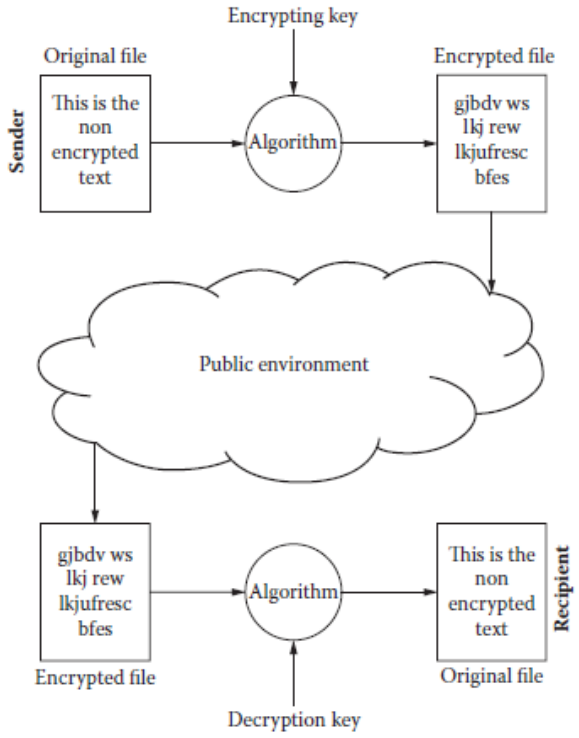
• Wszystkie pliki muszą mieć cykl życia - datę utworzenia, datę modyfikacji i datę wycofania. W pewnym momencie status ich znaczenia może ulec zmianie z aktywnej na usunięty lub do zarchiwizowania.

• 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

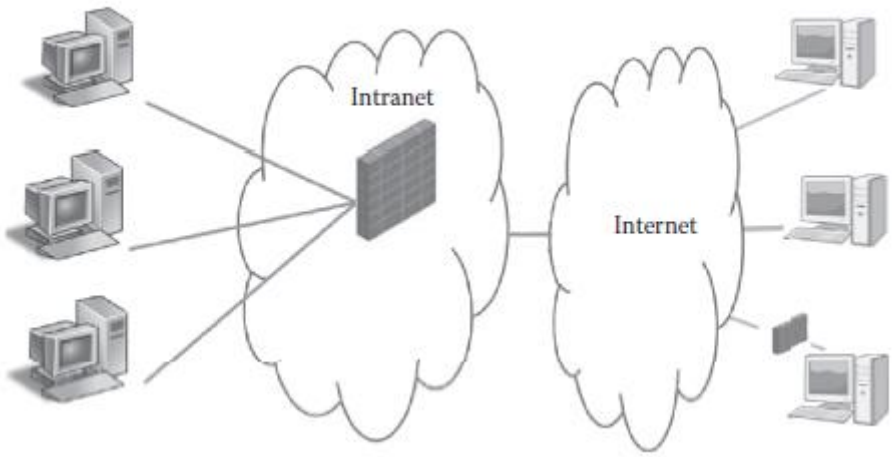
Dostęp lub transfer informacji cyfrowych stanowi lukę, narażając informacje na ryzyko. Takie ryzyko można jednak zminimalizować jeśli zastosowane zostaną odpowiednie środki ostrożności. Te środki ostrożności obejmują szyfrowanie, zapory ogniowe, certyfikaty cyfrowe, podpisy cyfrowe i kontrolę logowania.

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.

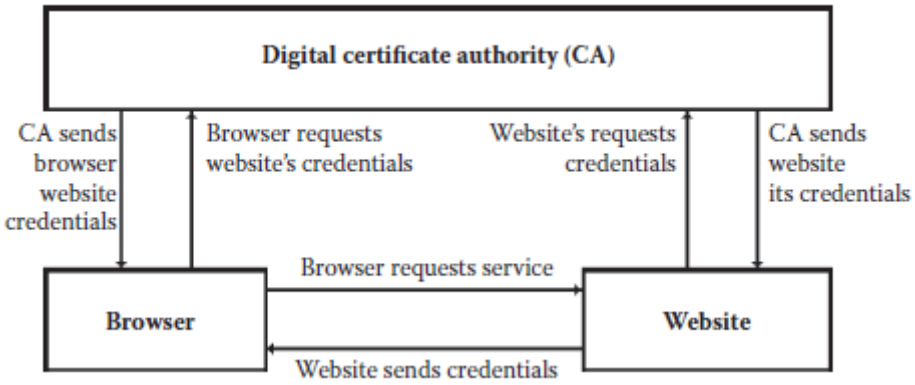


Zapory ogniowe: Zapory ogniowe są podstawą bezpieczeństwa danych. Ich fizyczną postacią może być oprogramowanie lub oprogramowanie zainstalowane na dedykowanym sprzęcie. Zapory ogniowe

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.

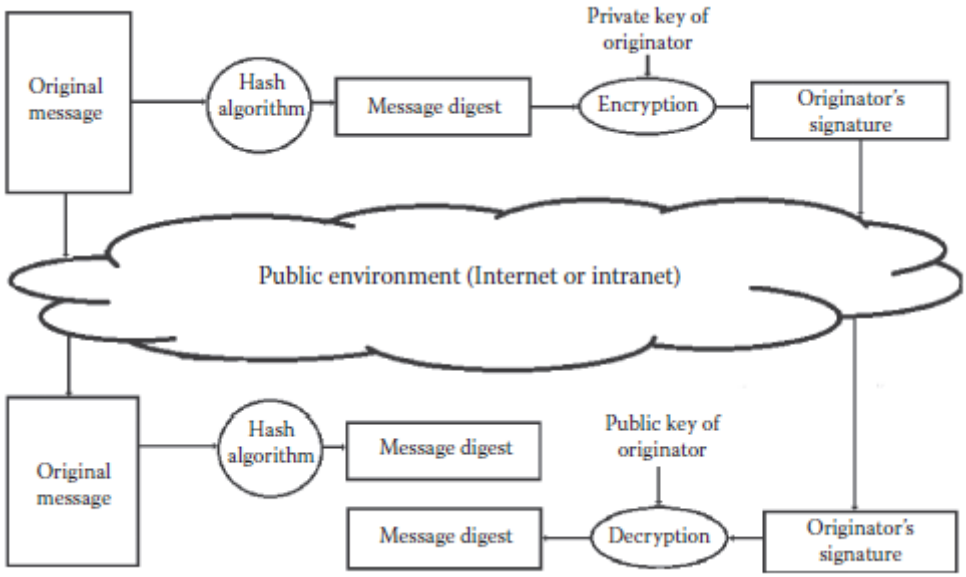


Certyfikaty cyfrowe : Certyfikat cyfrowy, znany również jako certyfikat klucza publicznego lub certyfikat tożsamości, służy do cyberprzestrzeni, czym jest karta kredytowa do handlu. W przypadku karty kredytowej strona trzecia, czyli firma wydająca kartę kredytową, potwierdza jakość karty. Na tej podstawie 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

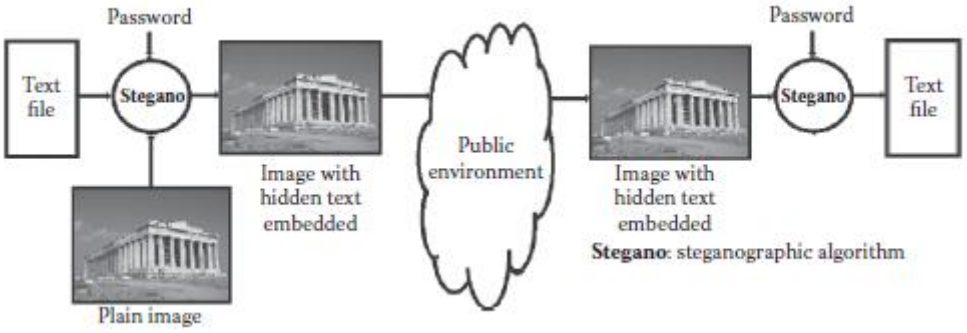
binarny, a na końcu tworzona jest krótka sekwencja liczbowa - ciąg znaków. Ze względów praktycznych ciąg ten jest unikalny dla tego pliku w kontekście tego algorytmu. Sekwencja, która może różnić się długością od 32 do 512 bitów, służy jako weryfikator autentyczności dołączonego pliku. Rysunek ilustruje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

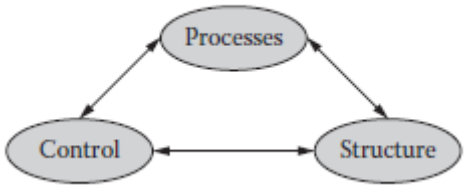
• Spamowa wiadomość e-mail może zawierać aktywne złośliwe oprogramowanie w opcji anulowania subskrypcji.

• 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

Cyberbezpieczeństwo i CIO

Cyberbezpieczeństwo jest integralną częścią każdej koncepcji bezpieczeństwa korporacyjnego lub krajowego.

Wprowadzenie

Z czasem zmienia się pozycja najbardziej krytycznej osoby w przedsiębiorstwie. Dzisiaj tą najbardziej krytyczną osobą jest Chief Information Officer (CIO). Na tym samym poziomie, powyżej lub poniżej, lub ta sama osoba jest Dyrektorem ds. Technologii (CTO) i dyrektorem ds. Bezpieczeństwa informacji (CISO) w przedsiębiorstwie. Dla wszystkich praktycznych celów rozważymy CIO jako trzy w jednym. Będąc wszystkimi trzema, oczekuje się, że CIO będzie wizjonerem organizacji, doradzającym w jaki sposób wykorzystać technologię do osiągnięcia celów organizacji. CIO jest odpowiedzialny za każdy aspekt informacji w przedsiębiorstwie.

Rolę CIO w organizacji można opisać następująco:

• Członek wyższego szczebla zespołu administracyjnego / zarządzającego / planowania

• Kierownik technologii i innych zasobów informacyjnych

• Odpowiada za planowanie IT

• Odpowiedzialny za rozwój nowych systemów

• Odpowiada za opracowanie i wdrożenie polityki

Pozycja CIO wymaga pewnego spektrum osobowości, wykształcenia i doświadczenia danej osoby.

Cyberprzestrzeń to labirynt nieskończonych luk w zabezpieczeniach, których istnienie jest zwykle wykrywane przez atakujących kosztem, przynajmniej dla pierwszej ofiary. Rolą CIO jest znajomość wszystkich mechanizmów ochronnych i zdolność do opracowywania większej liczby w razie potrzeby. Można mieć na to nadzieję, jeśli dyrektorzy IT wejdą na swoje stanowisko z dużym doświadczeniem i specjalistyczną wiedzą oraz ze świadomością, że stanowisko CIO jest pracą przez całe życie.

CIO: osobowość

Spotkajmy się z CIO i zobaczmy, jakie kwalifikacje i ścieżka kariery doprowadziły tę osobę na to stanowisko.Oto kwalifikacje osobiste i zawodowe, których CIO musi potrzebować, aby skutecznie sprostać wymaganiom stanowiska.

Zaufanie i etyka

Jedną z najbardziej zaufanych pozycji w dzisiejszym przedsiębiorstwie jest stanowisko CIO. CIO jest ochroniarzem informacji organizacji. CIO musi być pewny siebie i promieniować zaufaniem i sukcesem. Zaufanie to cecha osobista, często wyczuwana podświadomie, która sprawia, że człowiek jest mile widziany w każdym otoczeniu. Szacunek dla siebie, innych, organizacji i społeczeństwa jest fundamentem zaufania. Pewność siebie i promieniowanie sukcesu są osiągane tylko poprzez szereg wcześniejszych sukcesów, małych i prawdopodobnie dużych. Nie ma absolutnie żadnego substytutu dla konsekwentnego zachowania etycznego. Będą istnieć ciągłe naciski lub satysfakcjonujące okazje do bycia nieetycznymi. Jednak CIO musi stać ponad tymi pokusami, nie podejmować ryzyka, a ponadto powstrzymywać chciwość innych, którzy sugerują skróty do prostej linii etyki.

Komunikacja i inteligencja

CIO musi być świetnym komunikatorem w organizacji. Jest to osoba, która będzie musiała przekonać innych do zdobycia zasobów, gdzie słowo zasoby nie pozostawia nic na zewnątrz. Dyrektor IT może potrzebować kapitału na nową technologię lub może potrzebować lojalności i zaufania współpracowników we wszystkich kierunkach hierarchii. Perswazja jest potrzebna do komunikacji w górę, a motywacji i inspiracji do komunikacji w dół. We współczesnej organizacji nic nie osiąga się za pomocą żelaznych pięści. CIO musi uchwycić umysł i serca wszystkich w przedsiębiorstwie, zawsze pamiętając, że język „techniczny" może być nudny dla nietechnicznych. Poza organizacją CIO dołącza do odpowiednich stowarzyszeń, bierze udział w forach, bierze udział w konferencjach i prowadzi seminaria, zyskując w ten sposób widoczność i najważniejsze umiejętności polerowania. Nie możemy wykluczyć natury z obrazu CIO. Naturalna inteligencja jest algorytmem, który przekształca obserwacje w wiedzę, a wiedza w mądrość. Mądrość połączona z doświadczeniem zwykle powoduje zdrowy osąd. Jak mówi przysłowie: mądrzy ludzie uczą się na własnych błędach, podczas gdy mądrzy ludzie uczą się na błędach innych.

Przywództwo i przedsiębiorczość

Niektórzy twierdzą, że rodzi się lider; inni uważają, że można stworzyć lidera. CIO jako lider musi znajdować się powyżej poziomu obserwujących. Ta wyższość, w pełnym tego słowa znaczeniu, musi mieć zarówno cechy osobiste, jak i umiejętności techniczne. CIO jako lider, idący korytarzami przedsiębiorstwa, jak to się mówi, musi być postrzeganym jako przewodnik z boku, a nie jako mędrzec na scenie. Aby otrzymać CIO w ten sposób, osoba ta musi być bardzo pokorna, bardzo kompetentna i doświadczona. Wszyscy w organizacji chcą zobaczyć przyjaciela w osobie CIO. Wynika to z faktu, że CIO jest wspaniałym strażnikiem, obdarzonym autorytetem, który, miejmy nadzieję, pasuje do odpowiedzialności nałożonej na ramiona tej osoby. CIO i kierownictwo przedsiębiorstwa muszą zdać sobie sprawę, że CIO jest strategiczną pozycją, która wyznacza kierunek, a CIO nie powinien być uwikłany w problemy techniczne niskiego poziomu. Jednak CIO musi mieć doświadczenie, aby wskazać kierunek rozwiązania problemów.

Dyrektor ds. Informatyki zawsze szuka okazji do poprawy pozycji biznesowej organizacji, chętny do podjęcia niekatastroficznego ryzyka. Dyrektor ds. Informatyki musi być wizjonerem , który może podważyć konwencjonalną mądrość", w stylu nadzoru, który jest dobrze wyważony między przyznaniem autonomii a stosowaniem kontroli.

Odwaga i ograniczenia

Dyrektorzy IT z powyższymi kwalifikacjami muszą być w stanie przewidzieć wykonalność proponowanego pomysłu i muszą mieć niezbędną odwagę wynikającą z bezpieczeństwa pracy i wsparcia wyższej kadry kierowniczej, aby móc swobodnie i obiektywnie wyrażać swoje opinie. Podobnie CIO powinien być w stanie porzucić projekt, który wydaje się zmierzać w złym kierunku. Przy nieprzewidywalnych postępach technologicznych dobre pomysły mogą nie być tak dobre, ponieważ nowe rozwiązania są stale dostępne. CIO, oprócz rozpoznania ograniczeń technologicznych, powinni przede wszystkim rozpoznać własne ograniczenia, czy to ludzkie, czy techniczne. Sukces CIO jest jak wchodzenie po schodach, trzeba to robić krok po kroku. Tam nie jest to plac zabaw. Bycie CIO jest misją, a nie przyjemnym zajęciem. CIO jest integralną i najbardziej krytyczną częścią przedsiębiorstwa. CIO musi mieć romans z technologią. Miliony inżynierów na całym świecie produkują nowe technologie lub nowe złośliwe oprogramowanie, a CIO nigdy nie może powiedzieć „nie wiem". Dyrektor IT może tylko powiedzieć: „W tej chwili nie wiem, ale za 48 godzin będę miał wyedukowaną opinię na ten temat".

CIO: Edukacja

Stopnie naukowe

CIO musi posiadać wykształcenie wyższe wskazujące na wykształcenie w zakresie systemów informatycznych. Stopień (stopnie) musi zawierać słowo komputer lub informacja, podczas gdy odpowiedni program nauczania musi obejmować kursy, które rozpoczęły się liczbami binarnymi i bramkami logicznymi, a zakończyły kursami zwieńczenia, które rozwinęły się w sieci. Oczekuje się, że dyrektor ds. Informatycznych będzie miał wyższe wykształcenie techniczne. Wiele uniwersytetów oferuje obecnie tytuły MBA w systemach informatycznych, które najlepiej przygotowują kandydatów na stanowisko CIO.

Certyfikaty

Poza oczekiwanym wykształceniem wyższym, CIO musi mieć certyfikaty, które pokazują walutę technologiczną. W zależności od ścieżki kariery, jaką podjął się CIO w zawodzie systemów informatycznych, oczekuje się, że na takie stanowisko będą posiadać aktualne powiązane certyfikaty. Podczas gdy stopnie uniwersyteckie sugerują szeroką wiedzę na dany temat, certyfikacja potwierdza wiedzę specjalistyczną w określonym sektorze technologii.

Ustawiczne kształcenie i nabywanie umiejętności

Korzyści płynące z tworzenia cyberprzestrzeni na świecie mają niespotykane dotąd rozmiary. Wraz z tym pojawiła się straszna zależność. Awarie internetowe przypadkowe lub złośliwe mogą spowodować niezmierzone szkody. W związku z tym przywódcy muszą mieć świadomość tej słodko-gorzkiej sytuacji. Cyberprzestrzeń stała się infrastrukturą, na której praktycznie opiera się każde działanie. Zależność ta waha się od smartfonów po zautomatyzowaną produkcję, z praktycznie każdą aktywnością człowieka pomiędzy. Nasze absolutne poleganie na cyberprzestrzeni wymaga, aby liderzy byli stale edukowani w zakresie postępów i zagrożeń, jakie Internet przynosi światu. Taka edukacja pomoże liderom zidentyfikować i zminimalizować ryzyko cybernetyczne, przygotowując społeczeństwo na nadchodzące wydarzenia , korzyści i obawy. Cyberbezpieczeństwo niewątpliwie przejmie prowadzenie, ale świadomość bezpieczeństwa cybernetycznego dla wszystkich jest niezbędna jako prawo jazdy. Wiele narodów uznało potrzebę edukacji w cyberprzestrzeni, planując odpowiednie programy edukacyjne, koncentrując się na trzech celach . Mianowicie, do

1. Zwiększenie świadomości krajowej na temat zagrożeń związanych z cyberprzestrzenią.

2. Zwiększenie grona specjalistów ds. Bezpieczeństwa cybernetycznego.

3. Utwórz globalnie współpracujące siły cyberbezpieczeństwa.

CIO: Doświadczenie

CIO musiał osiągnąć pozycję w szeregach. Sama edukacja tego nie zrobi. Oznacza to, że dana osoba musiała przez wiele lat służyć w branży IT w znaczący sposób. Być może osoba ta zaczynała jako inżynier projektu lub programista, a następnie została analitykiem, a kilka lat później przełożonym pierwszego stopnia i tak dalej. Równolegle przyszły dyrektor ds. Informatycznych poszerzał wiedzę o powiązanych kursach, seminariach i, miejmy nadzieję, uzyskał po drodze kilka certyfikatów. Mając około dziesięć do piętnastu lat doświadczenia i mając pewność co do już nabytych kwalifikacji w dziedzinie IT, przyszły CIO wkracza na rynek, próbując wody. Reszta to kwestia dopasowania nabytych umiejętności miękkich i twardych do prezentowanych możliwości. Średnio około dwunastu lat od ukończenia college'u może dostać się na stanowisko CIO, w zależności od wielkości organizacji i tego, czy karty doświadczenia i edukacji są właściwie grane. Podczas planowania kariery przyszły CIO musi pamiętać, że „rekruterzy szukają sprawdzonych historii sukcesu, a nie ludzi, którzy mogą odnieść sukces”

CIO: Obowiązki

Z czasem IT ewoluowało jako integralny i niezbędny uczestnik każdej organizacji, a potrzeba centralnej postaci, CIO, stała się oczywista. W 1996 r. osiągnął punkt, w którym w Stanach Zjednoczonych uchwalono ustawę federalną, która obejmowała nawet obowiązki CIO w różnych departamentach rządu. Określanie priorytetów jest trudne. Oczywiste jest, że obowiązki CIO obejmują całe spektrum systemów informatycznych w organizacji. W efekcie CIO jest ministrem obrony organizacji. Inne obowiązki, które nie zostały wyraźnie określone w powyższym akcie, obejmują:

*Nabycie

*Zarządzanie wydajnością i wynikami

*Architektura

*Polityka

*Ciągłości działania

*Udoskonalenie procesu

*Planowanie i inwestowanie kapitału

*Zarządzanie programem

*Relacje z klientem

*Zarządzanie ryzykiem

*Bezpieczeństwo innowacji

*Zarządzanie przywództwem

*Planowanie strategiczne

*Ocena technologii operacyjnej

Kopia zapasowa i archiwizacja danych

Dyrektor ds. Informatyki musi zaprojektować wdrożenie planów sporządzonych przez administratora danych organizacji w celu tworzenia kopii zapasowych danych operacyjnych w czasie rzeczywistym. Dzięki wprowadzeniu chmury jako możliwego miejsca docelowego kopii zapasowej, należy uwzględnić dodatkowe obawy dotyczące bezpieczeństwa z powodu niejasności co do dokładnej fizycznej lokalizacji danych.

Kultura bezpieczeństwa

Dyrektorzy IT jako dyrektorzy ds. Bezpieczeństwa informacji w organizacji ponoszą odpowiedzialność za stworzenie korporacyjnej kultury bezpieczeństwa, która posłuży jako podświadomy przewodnik w działaniach wszystkich. Podstawowymi elementami kultury bezpieczeństwa są z jednej strony świadomość istnienia zagrożeń i ich potencjalnej szkody dla organizacji, z drugiej zaś przestrzeganie zasad bezpieczeństwa. Tworzenie kultury bezpieczeństwa nie jest łatwe, ponieważ stwarza wiele niedogodności. Jednak dzięki programom szkoleniowym zrozumiałe będzie, że środki bezpieczeństwa są bardzo niską ceną, jaką należy zapłacić za to, że nie doszło do incydentów bezpieczeństwa o potencjalnie katastrofalnych skutkach. Podczas gdy faktyczny personel bezpieczeństwa CIO może być niewielki, wirtualny personel powinien obejmować każdego członka organizacji.

Szkolenie cybernetyczne

Biorąc pod uwagę, że technologia nieustannie się rozwija, szkolenie personelu IT organizacji będzie musiało być ciągłe. Dyrektor ds. Informatycznych musi mieć ścieżkę kariery dla każdego członka działu IT, a szkolenie przyczyni się do realizacji ścieżki kariery na żywo. Szkolenie może odbywać się wewnętrznie, zewnętrznie, osobiście lub online. Certyfikaty muszą stanowić integralną część filozofii szkolenia organizacji, a także szkolenia sprzedawców, tam gdzie ma to zastosowanie.

Plany awaryjne

Dyrektor ds. Informatycznych, we współpracy z kierownikami działów organizacji, opracowuje plany awaryjne na wypadek możliwie największej liczby niepożądanych zdarzeń. Dyrektor ds. Informatycznych przeszedł przez szeregi toru operacyjnego organizacji i może błędnie sądzić, że pozycja jest nadal na poziomie operacyjnym. To bardzo źle i niestety wielu CIO gubi się w szczegółach technicznych. Pozycja CIO to pozycja strategiczna, a CIO musi być wolny od kapelusza operacyjnego CIO. Aby to osiągnąć, CIO muszą się „sklonować". Oznacza to, że podobnie jak na statkach, na których pierwszy oficer prowadzi statek, a nie kapitan, CIO musi mieć pierwszego oficera, który zajmie się wszystkimi operacyjnymi aspektami informatycznymi organizacji. W ten sposób CIO będzie mógł skoncentrować się na roli strategicznej - śledzić postęp technologiczny, zabezpieczyć zasoby na potrzeby IT organizacji i upewnić się, że morale i zaufanie do kadry IT są wysokie.

Odpowiedzialność

Często zdarza się, że CIO mają ubezpieczenie od odpowiedzialności cywilnej, szczególnie jeśli pracują jako niezależni konsultanci. Istnieje wiele firm, które oferują taki zakres, często obejmujący zakres 5 mln USD

CIO: Bezpieczeństwo informacji

Istnieje wiele elementów bezpieczeństwa informacji. Najważniejsze, sklasyfikujemy jako wewnętrzne i zewnętrzne.

Wewnętrzne składniki bezpieczeństwa informacji

Kontrola dostępu - elektroniczna .Tutaj mamy trzy pytania: Kto? Co? W jaki sposób? Czasami dodaje się jeszcze jedno pytanie: Kiedy? Dzisiejsze systemy baz danych umożliwiają kontrolę dostępu aż do komórki arkusza kalkulacyjnego. Programowanie bezpieczeństwa do tego poziomu może być uciążliwe, ale są to opcje oferowane przez technologię i powinny być ważone względem znaczenia chronionych danych. Dostęp do danych można również blokować czasowo. Dane mogą być dostępne w godzinach pracy lub po konkretnym włączeniu. Ponieważ biometria wciąż nie jest głównym narzędziem kontroli dostępu, nazwa użytkownika i hasła pozostają dominującymi mechanizmami kontroli dostępu. Lukę w zabezpieczeniach hasłem można wyeliminować za pomocą uwierzytelniania dwuskładnikowego. Jest to technologia, w której po wprowadzeniu nazwy użytkownika serwer wysyła użytkownikowi jednorazowe hasło (OTP) za pośrednictwem względnie bezpiecznego medium, takiego jak e-mail lub SMS na telefon komórkowy użytkownika. Drugim czynnikiem uwierzytelnienia może być jedna z kilku opcji oprócz wyżej wymienionych. Może to być parametr biometryczny - odcisk palca lub próbka głosu - lub może to być urządzenie - bezprzewodowe lub USB - które za pośrednictwem komputera logowania wysyła do serwera rozpoznawalny i możliwy do zidentyfikowania kod.

Kontrola dostępu – fizyczna. W przedsiębiorstwie często ma to miejsce ,że dostęp jest przyznawany dla określonych obszarów obiektów. W takich przypadkach zamki szyfrowe lub urządzenia przesuwające karty umożliwiają autoryzowany dostęp. W pierwszym przypadku wadą jest możliwa

utrata lub kompromis kodu dostępu, podczas gdy w drugim przypadku wadą jest możliwa utrata samej karty. Praktycznym rozwiązaniem fizycznego dostępu mogą być mobilne blokady telefoniczne, w których tylko autoryzowane numery telefonów mogą odblokowywać i zapewniać dostęp. Takie technologie rejestrują także znacznik czasu interakcji i zapisują wszystkie nieautoryzowane próby wejścia.

Zasady cybernetyczne

Jednym z głównych obowiązków CIO jest opracowanie polityki bezpieczeństwa informacji organizacji. Ta polityka wyszczególnia reguły, na podstawie których informacje przemieszczają się w obrębie organizacji i od organizacji do innych zewnętrznych.

Cyber świadomość i szkolenie

Cyber świadomość „chroni cię dane osobowe ... i ... bezpieczeństwo twojego komputera ” . CIO promuje świadomość cyberbezpieczeństwa poprzez komunikację wewnętrzną, taką jak okazjonalne biuletyny e-mail i seminaria, podkreślając, że cyberbezpieczeństwo jest zbiorowym zadaniem i misją wewnątrz organizacji.

Cyber świadomość może być określona ilościowo za pomocą następującej listy porad:

• Zawsze miej zainstalowane niezawodne i samoaktualizujące się oprogramowanie antywirusowe.

• Zawsze używaj najnowszych wersji potrzebnego oprogramowania, w tym zainstalowanego systemu operacyjnego.

• Zainstaluj łatki, gdy tylko zostaną udostępnione.

• W środowisku Wi-Fi wyłącz transmisję SSID i zastosuj szyfrowanie WAP / WEP. Tam, gdzie to możliwe, zaprogramuj punkt dostępu do MAC dozwolonych komputerów.

• W sieciach społecznościowych zapoznaj się ze wszystkimi środkami bezpieczeństwa i ochrony prywatności i zastosuj je w celu zapewnienia maksymalnej ochrony. Nie publikuj poufnych informacji i niekompletnych zdjęć.

• Wysyłając poufne informacje, zaszyfruj je i wyślij odbiorcy hasło za pośrednictwem wspólnie uzgodnionego nośnika, takiego jak SMS, e-mail lub telefon.

• Przejrzyj opcje plików cookie w przeglądarce i wybierz tę, która będzie Ci odpowiadać w zależności od potrzeb związanych z surfowaniem. Co więcej, zaprogramuj przeglądarkę, aby wyświetlała monity przed zaakceptowaniem plików cookie.

• Zaprogramuj swoją przeglądarkę, aby automatycznie wyłączała się po X minutach bezczynności i aby usuwać tymczasowe pliki internetowe oraz ewentualnie historię i pliki cookie, jeśli to konieczne.

Trening

Szkolenia dotyczące świadomości cybernetycznej można znaleźć bezpłatnie i może zawierać następujące części:

-Wprowadzenie do Cyber Safety, obejmujące ustawienia bezpieczeństwa na komputerze osobistym i telefonie komórkowym, ustawienia ochrony przeglądarki, szyfrowanie dokumentów i wybór hasła.

-Ataki złośliwego oprogramowania, obejmujące wirusy i sposób, w jaki infekują komputery i urządzenia mobilne oraz ochronę poprzez odpowiednie ustawienia i przy użyciu oprogramowania antywirusowego.

-Ataki z wyższej półki, obejmujące rozproszone ataki typu „odmowa usługi” oraz środki ochronne.

-Cyberprzestępczość, obejmująca różne systemy przestępczości w cyberprzestrzeni oraz sposoby ich rozpoznania.

-Netykieta, obejmująca społecznie i profesjonalnie przyjętą etykietę w interakcjach przez Internet. Obejmie to czat, posty w serwisach społecznościowych i e-maile.

Ciągłości działania

CIO jest odpowiedzialny za opracowanie Planu ciągłości działania, który posiada wiedzę i aprobatę kierownictwa wyższego szczebla organizacji. Plan obejmuje „zapobieganie, łagodzenie, przygotowanie, reakcja i odzyskiwanie [z normalnych działań organizacji] z sytuacji awaryjnych ”. Szczegółowe standardy bezpieczeństwa informacji są określone w różnych opublikowanych standardach. Aby skutecznie zająć się sytuacją kryzysową, która spowoduje brak ciągłości w normalnych działaniach organizacji, dyrektor ds. Informatycznych musi wykonać co najmniej następujące dwa zadania:

1. Analiza przyczynowo-skutkowa nieciągłości biznesowej. Jest to badanie, które ocenia konsekwencje możliwej niekorzystnej sytuacji, która zmusi organizację do przerwania dostawy oczekiwanych produktów lub usług. W kontekście systemów informacyjnych niekorzystne sytuacje mogą być związane z operacjami wewnątrzorganizacyjnymi lub współpracą międzyorganizacyjną. Jak na przykład,

a. Front Office. Serwer witryny został zamknięty, a przyczyną może być niedostateczna zdolność do obsługi legalnych zadań, atak typu „odmowa usługi”, atak złośliwego oprogramowania, klęska żywiołowa lub problem personelu.

b. Zaplecze biurowe. Awaria magazynu lub obliczenia bazy danych, gdzie podobnie przyczyną może być niedostateczna pojemność, złośliwe oprogramowanie, błąd niezwiązany ze złośliwym oprogramowaniem, atak złośliwego oprogramowania, katastrofa naturalna lub problem personelu.

c. Awaria w zależności. Organizacja dodaje wartość do określonego produktu lub usługi, a dostawca zawiódł. Na przykład organizacja świadcząca usługi edukacyjne online korzysta z dzierżawionej platformy, na której występują problemy operacyjne.

d. Brak zgodności. Działania organizacji są zawieszane do momentu osiągnięcia zgodności. Straty niektórych danych mogą wymagać powiadomienia organów rządowych przed wznowieniem działalności.

Dyrektor ds. IT przeprowadza analizę dotyczącą powyższych możliwych przyczyn nieciągłości biznesowej i wiele innych, a także opracowuje Plan naprawy gospodarczej.

2. Plan naprawy gospodarczej. Jest to plan opracowany przez biuro CIO, przyjęty przez kierownictwo wyższego szczebla organizacji i gotowy do wdrożenia w razie nagłej potrzeby. Plan określa, z imienia i nazwiska lub stanowiska, osobę, która będzie kierować procesem odzyskiwania działalności, obowiązki i władzę tej osoby, a także linię dowodzenia, której należy przestrzegać, dopóki organizacja nie wyjdzie ze stanu wyjątkowego.

CIO: Zmiana roli

W miarę, jak technologia staje się coraz bardziej kluczowym kamieniem węgielnym każdej organizacji, rola CIO zmienia się „Od Stewarda technologicznego do lidera biznesu ... W tym nowym świecie transformacji opartej na technologii… CIO odgrywają coraz większą rolę”. Misją CIO nie jest już nadzorowanie codziennych działań działu przetwarzania danych, ale pomoc liderom organizacji w

wykorzystaniu informacji i technologii w celu zwiększenia wartości produkowanej i dostarczanej usługi interesariuszom. Prawdziwą miarą sukcesu organizacji jest korzyść oferowana interesariuszom w stosunku do dostępnych zasobów. Obecnie praktycznie każda organizacja wykorzystuje informacje, aby zmaksymalizować tę korzyść. Celem jest zwiększenie produktywności oferowanych produktów lub usług dla użytkownika, bardziej reagujący na potrzeby rynku, a przede wszystkim dostępne dla rynków docelowych. CIO jest rewolucyjną wizją transformacji, która chce, aby organizacja wykorzystała postęp technologiczny, aby osiągnąć nowy poziom osiągnięć. Mogą być mierzalne pod względem wydajności, świadczonych usług lub zysków. W tym zadaniu CIO znajdzie technologię jako wiernego sojusznika, a kulturę organizacyjną i biurokrację jako stałego przeciwnika. Aby jak najlepiej służyć ich organizacjom, CIO muszą uzyskać niezbędne uprawnienia zasoby, widoczność i uczestnictwo, aby nie byli narażeni problemy organizacyjne i obawy w celu przedstawienia rekomendacji opartych na technologii. Z czasem odizolowany kierownik działu IT został podniesiony z maszynowni i stał się centralną postacią w C-Suite noszącą tytuł CIO. Ponieważ technologia jest obecnie podstawą większości działań biznesowych, oczekuje się, że CIO musi „... być dobrym konsultantem biznesowym dla CEO, COO, a nawet CFO."

Zwiększanie wartości biznesowej dzięki Cyberbezpieczeństwu

Wartość większości produktów lub usług często obejmuje pewne wspólne elementy, które czynią je atrakcyjnymi. W cyberprzestrzeni tymi komponentami są prywatność, bezpieczeństwo i ochrona, zbiorowo oznaczające cyberbezpieczeństwo. Dlatego obecność cyberbezpieczeństwa dodaje wartości, a jej brak zmniejsza wartość. Im więcej „inteligentnych" produktów i usług, tym wyższe oczekiwania dotyczące cyberbezpieczeństwa. W przeszłości edukacja bez umiejętności obsługi komputera była uważana za niedostateczną. Dzisiaj umiejętności komputerowe są uważane za coś oczywistego, a edukacja bez umiejętności w zakresie cyberbezpieczeństwa jest niewystarczająca, jeśli nie niebezpieczna. Ponieważ każdy aspekt życia stara się czerpać korzyści z cyberprzestrzeni, cyberprzestępczość jedzie jak pasożyt żyjący ze zdrowych organizmów. Ponieważ wartość funkcjonalna jest wbudowywana w produkt lub usługę w fazie projektowania, podobnie cyberbezpieczeństwo musi być w niej osadzone.

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”.

Włamania do cyberprzestrzeni

Cyberbezpieczeństwo to środki wbudowane w informacje system podczas procesu rozwoju.

Wprowadzenie

Włamanie, w kontekście systemów informatycznych, stanowi naruszenie ustalonych zasad dostępu do danych, przy czym naruszenie może dotyczyć odczytu lub modyfikacji chronionych danych. Systemy informacyjne są chronione przez dedykowane systemy analizy ruchu zaprojektowane do wykrywania i, miejmy nadzieję, blokowania włamań. Takie systemy wykonane ze sprzętu i / lub oprogramowanie, są określane jako systemy wykrywania i zapobiegania włamaniom. W zależności od konkretnej aplikacji, system może być systemem IDS, to znaczy tylko systemem wykrywania włamań bez możliwości zapobiegania, lub może być systemem IDPS, czasem wciąż określanym jako IDS, który ma zarówno funkcje, wykrywanie, jak i zapobieganie. IDPS wdrażają reguły ustanowione przez administratora bezpieczeństwa, mające zastosowanie do ochrony punktów dostępu lub wejścia. W oparciu o te zasady IDPS przekazuje, blokuje, opóźnia lub przekierowuje ruch danych. Wybrane działanie nie może odbywać się z ludzką prędkością, a zatem wymaga od eksperta systemu, najlepiej ze sztuczną inteligencją, do decydowania z elektroniczną prędkością o potrzebnym działaniu. IDPS są ogólnie podzielone na cztery rodzaje systemów, a mianowicie

• W oparciu o sieć

• Host-Based

• Analiza zachowania sieci

• Bezprzewodowy

Wymagania IDPS to mapa polityki bezpieczeństwa organizacji w kierunku włamań.

USŁUGI BEZPIECZEŃSTWA	**:**	**UWAGI OPERACYJNE**
Monitorowanie	:	Skalowalności
Urządzenia	:	Niezawodność
Funkcje	:	Interoperacyjność
Możliwości	:	Rekonfiguracja
Wykrywanie	:	Dokumentacja
Zapobieganie	:	Wsparcie techniczne
Raportowanie	:	Szkolenie
WYDAJNOŚĆ	**:**	**SKUTECZNOŚĆ**
Obliczeniowy	:	Koszt początkowy
Przechownie	:	Koszt konserwacji

Wdrożenie tych wymagań opiera się na dostępnych technologiach zastosowanych do przewidywanych potrzeb, z parametrem opłacalności. Istnieje szeroka gama narzędzi IDPS, które zapewniają monitorowanie zdarzeń i bezpieczeństwo systemu informatycznego w stosunku do znanych zagrożeń. Najważniejszym celem intruza jest mechanizm ochronny systemu informatycznego. Początkowo, poprzez różnorodne ataki, intruzi próbują określić mocne i słabe strony IDPS, próbując rozpoznać

obecność luk w zabezpieczeniach, przez które mogą wejść do systemu i uzyskać dostęp do uszkodzonych zasobów lub uszkodzić je. Takimi zasobami mogą być listy haseł, pliki wrażliwych treści lub mechanizmy dostępu.

Konfiguracja IDPS

Ogólnie rzecz biorąc, każdy system składa się z trzech głównych komponentów: czujników, w których dane są gromadzone ze środowiska i częściowo przetwarzane; procesor, który podejmuje decyzje w wyniku oceny danych i korelacji; oraz siłowniki, które napędzane przez procesor wpływają na środowisko. Podobnie w przypadku IDPS istnieją czujniki, oprogramowanie przetwarzające oraz dotknięte nimi jednostki lub funkcje.

Czujniki

Czujniki są istotnymi elementami procesu wykrywania włamań, których funkcją jest rozpoznawanie wystąpienia potencjalnie szkodliwych zdarzeń. Lokalizacja czujników w systemie informacyjnym jest niezwykle ważna i ma ogromne znaczenie. Dlatego przed zidentyfikowaniem lokalizacji czujników należy dokładnie ustalić topologię systemu informacyjnego. Takie lokalizacje są punktami wejścia do funkcji lub obszarów systemu. Typowymi przykładami są interfejsy korporacyjne do świata zewnętrznego, takie jak połączenia z Internetem za pośrednictwem sieci LAN lub WLAN, a także zdalny dostęp za pośrednictwem modemów. W przypadku organizacji podzielonych na działy czujniki mogą być również umieszczane w międzywydziałowych punktach wejścia, monitorując dostęp do cennych zasobów w ramach działu. Bardzo ważne są również interfejsy ekstranetowe. Są to punkty wejścia, w których partnerzy będą uzyskiwać dostęp i ewentualnie modyfikować, jeśli zostaną autoryzowane, krytyczne dane w korporacyjnych bazach danych. Zdarzały się przypadki, gdy intruz z sieci A wchodzi do sieci korporacyjnej B za pośrednictwem ekstranetu A – B, a podczas gdy w B, poprzez ekstranet B – C, uzyskuje dostęp do sieci korporacyjnej C, na którą intruz nie miał autoryzacji. To wyraźnie pokazuje, że organizacja B ponosi odpowiedzialność w stosunku do swoich partnerów ekstranetowych.

Nie można nie doceniać podatności sieci wewnątrz korporacyjnej, a czujniki należy umieszczać na przejściach międzywydziałowych. Tak więc topologia sieci korporacyjnej i lokalizacja krytycznych zasobów są dobrze znane przed umieszczeniem czujników. Równie ważne jest, aby czujniki były odpowiednio zaprogramowane pod kątem tego, czego będą „szukać". Umieszczone w strategicznych lokalizacjach czujniki monitorują ruch zgodnie z określonymi kryteriami. Oznacza to, że czujniki szukają wystąpienia określonych zdarzeń i zgłaszają się do agentów. Agenci to oprogramowanie, które odbiera obserwacje czujników i ocenia, jakie zagrożenie może stwarzać samo zdarzenie lub w połączeniu z innymi zdarzeniami. Agenci mają sztuczną inteligencję, co oznacza, że podejmują decyzje na podstawie kryteriów, które mogą ulec zmianie w zależności od różnych okoliczności. Ponadto dzięki bezpiecznej komunikacji między agentami agenci wspólnie monitorują całą sieć przedsiębiorstwa. Dane z czujników mogą być tak proste, jak zliczanie liczby awarii próby podania nazwy użytkownika lub hasła. Na podstawie tej liczby agent decyduje o wymaganej akcji. Parametrem, który może statystycznie dostarczyć informacje, jest odstęp czasu między przesłaniem nazwy użytkownika a hasłem. Ten interwał wskazuje czas, jaki zajęło użytkownikowi wprowadzenie hasła. Strona hasła może mieć krótki kod wykonywalny, który zlicza odstępy czasu między wpisanymi znakami. Dotyczy to wpisu nazwy użytkownika lub hasła. Wytworzona dynamika naciśnięć klawiszy może statystycznie zapewnić dość wiarygodny mechanizm uwierzytelniania semibiometrycznego, służący jako cyfrowa identyfikacja użytkownika. Czujniki mogą być umieszczone w linii z przepływem danych służących jako zapora ogniowa. Będąc w linii czujnik może blokować podejrzany ruch, zapobiegając w ten sposób realizacji próby ataku. Czujniki mogą znajdować się z boku, dotykając przepływu ruchu i wysyłając zebrane dane do procesora IDPS. Będąc z boku, czujnik biernie obserwuje ruch bez wpływu na prędkość sieci.

Oczywiście nie może blokować podejrzanego ruchu. Tak czy inaczej, wyniki czujników są przekazywane do procesora IDPS, skąd może dojść do działania blokującego.

Procesor

Procesor zbiera zarejestrowane działania dostarczone przez czujniki i agentów i koreluje je w poszukiwaniu identyfikacji złośliwego oprogramowania lub nieprawidłowych sytuacji. Wydajność musi być dokładnie przetestowana - z IDPS offline i online - z ciągle aktualizowanymi kryteriami, aby odzwierciedlić najnowsze technologie obronne, a także stale rozwijające się możliwości szkodliwego oprogramowania.

Konsole

Procesor dostarcza wszystkie ustalenia do konsol, gdzie administratorzy nadzorują wydajność systemu. Parametry wykrywania i przetwarzania mogą być regulowane przez procesor w czasie rzeczywistym lub przez działania administratora.

Sieć

Komponenty IDPS - czujniki, procesor i konsole - komunikują się ze sobą za pomocą własnej sieci, niezależnej od sieci produkcyjnej, która jest dostępna przez Internet. W ten sposób IDPS staje się odporny na ataki włamaniowe, ponieważ jest fizycznie lub logicznie izolowany od sieci.

Możliwości IDPS

Możliwości IDPS różnią się w zależności od stopnia zaawansowania systemu. Jednak w minimalnym stopniu dyrektor ds. Informacji (CIO) użyje IDPS do niezależnego potwierdzenia działania zapory, oceny oczekiwanej zdolności filtrowania i ostrzegania, a także do powiadomienia o nietransakcyjnych czynnościach, takich jak skanowanie IP lub skanowanie portów, które, choć nie zagrożenie jest prekursorem możliwego zbliżającego się ataku włamaniowego. W procesie nadzoru nad przypisaną działalnością IDPS rejestrują informacje związane z nimi i zgłaszają się do różnych organów, zgodnie z zaprogramowaniem. Takie wydania mogą być planowymi raportami wydawanymi w określonych punktach czasowych, raportami wyjątków wydawanymi automatycznie, ponieważ miało miejsce zdarzenie specjalne, lub raportami na żądanie, w których autoryzowani odbiorcy mogą otrzymywać raporty niestandardowe. Ponadto w przypadku rozpoznanego włamania IDPS może gromadzić i rozpowszechniać informacje peryferyjne, które mogą później pomóc w dochodzeniu kryminalistycznym dotyczącym włamania. Podstawowe możliwości IDPS można zaklasyfikować jako

• Pozyskiwanie informacji

• Rejestrowanie informacji

• Techniki wykrywania

• Działania zapobiegawcze

Pozyskiwanie informacji

Zbieranie informacji odbywa się za pomocą czujników, które zapewniają wstępne przetwarzanie przed przesłaniem wyników do procesora IDPS.

Rejestrowanie informacji

Rejestrowanie zdarzeń wraz z ich klasyfikacją powoduje gromadzenie dużej ilości danych związanych z wykrytymi zdarzeniami.

1. Znacznik czasu: data i godzina. Często IDPS może mieć własne zegary czasowe, aby najlepiej utrzymać dokładne zapisy.

2. Adresy: źródło i miejsce docelowe (IP, MAC, IMEI)

3. Numery portów: źródło i miejsce docelowe

4. Typy portów: typy i kody TCP, UDP lub ICMP

5. Protokół warstwy: sieć, transport lub aplikacja

6. Numer identyfikacyjny: połączenie lub sesja

7. Ocena: Priorytet lub znaczenie do rozważenia przez procesor

8. Naruszenie: rodzaj naruszenia lub ostrzeżenia

9. Rozmiar: liczba bajtów przesłanych przez połączenie

10. Poświadczenia: nazwa użytkownika, hasło, wszelkie kody specjalne

11. Ładowność: Wymieniane dane na poziomie aplikacji

Techniki wykrywania

Techniki wykrywania włamań można podzielić odpowiednio na trzy kategorie

• Wykrywanie oparte na sygnaturach

• Wykrywanie na podstawie anomalii

• Analiza stanowa protokołu

W wykrywaniu opartym na sygnaturach IDPS ma bazę danych parametrów wskazujących na znanego wirusa. Na przykład, jeśli plik o nazwie miłość. exe jest znany jako wirus, jego obecność wygeneruje alert, a IDPS podejmie odpowiednie działania. Ponadto, jeśli źródło lub miejsce docelowe pakietu ma adres IP z czarnej listy, adres MAC lub międzynarodowy identyfikator urządzenia mobilnego (IMEI), ponownie zostanie wygenerowany alert. Możliwe, że na podstawie adresu IP można umieścić na czarnej liście cały region geograficzny lub utworzyć zasób niedostępny na przykład w godzinach wolnych od pracy. W przypadku wykrywania opartego na sygnaturach używane są czarne listy (gorące listy) i białe listy. Oczywiście wykrywanie oparte na sygnaturach nie jest możliwe w przypadku nieznanych zagrożeń. Czarne listy zawierają sygnatury dyskretnych bytów, które mogą być związane z włamaniami. Takimi jednostkami są hosty, numery portów, aplikacje, nazwy plików lub rozszerzenia plików lub inne wymierne parametry, które można rozpoznać w komunikacji sieciowej. Białe listy zawierają sygnatury dyskretnych bytów które mogą podnieść flagę włamania, podczas gdy w rzeczywistości wiadomo, że są łagodne.

W wykrywaniu opartym na anomaliach IDPS ma bazę danych profili, które reprezentują „normalne" zachowanie sieci. Jeśli coś wydaje się niezwykłe, podnosi się flagę. To jest jak kontrola paszportowa na przejściach międzynarodowych. Jeśli dana osoba jest na czarnej liście lub zauważono coś dziwnego, pojawia się alert. Profile te opisują oczekiwane zachowanie aplikacji, sieci, hostów, a nawet indywidualnych użytkowników. Parametry takich profili mogą być oparte na informacjach statystycznych i mogą się dynamicznie dostosowywać. Oznacza to, że zastosowanie sztucznej inteligencji może pozwolić na stopniową zmianę tych profili bez tworzenia ostrzeżenia. Odchylenie od tych profili zabrzmi alarm i IDPS zajmie odpowiednie działanie. W przypadku wykrywania na podstawie anomalii wymagana jest znaczna ilość dostrajania. Ciasne progi spowodują fałszywe alarmy, natomiast

luźne progi mogą nie rozpoznać złośliwej aktywności. Ataki typu „odmowa usługi" (DoS) można rozpoznać za pomocą sztucznej inteligencji, która monitoruje tempo wzrostu ruchu sieciowego. „Jeśli sztuczna inteligencja jest wbudowana w routery internetowe, routery mogą wspólnie stworzyć internetowy SCADA zdolny do wykrywania i zapobiegania potencjalnym atakom DoS". Jednak „systemy IDS oparte na anomaliach są bardziej podatne na generowanie fałszywych alarmów ze względu na ciągle zmieniający się charakter sieci, aplikacji i exploitów". „Główną zaletą metod wykrywania opartych na anomaliach jest to, że mogą być bardzo skuteczne w wykrywaniu nieznanych wcześniej zagrożeń". W stanowej analizie protokołu opracowywane są modele wydajności protokołu, które służą jako odniesienia nominalne. W pewnym sensie technika ta przypomina wykrywanie oparte na anomaliach, ale zamiast statystycznie budować modele normalnej pracy, tutaj stosuje się profile dostarczone przez dostawcę. „Kiedy przeprowadzamy analizę stanową protokołu, monitorujemy i analizujemy wszystkie zdarzenia w ramach połączenia lub sesji" [6], a następnie mapujemy zachowanie na dostępne profile. Ta technika wykrywania, choć przydatna, nie może wykryć ataków, chyba że nastąpi naruszenie oczekiwanego zachowania.

Działania zapobiegawcze

IDPS, jak sugeruje ich nazwa, po wykryciu oczekuje się, że faktycznie zapobiegnie próbie wtargnięcia. Można to osiągnąć na różne sposoby, w tym

• Blokowanie dostępu do wszystkich usług docelowych zasobów (bazy danych, serwera lub aplikacji).

• Blokowanie wszelkiej komunikacji z użytkownikami posiadającymi określony identyfikator, taki jak adres IP, adres MAC, numer użytkownika lub inne unikalne cechy podejrzanego atakującego.

• Blokowanie dalszej aktywności sesji połączenia sieciowego, które spowodowało incydent.

• Blokowanie tylko zainfekowanej części transakcji. Dotyczy to załącznika do wiadomości e-mail lub toksycznego pliku towarzyszącego plikowi HTML.

• Blokowanie żądania atakującego przez zmianę kryteriów zapory sieciowej.

Jest bardzo możliwe, że IDPS może przegapić atak, tworząc fałsz negatywny lub może zablokować bona fide użytkownika, tworząc fałszywie dodatni. Jednak dzięki szeroko zakrojonym testom wstępnym i dostosowaniu, IDPS może asymptotycznie zbliżyć się do perfekcji.

Zarządzanie IDPS

Po nabyciu IDPS jego zarządzanie dotyczy wdrożenia, działania i utrzymania systemu. Organizacje powstrzymują się od wewnętrznego opracowywania IDPS z dwóch powodów. Jednym z nich jest to, że IDPS, aby był potężny, musi być bardzo złożony. Po drugie, IDPS są łatwo dostępne i można je konfigurować ponownie.

Realizacja

Wdrożenie nabytego produktu IDPS składa się z pięciu etapów.

• Krok pierwszy: identyfikacja funkcji produktu

• Krok drugi: Zaprojektowanie architektury / topologii, w której cechy produktu są odwzorowane na wymagania dotyczące wykrywania włamań i zapobiegania w systemie informatycznym, który ma być chroniony

• Krok trzeci: instalacja IDPS, która może być oprogramowaniem aplikacyjnym lub sprzętowym

• Krok czwarty: Progresywne testowanie IDPS

• Krok piąty: Aktywacja systemu, z możliwym powrotem do dowolnego z kroków

Krok pierwszy: funkcje

Dostępnych jest wiele IDPS. Niektóre mają formę aplikacji. Oznacza to, że IDPS to oprogramowanie o minimalnym kodzie, które szeroko wykorzystuje procedury lub moduły dostępne w systemie operacyjnym hosta i jest oczywiście specyficzne dla systemu operacyjnego. Inne są w formie urządzenia. Oznacza to, że oprogramowanie jest samowystarczalnym pakietem z własnymi procedurami i jest niezależne od systemu operacyjnego hosta.

Krok drugi: architektura

Zaprojektowana architektura zapewni topologię zastosowanego IDPS, biorąc pod uwagę lokalizacje monitorowania i poziom oczekiwanej niezawodności. W celu zwiększenia niezawodności zastosowano redundancję czujników, gdy wiele czujników monitoruje tę samą aktywność. Architektura IDPS zajmuje się także lokalizacją innych komponentów IDPS, takich jak serwery i konsole administracyjne. IDPS połączy się z chronionym przez siebie systemem informatycznym w celu gromadzenia danych i wpływania na niezbędne działania.

Krok trzeci: instalacja

Po zidentyfikowaniu rozwiązania IDPS i zdefiniowaniu topologii instalacja może być kontynuowana. Zazwyczaj urządzenia IDPS oparte na urządzeniach są łatwiejsze do wdrożenia. Najważniejszym parametrem pozostaje jednak ustawienie czujników. W zależności od konkretnej aplikacji bezpieczeństwa czujniki mogą być umieszczone przed lub za zaporami ogniowymi, w krytycznych podsieciach, na serwerach WWW i e-mail oraz w krytycznych bazach danych.

Krok czwarty: testowanie

Testowanie systemu i szkolenie operatora powinny przebiegać równolegle. Testowanie jest długim procesem, podczas którego kryteria wykrywania i zapobiegania są dostosowywane w celu zminimalizowania fałszywych alarmów. Szkolenie operatorów będzie działaniem ciągłym, w miarę wprowadzania nowych zagrożeń i aktualizacji oprogramowania.

Krok piąty: Aktywacja

Jest to ostatni etap, w którym system wchodzi w życie. Praktyka pokazała, że kiedy IDPS jest aktywowany przy wszystkich czujnikach aktywnych jednocześnie, duża liczba fałszywych alarmów przytłacza operatora. Sugeruje się, że aktywacja czujników odbywa się w sposób progresywny, tak aby można było wprowadzić dodatkowe dostrojenie. Stopniowe wdrażanie IDPS najlepiej ujawni ukryte problemy i zmaksymalizuje skuteczną ochronę systemu informatycznego. W fazie aktywacji tymczasowe, częściowe lub całkowite awarie systemu mogą okazać się konieczne do logicznego i fizycznego zaangażowania IDPS w sieć produkcyjną.

Na etapie produkcji konieczna będzie ciągła aktualizacja bazy danych podpisów, a także korekty progów. Biorąc pod uwagę znaczenie IDPS w bezpiecznym działaniu systemu informatycznego, sugeruje się, aby poświadczenia administratorów obejmowały uwierzytelnianie dwuskładnikowe, szczególnie w przypadku korzystania z dostępu zdalnego.

Operacja

Produkty IDPS są zwykle obsługiwane za pomocą konsoli, która wykorzystuje graficzny interfejs użytkownika, a niektóre oferują również interfejs wiersza poleceń. Za pomocą konsoli administrator może wykonywać szeroki zakres czynności, w tym

• Monitorowanie i analiza danych IDPS

• Konfiguracja i aktualizacja parametrów czujnika i serwera zarządzania, w tym segmentacja misji IDPS na sektory, ułatwiając w ten sposób operacje i rozwiązywanie problemów

• Konfiguracja kont użytkowników i parametrów autoryzacji, w tym określone uprawnienia i czujniki do monitorowania

• Projektowanie i przygotowanie harmonogramu, na żądanie i raportowanie wyjątków

Za pomocą konsoli operatorzy mogą definiować, edytować, przechowywać i pobierać zapytania. Można także tworzyć zdefiniowane przez użytkownika filtry zapytań i profile alertów oraz przygotowywać raporty niestandardowe.

Konserwacja

IDPS musi być utrzymywany w sposób ciągły. Oczekiwana konserwacja składa się zasadniczo z trzech części - potwierdzających prawidłowe działanie, aktualizację oprogramowania i szkolenie odpowiedzialnego personelu.

Konserwacja to nieuniknione zadanie - wykonywane online i offline - wpłynie to na oczekiwaną ciągłość usługi. Potwierdzenie prawidłowego działania obejmuje monitorowanie i testowanie. Testowanie może odbywać się okresowo i może odbywać się w środowisku testowym offline lub w trakcie produkcji systemu - w trybie online. Aktualizacja oprogramowania obejmuje aktualizację bazy sygnatur zagrożeń; dostosowanie poziomów zagrożenia; aktualizacja oprogramowania dostarczonego przez dostawcę poprzez instalację poprawek; oraz rekonfigurację systemu, gdy wymagają tego nowe wymagania, technologie i zagrożenia. Po każdej aktualizacji wymagany jest dokładny test. Wskazane jest, aby przed zastosowaniem aktualizacji potwierdzić ich autentyczność za pomocą dostępnych mechanizmów. Zazwyczaj sumy kontrolne plików aktualizacyjnych obliczone przez administratora muszą odpowiadać sumom dostarczonym przez dostawcę. Ponadto tworzenie kopii zapasowych starych konfiguracji jest zawsze dobrym pomysłem. Ciągłe szkolenie odpowiedzialnego personelu jest absolutnie niezbędnym zadaniem w celu rozwijania umiejętności najlepszej obrony systemu. Szkolenie zazwyczaj odbywa się na miejscu, po wstępnym zapewnieniu przez sprzedawcę, aby wszyscy mogli nabrać tempa.

Dokumentacja produktu jest zawsze doskonałym źródłem informacji, na których operatorzy mogą polegać, nie wspominając już o oczekiwanej dostępności wsparcia przez czat na żywo. Skuteczny nadzór i działanie IDPS wymaga specjalistów IT posiadających umiejętności w zakresie bezpieczeństwa informacji i administracji sieci, a także administracji systemem, na których można budować swoją stale rosnącą wiedzę w zakresie bezpieczeństwa cybernetycznego z naciskiem na włamania, wykrywanie i zapobieganie. W tym celu wskazane jest dołączenie do grupy użytkowników danego produktu, ponieważ służy on jako forum gdzie pojawiają się problemy i obawy i, miejmy nadzieję, znajdują rozwiązania. Aby skoncentrować się na swojej podstawowej działalności, wiele organizacji zleca bezpieczeństwo swojego systemu informatycznego firmom poświęconym tej dziedzinie z dużym doświadczeniem i wiedzą specjalistyczną. Oczywiście outsourcing musi być oceniany pod kątem misji i ograniczeń organizacji.

Klasyfikacja IDPS

IDPS są podzielone na następujące cztery ogólne kategorie. Oparty na hoście, który analizuje zdarzenia wewnątrz określonego hosta (komputera) w poszukiwaniu działań, które mogą sugerować włamanie. Oparty na sieci, który analizuje aktywność protokołu w określonej sieci (urządzeniach lub segmentach) w poszukiwaniu nieprawidłowości protokołu Network Behavior, który analizuje zdarzenia, które mogą ujawnić zasady naruszenia, obecność złośliwego oprogramowania lub rozproszona odmowa usługi. Bezprzewodowy, który sprawdza ruch sieci bezprzewodowej podejrzane działania

IDPS oparty na hoście

IDPS oparty na hoście jest systemem wykrywania i zapobiegania włamaniom który dotyczy pojedynczego hosta, to znaczy jednej stacji roboczej lub serwera (sieć, e-mail, DNS lub inny). Zazwyczaj ten IDPS monitoruje następujące sześć obszarów i działań:

• Zewnętrzny interfejs przewodowy

• Bezprzewodowy (Wi-Fi i Bluetooth)

• Ruch modemowy

• Status pliku (dostęp, modyfikacja i tworzenie)

• Konfiguracja systemu (statyczna lub dynamiczna)

• Uruchamianie procesów (zarówno systemowych, jak i aplikacji)

Obserwacje w powyższych obszarach są porównywane z szablonami oczekiwanej wydajności i może powodować alerty wykrywania i / lub działania zapobiegawcze.

IDPS oparty na hoście może być oparty na oprogramowaniu, w którym to przypadku jest instalowany wewnątrz samego monitorowanego hosta, lub może być oparty na urządzeniu, w którym to przypadku jest oddzielnym fizycznym elementem sprzętowym umieszczonym w linii między monitorowanym hostem a ścieżka do Internetu lub intranetu. W przypadku aplikacji istnieją dwa podejścia: jedno, gdzie agent monitoruje wyniki działań, a drugi, w których część kodu (zwana shims) jest wstawiany w wybrane miejsca, takie jak system operacyjny, kod systemu operacyjnego, kod aplikacji lub protokoły, służąc jako mini-zapory ogniowe zdolne do wykrywania i blokowania niepożądanej aktywności. W przypadku urządzenia urządzenie jest fizycznie poza hostem i nie ma możliwej mikrokontroli zapewnionej przez podkładki, ale jest niezależne od zastosowanego systemu operacyjnego. Rejestrowane parametry wykrytych zdarzeń obejmują

• Rodzaj zdarzenia i jego priorytet.

• Znacznik czasu na podstawie przypisanego źródła. Większość IDPS generuje własne znaczniki czasu zamiast kopiować je z zewnętrznego źródła.

• Powiązane adresy portów i IP (Internet i intranet).

• Nazwy plików i ich ścieżki (katalogi, podkatalogi itp.).

• Poświadczenia autoryzacji / uwierzytelnienia (nazwy użytkowników).

Host IDPS sprawdza kody pod kątem złośliwego oprogramowania, wykonując je w środowisku piaskownicy, to znaczy w środowisku, w którym wykonanie nie może zaszkodzić innym programom, ani nie może wykorzystywać zabronionych zasobów. W tym nadzorowanym wykonaniu agent IDPS szuka

• Naruszenia, takie jak zapuszczanie się w nieautoryzowane miejsce

• Eskalacja uprawnień

• Przepełnienie bufora, stos lub stos

• Nieautoryzowane wywołania biblioteki

• Sekwencje instrukcji, które mogą być albo kopiowaniem klawiszy, albo próbą instalacji rootkitów

IDPS oparty na hoście sprawdza również integralność, właściwości i dostęp do plików. Integralność jest sprawdzana za pomocą testu sumy kontrolnej; jeśli jest niepoprawny, oznacza to, że zawartość pliku została zmieniona. Suma kontrolna jest resztką, resztką, sekwencją binarną powstałą po przejściu zawartości pliku przez z góry określony algorytm. Właściwości pliku są bardzo ważne dla bezpieczeństwa i integralności zawartości pliku. Właściwości obejmują uprawnienia dostępu - odczyt / zapis, autorstwo pliku, znaczniki czasu dostępu i modyfikacji, podpis cyfrowy i ewentualnie inne parametry w zależności od typu pliku. Kontrola dostępu do plików jest najważniejszą funkcją bezpieczeństwa. Umieszczenie podkładki dystansowej może wykryć naruszenia zasad, a nawet wdrożyć zasady bezpieczeństwa poprzez blokowanie dostępu. IDPS oparty na hoście, podobnie jak inne systemy, wymaga strojenia. Musi to mieć miejsce przy początkowej aktywacji, a także po instalacji lub wymianie wybranych chronionych plików. Ponadto, białe i czarne listy muszą być aktualne, aby zapobiec fałszywym wykryciom. Przed wdrożeniem konflikt z innymi systemami ochrony musi zostać rozwiązany, aby uniknąć nieprawidłowego działania w obu systemach. Z powodu ciągłej czujności IDPS oparte na hoście stanowią obciążenie dla chronionego hosta, wymagając znacznego czasu procesora i miejsca w pamięci i dysku. Ponadto między instalacją a wdrożeniem wymagane są szeroko zakrojone testy w celu zapewnienia poprawnej integracji IDPS z hostem. Takie testy będą musiały odbywać się w trybie offline, co spowoduje, że host będzie nieczynny w tym okresie.

IDPS oparty na sieci

W sieci IDPS czujniki mogą być aplikacjami lub urządzeniami i mogą monitorować więcej niż jedno urządzenie lub segment w sieci. Aby zastosować środki zapobiegawcze, czujniki muszą być zainstalowane w linii. Czujniki liniowe muszą mieć bardzo dużą prędkość, aby nie powodowały zatorów komunikacyjnych. Jeśli obsługa ruchu osiągnie punkt prawie nasycenia, ruch musi przepuścić niezaznaczony lub ruch o niskim priorytecie zostać zrzucony, aby zmniejszyć obciążenie. W przypadku instalacji pasywnej obserwacje są zgłaszane tylko bez możliwości blokowania wykrytych zdarzeń. Czujniki pasywne przekazują zebrane dane do serwera zarządzania, gdzie są analizowane i gdzie można podjąć działania zapobiegawcze.Sieciowe IDPS z czujnikami wbudowanymi mogą interweniować i zapobiegać próbom wykonania zdarzenia, podczas gdy sieciowe IDPS z pasywnymi czujnikami służą jedynie jako obserwatorzy i reporterzy zdarzeń. IDPS oparte na sieci analizują działania w warstwach sieci, transportu i aplikacji, a większość wykorzystuje wszystkie trzy techniki wykrywania omówione wcześniej , a mianowicie wykrywanie oparte na sygnaturach, wykrywanie oparte na anomalii i analizę stanowego protokołu. Procesy wykrywania można rozdzielić na kilka czujników obsługiwanych przez moduł równoważenia obciążenia IDPS. IDPS oparty na sieci jest w zasadzie obserwatorem obserwującym przepływający ruch sieciowy. W tym procesie IDPS poszukuje naruszeń, zgodnie z ustalonymi kryteriami. IDPS zgłasza takie naruszenia na odpowiednim serwerze zarządzania IDPS, który może zastosować środki zapobiegawcze. Rodzaje gromadzonych danych obejmują adresy IP i MAC komunikujących się hostów, a także typ i wersję systemu operacyjnego. Ustalenie wersji prowadzi do informacji o istnieniu możliwych luk, które należy chronić. Inne zebrane parametry to liczba używanych portów, aplikacji i ich wersji, liczba przeskoków w podróży między dwoma hostami oraz inne dane, które normalnie są zawarte w protokołach komunikacyjnych.

System analizy zachowania sieci

System analizy zachowań sieci (NBA), jak sama nazwa wskazuje, bada zachowanie skończonej sieci i zwykle jest oparty na urządzeniach. NBA biernie obserwuje liczne punkty i działania protokołów w sieci i tworzy punkt odniesienia, który stale się aktualizuje i stanowi „normalne zachowanie w ruchu". NBA wykorzystuje ten model jako punkt odniesienia do wykrywania odchyleń, a także do rozpoznawania trendów w korzystaniu z różnych zasobów. NBA idealnie nadaje się do wykrywania ataków DoS lub ciągłych prób łamania kodów autoryzacyjnych. Czujnik NBA może być instalowany w trybie, w linii lub pasywny. W trybie in-line NBA służy jako minifirewall, blokując żądania od podejrzanych hostów. W trybie pasywnym NBA zbiera dane z podsłuchiwanego ruchu - takie jak adresy IP komunikujących się hostów, używane protokoły i aktywne aplikacje - i interweniuje w razie potrzeby, przerywając połączenia, które wspierają działania, którym nie można ufać. Rycina 7.8 ilustruje topologię systemu wykrywania włamań NBA.

Bezprzewodowe IDPS

Bezprzewodowy IDPS monitoruje wydajność bezprzewodowych sieci lokalnych (WLAN). Faktyczną technologią WLAN jest Wi-Fi, oficjalnie znany jako IEEE 802.11. Ta technologia działa w widmach podzielonych na kanały, w których komunikacja nieustannie zmienia kanały. Dlatego bezprzewodowy IDPS powinien mieć jeden czujnik na kanał, aby zmaksymalizować jego wydajność. Jeśli jest tylko jeden czujnik, czujnik ten będzie musiał przeskakiwać z kanału na kanał, naturalnie tracąc aktywność na drodze. Bezprzewodowe IDPS mogą być autonomiczne lub osadzone w bezprzewodowym punkcie dostępowym (AP), skąd monitorują aktywność sieci. Mimo że technologia Wi-Fi zapewnia bezpieczeństwo danych za pośrednictwem WEP (Wired Equivalent Privacy), jej siła szyfrowania jest uważana za słabą i podatną na złamanie i konieczne są dodatkowe środki. Nawet jeśli organizacja nie ma działającej sieci bezprzewodowej, można wdrożyć bezprzewodowy IDPS, aby zbadać fale radiowe i upewnić się, że żaden nieautoryzowany punkt dostępowy nie jest podłączony do sieci organizacji. Jako minimum należy użyć wyszukiwarki Wi-Fi, aby potwierdzić, że żaden nieautoryzowany punkt dostępowy nie jest podłączony w sieci LAN organizacji. Rysunek 7.10 pokazuje typową wyszukiwarkę Wi-Fi. Jeśli organizacja rzeczywiście ma działające sieci WLAN, „Obecnie dostępne są rozwiązania, w których pozycjonowanie czujników RF może geometrycznie ustalić, czy klient znajduje się w autoryzowanym obszarze fizycznym. Takie technologie, które wymagają szkolenia w terenie i dokładnego dostrojenia, zapewniają 100% bezpieczeństwa podczas testów ". Rozmieszczenie czujników musi uwzględniać różne czynniki, w tym:

• Zasięg czujników i plan piętra budynku

• Topologia bezprzewodowych punktów dostępowych organizacji

• Topologia przewodowej sieci organizacji

• Koszt IDPS a wartość chronionych danych

• Fizyczne bezpieczeństwo urządzeń

• Zastosowane technologie IDPS

Wykryte zdarzenia są oceniane w odniesieniu do kryteriów podobnych do kryteriów pozostałych trzech typów IDPS opisanych powyżej. Oczekiwane możliwości bezprzewodowego IDPS obejmują:

• Rozpoznanie obecności wszystkich urządzeń bezprzewodowych-punktów dostępowych lub stacji.

• Określenie fizycznej lokalizacji dowolnego urządzenia bezprzewodowego - AP lub stacji. Znalezienie fizycznej lokalizacji odbywa się poprzez triangulację, która będzie wymagać zastosowania kilku czujników.

• Uznanie naruszeń zasad.

• Możliwość wykonania akcji zapobiegawczej, gdy wciąż jest w trybie wykrywania. Odbywa się to za pomocą dwóch niezależnych modułów RF, jeden nasłuchuje cały czas, a drugi przesyła informacje o zdarzeniach.

• Wykrywanie obecności

• Ataki typu man-in-the-middle

• Ataki DoS

• Skanery sieci bezprzewodowej używane przez wardrivers (Wardrivers to osoby, które jeżdżą po ulicach, aby zlokalizować sieć bezprzewodową do użycia lub ataku.

Rejestrowane parametry wykrytych zdarzeń obejmują:

• Identyfikacja numeru MAC lub IMEI urządzenia bezprzewodowego podejrzewanego o zdarzenie.

• Liczba kanałów, przez które miało miejsce wydarzenie.

• Adres intranetowy przypisany do urządzenia bezprzewodowego przez AP. Zazwyczaj jest to adres 192.168.1.xx, gdzie xx to numer przypisany do urządzenia.

• Znacznik czasu na podstawie przypisanego źródła. Większość IDPS generuje własne znaczniki czasu zamiast kopiować je z zewnętrznego źródła.

• Rodzaj zdarzenia i poziom priorytetu według klasyfikacji IDPS.

• Numer czujnika, jeżeli należy zastosować wieloczujnikowy IDPS.

• Rodzaj zastosowanych środków zaradczych. Zazwyczaj zakończenie połączenia i zapobieganie nowemu połączeniu z podejrzaną jednostką.

Wstępne wdrożenie bezprzewodowego IDPS wymaga inicjalizacji, w której wprowadzane są parametry legalnych jednostek i przeprowadzane jest dostrajanie, aby upewnić się, że chroniony teren jest odpowiednio objęty.

Przewidywanie ataków cyberbezpieczeństwa

Przyspieszenie ataków cyberbezpieczeństwa umożliwiło ostrożnym obserwatorom dokonywanie prognoz, z których większość niestety się sprawdziła. Predyktorzy opracowali algorytmy - metodologie - w których komponenty wejściowe obejmują dogłębną znajomość organizacji

• Umiejętności na poziomie C-Suite

• Umiejętności w maszynowni IT

• Konfiguracja systemu informacyjnego

• Operacje biznesowe

• Plan ciągłości działania

• Zależność od podmiotów zewnętrznych

Ponadto w tym algorytmie predykcyjnym wprowadzono aktualny i prognozowany stan techniki szkodliwego oprogramowania. Wiedza uzyskana z tych ćwiczeń pomaga lepiej zrozumieć organizację

• Filozofia cyberbezpieczeństwa

• Obszary krytyczne w stosunku do celów organizacyjnych

• Narażenie na cyberbezpieczeństwo

• Następstwa poważnego cyberataku

• Możliwe możliwości cyberobrony

Analizy, takie jak powyższe, powinny być przeprowadzane w organizacji raz w roku, jeśli nie w sposób ciągły, przy czym oprócz oceny zdolności obronnych pierwszej linii należy zaprojektować i przetestować tworzenie kopii zapasowych danych oraz redundancję operacyjną / funkcjonalną. Zazwyczaj taka samoocena cyberbezpieczeństwa składa się z czterech części, a mianowicie:

• Podstawowa konfiguracja zabezpieczeń systemu, w której narzędzia oceny ryzyka ujawniają luki, które należy wyeliminować lub zminimalizować.

• Modelowanie, symulacja i analiza, w których symulowane są wektory ataków i oceniana jest ekspozycja cybernetyczna.

• Demonstracja podatności, w której rzeczywiste testy penetracyjne są stosowane w systemie, oceniając jego działanie w warunkach pożaru na żywo.

• Alokacja działań naprawczych i ryzyka rezydualnego, w których dokonuje się ustalania priorytetów ryzyka i przydzielane są środki zaradcze, w zależności od tego, jak krytyczny może być niekorzystny wpływ.

Biorąc pod uwagę, że na cyber bitewnym polu broń ofensywna nie jest jak dotąd ani znana, ani znormalizowana, nie należy się spodziewać podatności na zero dni, a dzięki odpowiednim redundancjom i lustrzanym bazom danych obrażenia cybernetyczne zostaną zminimalizowane.

Trendy w zakresie cyberbezpieczeństwa

Konfrontacja w zakresie cyberbezpieczeństwa podlega dwustopniowej ewolucji, a mianowicie cyberatakom prowadzącym scenę i cyberobrony, która się rozwija. W atakach cybernetycznych tradycyjne ataki, takie jak rozproszona odmowa usługi (DDoS), maleją, a liczba ransomware rośnie i rośnie. Niestety dostępność waluty internetowej, takiej jak BitCoin, ułatwia anonimową płatność żądanego okupu. Przewiduje się, że korzystanie z urządzeń Internetu Rzeczy w krytycznych aplikacjach przyciągnie Ransomware-of-Things (RoT) w celu ich zainfekowania, utrzymując ich unikalną operację w niewoli do momentu zrealizowania niemożliwej do wykrycia płatności. W cyberobronie ośmioznakowe hasło jest zastępowane wieloskładnikowym, zwykle dwuskładnikowym schematem autoryzacji, przy czym jeden ma charakter biometryczny. Ponadto wykorzystanie szyfrowania wzrosło wraz ze wzrostem świadomości cyberbezpieczeństwa. Obserwuje się także trend wzrostu edukacji w zakresie bezpieczeństwa cybernetycznego, prowadzący do uzyskania certyfikatów i stopni uniwersyteckich. Jednak zapotrzebowanie nie jest zaspokojone, co powoduje nadmierną liczbę subskrybowanych programów

Obrona cyberprzestrzeni

Cyberbezpieczeństwo jest integralną częścią każdej koncepcji bezpieczeństwa korporacyjnego lub krajowego

Wprowadzenie

Zagrożenia dla danych pochodzą ze wszystkich azymutów. Dane są zagrożone zarówno podczas przechowywania, jak i podczas transportu, a specjaliści ds. Bezpieczeństwa danych muszą wdrożyć czujniki i bariery, aby żadne złośliwe oprogramowanie nie mogło wpłynąć na dane organizacji. Istnieje mnóstwo technik i narzędzi, które chronią dane, a przy odpowiednim wdrożeniu maksymalizują bezpieczeństwo systemu informatycznego. Narzędzia bezpieczeństwa danych można ogólnie pogrupować w zorientowane na ochronę komputera i ochronę sieci, przy czym te pierwsze dotyczą danych tworzonych lub przechowywanych na komputerze, a te drugie dotyczą danych w tranzycie podróżujących przez sieci.

Aplikacje do ochrony plików

Istnieje wiele pojedynczych funkcji, a także kompleksowe oprogramowanie do ochrony plików, które po zainstalowaniu chronią komputer przed wieloma niepożądanymi zdarzeniami.

Kopia zapasowa pliku

Tworzenie kopii zapasowych plików jest podstawową funkcją, którą musi mieć każda stacja robocza lub system informacyjny. Kopia zapasowa plików może odbywać się w trybie offline na podłączonym urządzeniu wymiennym lub w systemie pamięci masowej dostępnym w intranecie lub online przez FTP w lokalizacji dostępnej w Internecie. Przechowywanie kopii zapasowych może odbywać się w czasie rzeczywistym, zgodnie z harmonogramem lub na żądanie. Pamięć może mieć opcje szyfrowania i kompresji. Ponadto opcje przechowywania kopii zapasowych często oferują „automatyczną archiwizację starych wersji". Chociaż nie jest to zalecane, większość aplikacji do tworzenia kopii zapasowych oferuje partycjonowanie głównego dysku, tworząc obszar kopii zapasowych plików. Chociaż jest to lepsze niż brak tworzenia kopii zapasowej, najlepiej miejsce na kopię zapasową musi znajdować się na fizycznie innym nośniku. Rysunek 8.1 ilustruje różne opcje tworzenia kopii zapasowych plików. Chociaż tworzenie kopii zapasowych plików jest niewątpliwie koniecznym środkiem, odzyskiwanie może być bardzo czasochłonnym procesem ponownej instalacji setek aplikacji i plików. Można tego uniknąć, jeśli zamiast tworzyć kopię zapasową plików, od czasu do czasu wykonywana jest kopia zapasowa pełnego obrazu zagrożonych dysków. Ten obraz binarny, archiwizowany z częstotliwością ustalaną przez administratora danych, będzie znacznie szybciej mapowany z powrotem na dyski w celu szybkiego i bardziej wiernego odzyskiwania. Obraz nośnika pamięci jest pojedynczym plikiem binarnym, który zawiera każdy bit tego nośnika, w tym wszystkie bity partycjonowania sektora. Takim nośnikiem może być taśma, dysk USB lub dowolny dysk (twardy, dyskietka, CD, DVD itp.), Gdzie obraz jest idealną logiczną repliką zarchiwizowanego nośnika.

Odzyskiwanie po awarii

Odzyskiwanie po awarii dotyczy sytuacji awaryjnych, w których pliki operacyjne organizacji są uszkodzone w stopniu przekraczającym dopuszczalne użycie. Odzyskiwanie po awarii wymaga, aby całe oprogramowanie organizacji było przechowywane w co najmniej dwóch lokalizacjach, jednym w siedzibie, a drugim poza lokalem, i było dostępne online. Systemy odzyskiwania po awarii składają się z serwerów i dużych urządzeń pamięci masowej zapewniających szeroki zakres funkcji, w tym:

• Kopia zapasowa obrazu dysku

• Kopia zapasowa plików operacyjnych i archiwalnych

• Kopia zapasowa aplikacji (z przechowywaniem numerów licencji)

• Przywracanie systemu od zera (mapowanie binarne)

• Tworzenie kopii zapasowej na dysku / udziale sieciowym

• Tworzenie kopii zapasowych na taśmach i bibliotekach taśm

• Tworzenie kopii zapasowych w pamięci online

• Zdalne i scentralizowane zarządzanie

• Katalog kopii zapasowych i wyszukiwanie

• Przywróć na innym sprzęcie lub maszynie wirtualnej (VM)

• Usuwanie duplikatów

Termin „duplikacja" oznacza usunięcie wszystkich duplikatów, więc cokolwiek jest przechowywane lub przesyłane, jest tak unikalne, jak to możliwe. W ten sposób wymagana pojemność pamięci i czas transmisji po awarii są zminimalizowane. Odzyskiwanie po awarii, które jest bardzo podstawową funkcją organizacji, wymaga przydzielenia dedykowanego zespołu do tego zadania, który dzięki szkoleniom i praktyce może zapewnić ciągłość biznesową w minimalnym czasie.

Usuwanie historii

Usuwanie historii może być bardzo ważną kwestią w wielu organizacjach. W starym papierowym świecie niszczarka papieru lub pojemnik na ogień całkowicie wyeliminowałyby istnienie wybranych dokumentów. Chociaż istnieje wiele elektronicznych sposobów niszczenia dokumentu elektronicznego, agencje wywiadowcze często wymagają, aby fizyczny nośnik, na którym rezyduje lub znajduje się wrażliwy dokument elektroniczny, był fizycznie niszczony na małe kawałki o wymiarach mniejszych niż 4 × 4 mm. Komunikat, wynikający z tej opcji, jest taki, że żadne elektroniczne usuwanie plików nie jest wystarczająco silne, aby absolutnie zaufać. Wiele przeglądarek internetowych oferuje prywatne tryby surfowania, zwane incognito, inPrivate lub innymi nazwami, w których twierdzi się, że po wyjściu z tego trybu komputer nie zachowuje śladu surfowania w tym trybie. Według ekspertów kryminalistyki dostępne są narzędzia umożliwiające odzyskiwanie takich plików i innych danych.

Niszczenie i wycieranie

Niszczenie plików jest procesem elektronicznym, w którym plik jest kilkakrotnie zapisywany z kilkoma wzorami, tak więc według twórcy e-shreddera plik jest całkowicie niszczony. Wiele produktów antywirusowych zawiera niszczarkę elektroniczną. Wymazywanie dysku to koncepcja całkowitego wyczyszczenia dysku i sformatowania go. Jest to potrzebne w przypadku przenośnych urządzeń pamięci masowej, dysków twardych lub półprzewodnikowych urządzeń USB. Takie produkty „całkowicie i łatwo usuwają wszystkie dane na żywo, aby nie można było ich odzyskać za pomocą żadnej istniejącej technologii".

Odzyskaj plik

Cofnięcie usunięcia pliku pozwala odzyskać określony plik, który został usunięty. Po usunięciu pliku jego zawartość nie jest usuwana, tylko jego miejsce jest dodawane na liście dostępnych sektorów. Z tego powodu usunięty plik może zostać przywrócony, chyba że został faktycznie nadpisany. Dostępnych jest kilka skutecznych narzędzi z wystarczającą liczbą parametrów wyszukiwania, co

pozwala wykryć pliki i cofnąć proces usuwania krócej niż w innych przypadkach, choć czasami mierzone w godzinach

Szyfrowanie plików

Szyfrowanie plików jest niezbędną praktyką w utrzymywaniu bezpieczeństwa plików, ale posiadanie hasła do każdego dokumentu może przynieść efekt przeciwny do zamierzonego.

Jednak poufne dokumenty wymagają ochrony i należy zidentyfikować opcję szyfrowania. Pakiety automatyzacji pakietu Office zapewniają opcję szyfrowania, w której w razie potrzeby można przypisać dwa hasła, jedno tylko do odczytu, a drugie do modyfikacji. Można używać zewnętrznych aplikacji szyfrujących, które zapewniają równie silne szyfrowanie. Inne oprogramowanie do szyfrowania umożliwia tworzenie „wirtualnego zaszyfrowanego dysku w pliku ... [który można zamontować] ... jako dysku wirtualnego, do którego można uzyskać dostęp za pomocą litery dysku" .Może to być dysk główny lub przenośny. Gdy pliki są przechowywane na tym dysku wirtualnym, są one szyfrowane i przenoszą klucz hasła dysku. Jest to bardzo interesująca technologia, w której nie ma potrzeby stosowania indywidualnych haseł dla poszczególnych plików.

Rejestratory

Rejestratory to oprogramowanie lub sprzęt, które kopiują informacje podczas ich generowania i przechowują je w określonym miejscu. To miejsce może znajdować się na komputerze, na którym informacje zostały wygenerowane, lub może być w odległym miejscu dostępnym w sieci, przewodowym lub bezprzewodowym. Administrator może zainstalować rejestrator w celu gromadzenia statystyk do analizy lub w celu tajnego monitorowania niczego niepodejrzewającego użytkownika. Możliwe jest również, że haker sieciowy zainstaluje program rejestrujący na niechronionym komputerze. Zarejestrowane informacje mogą być przechowywane lokalnie lub zdalnie. W tym drugim przypadku komunikacja może odbywać się za pośrednictwem

• FTP, wysłane na serwer lub bazę danych

• E-mail w regularnych odstępach czasu

• Bezprzewodowy oznacza — Wi-Fi lub Bluetooth

• Zdalne logowanie - komunikacja między komputerami

Klawiatura jest głównym interfejsem człowiek-maszyna i jest bardzo wrażliwym punktem wejścia. Rejestratory klawiszy działają w różnych trybach, przy czym najłatwiej jest to zrobić dzięki oprogramowaniu zainstalowanemu w tym celu. Inne tryby to fale akustyczne lub elektromagnetyczne. Wciśnięcie każdego klawisza generuje niepowtarzalny dźwięk oparty na mechanicznej konstrukcji klawiatury, i możliwe jest, że dźwięki te zostaną zarejestrowane i przeanalizowane, co prowadzi do sekwencji naciśnięć klawiszy. W przypadku klawiatur bezprzewodowych komunikacja może być przechwytywana z powietrza i podobnie ujawnia naciśnięcia klawiszy. W klawiaturach przewodowych przewody łączące promieniują fale elektromagnetyczne, reprezentując standardowe sekwencje zer i jedynek odpowiadające naciśnięciom klawiszy.

Anti-Loggery

Anty-loggery to oprogramowanie zaprojektowane specjalnie do wykrywania obecności kodu rejestrującego. Chociaż typowe oprogramowanie antywirusowe wykrywa wiele trybów rejestrowania, dedykowane oprogramowanie antywirusowe może lepiej to obsłużyć i bardzo ważna potrzeba bezpieczeństwa. Za pierwszym razem szyfrowanie naciśnięć klawiszy zostało aktywowane, co

spowodowało, że pismo zostało wyróżnione pogrubioną czcionką. Po raz drugi słowo zostało wpisane po dezaktywacji szyfrowania klawiszy. Podczas aktywacji keyloggera, zainstalowane oprogramowanie antywirusowe zostało ostrzeżone, że ten program może być niebezpieczny.

Aplikacje wydajności komputera

Aby komputer działał w najlepszym wydaniu, pliki i ich wzajemne relacje muszą być wolne od błędów. Dostępne są aplikacje, które skanują komputer, identyfikują błędy i przywracają pliki do prawidłowego stanu. Takie aplikacje obejmują następujące funkcje, które mają zapewnić stabilną pracę komputera i maksymalną dostępność zasobów.

• Naprawa rejestru

• Anti-rootkity

• Antywirus

• Niepotrzebne pliki

• Fragmentacja

Naprawa rejestru

W systemie operacyjnym rejestr plików - centralna baza danych systemu - ułatwia komunikację między plikami i dostęp do plików. Z czasem jednak gromadzą się stare i luźne pliki, które często są uszkodzone. Gdy wystąpią błędy rejestru, komputer zwalnia, aplikacje się zawieszają, a sam komputer często ulega awarii. „Naprawiając te przestarzałe informacje w rejestrze systemu Windows, system będzie działał szybciej i bezbłędnie” [14]. Tabela 8.4 zawiera listę typowych błędów wykrytych i naprawionych przez narzędzia do naprawy rejestru.

Anti-Rootkity

Rootkit to złośliwe oprogramowanie szpiegujące, które hakerzy wkładają do aplikacji lub systemu operacyjnego w celu utworzenia zapadni. Dostęp do zapadni omija wszystkie kontrole bezpieczeństwa. Dzięki tym zapadniom hakerzy omijają wszystkie środki bezpieczeństwa i uzyskują dostęp do zasobów jako autoryzowany użytkownik. „Rootkity mogą leżeć ukryte na komputerach i pozostać niewykryte przez oprogramowanie antywirusowe”. Anti-rootkity sprawdzają każdą nową instalację programu w poszukiwaniu programów szpiegujących. Usunięcie oprogramowania szpiegującego z aplikacji jest jak operacja chirurgiczna i musi zostać wykonane bez wpływu na nominalną wydajność aplikacji. Rootkity w programach zainstalowanych przed instalacją rootkita mogą nie zostać wykryte. Dlatego zaleca się ponowną instalację programów po instalacji programu antywirusowego.

Antywirusowe

Wirus to złośliwe oprogramowanie, które uszkadza pliki, powoduje problemy operacyjne i powoduje awarie aplikacji, a często także systemu operacyjnego. Najczęstszym działaniem wirusa jest pisanie na obszarach przeznaczonych dla systemu operacyjnego i sterowników lub na kodzie aplikacji.

Niepotrzebne pliki

Niepotrzebne pliki to pliki, które zostały odinstalowane przez procesy lub nie są już powiązane z żadną prawidłową aplikacją. Rezultatem jest szybszy wykonywanie aplikacji, usuwane byłyby niepotrzebne programy do czyszczenia plików

• Pliki tymczasowe systemu Windows

• Nieprawidłowe menu startowe

• Przestarzałe pliki w plikach programu

• Nieprawidłowe skróty

• Nieprawidłowe pliki msi

• Zdefiniowane przez użytkownika niepotrzebne pliki i foldery

• Puste pliki i foldery

• Nieprawidłowe pliki i foldery

Fragentacja

Termin fragmentacja odnosi się do sposobu zapełniania dysku twardego. Ponieważ miejsce na dysku twardym jest wykorzystywane do operacji ciągłego zapisu i usuwania, tworzone są puste przestrzenie zwane fragmentami. Fragmenty zapobiegają ładowaniu dużych aplikacji w sąsiadujących sektorach. Aplikacje przechowywane w różnych nieciągłych sektorach na dysku twardym wymagają użycia do zarządzania pamięcią, co spowalnia działanie konkretnej aplikacji. Defragmentacja próbuje skonsolidować całą dostępną przestrzeń razem, aby duże aplikacje mogły być instalowane bez partycji. Problemy spowodowane fragmentacją plików obejmują

• Awarie i system zawiesza się / zawiesza

• Powolne uruchamianie i komputery, które nie uruchamiają się

• Długi czas tworzenia kopii zapasowej i przerwana kopia zapasowa

• Uszkodzenie pliku i utrata danych

• Błędy w programach

• Wykorzystanie pamięci RAM i problemy z pamięcią podręczną

• Awarie dysku twardego

• Ogólna powolna wydajność serwera domino

• Długotrwałe blokady w dzienniku konsoli

• Limity czasu semaforów

Narzędzia ochronne

W wyniku bycia częścią cyberprzestrzeni system informacyjny jest narażony na wiele niebezpieczeństw. Na szczęście istnieje również wiele aplikacji cyberobrony, które minimalizują to ryzyko. Trochę aplikacje, które są łatwo dostępne, opisano poniżej.

Analizator bezpieczeństwa

Istnieje bardzo przydatne narzędzie oferowane bezpłatnie, które zapewnia dogłębną analizę cyberbezpieczeństwa hosta podłączonego do sieci. Jest to Microsoft Baseline Security Analyzer (MBSA). To narzędzie skanuje komputer i dla każdego wykrytego problemu generuje raport z analizy bezpieczeństwa

• Co zostało zeskanowane

• Szczegóły wyniku

• Jak to naprawić

MBSA może przeskanować pojedynczy komputer lub wiele komputerów lub może pobrać raporty ze skanowania z wcześniejszych analiz. MBSA to narzędzie systemu Windows, sprawdzające i raportujące następujące kwestie:

• Luki administracyjne w systemie Windows

• Luki administracyjne IIS (Internet Information Services)

• Luki administracyjne w SQL

• Aktualizacje bezpieczeństwa

Problemy sprawdzone przez MBSA obejmują

• Lokalne hasła dostępu

• Obecność

• Wygaśnięcie

• Siła

• Konfiguracja systemu plików

• uprawnienia administracyjne

• Konta gości

• Niekompletne aktualizacje

• Zapora systemu Windows

• Audyt zdarzeń - logowanie / wylogowywanie

• Zainstalowane usługi

• Wspólne zasoby - dyski

Raport przedstawia zidentyfikowane problemy i zawiera kroki dla rozwiązania każdego problemu. Jest to bardzo proste narzędzie, które musi być zainstalowane na każdym komputerze i często uruchamiane.

Analizator haseł

Istnieje wiele metod i oprogramowania do łamania haseł oraz znajomość „siły" używanych przez nas haseł może być bardzo ważna. Wiele systemów informatycznych automatycznie odrzuca przypisywanie „słabych" haseł. Istnieje wiele teorii na temat tego, co stanowi silne lub słabe hasło, i istnieje wiele mierników haseł w Internecie. Hasła takie jak hasło uzyskują wynik 8%, a hasło takie jak Uo5 $ Pw9 # 3 otrzymuje wynik 100%.

Hasła w systemach operacyjnych Windows są przechowywane w znanych lokalizacjach, ale w formie skrótowej. To znaczy hasło to przetaczane przez algorytm mieszający i generowany jest kod. Jednak znanych jest wiele algorytmów mieszających. Dlatego jeśli hasło hashcode odpowiada hashcode znanego hasła, można stwierdzić, że znaleziono nieznane hasło. Wśród aplikacji do wykrywania haseł

znajduje się oprogramowanie Cain & Abel Password Protection (C&A) , które zostało zaprojektowane dla systemów operacyjnych Microsoft i twierdzi, że wykonuje następujące czynności:

• Umożliwia łatwe odzyskanie kilku rodzajów haseł poprzez wąchanie sieci

• Łamanie zaszyfrowanych haseł za pomocą

• Atak słownikowy

• Brutalny atak

• Atak kryptoanalizy

• Nagrywanie rozmów VoIP

• Dekodowanie zaszyfrowanych haseł

• Odzyskiwanie kluczy sieci bezprzewodowej

• Ujawnianie skrzynek z hasłami

• Odkrywanie buforowanych haseł

• Analiza protokołów routingu

W technice Ataku Słownikowego obliczane są kody skrótu odpowiadające rzeczywistym słowom. Każdy hashcode jest porównywany z hashcode hasła. W przypadku dopasowania zakłada się, że słowo odpowiadające pasującemu hashcode jest poszukiwanym hasłem. Zaletą tej metody jest to, że jest ona dość szybka i prosta. Jeśli jednak hasło nie jest prawidłowym słowem, ale zawiera znaki specjalne lub cyfry, technika ta zawodzi.

W technice Ataku Brute Force generowane są skróty wszystkich możliwych kombinacji znaków, a ostatecznie znajduje się hasło. Proces ten może potrwać długo, w zależności od dostępnej mocy obliczeniowej, ale teoretycznie na końcu znajduje się hasło. W technice ataku kryptoanalizacyjnego w bazach danych dostępne są wstępnie obliczone kody skrótu odpowiadające rzeczywistym hasłom alfanumerycznym, zwane tablicami Rainbow. Hashcode hasła pobrany z listy komputerów PC jest porównywany z hashcodes w bazie danych, w której można znaleźć dopasowanie, w zależności od wielkości bazy danych. Dodatkowe usługi świadczone przez C&A obejmują:

Sniffer analizujący zaszyfrowane protokoły i analizujący sieć i ruch

Przeglądarka haseł, która może ujawniać hasła aplikacji Microsoft

Dumper, która zrzuca Tajemnice lokalnego organu bezpieczeństwa (LSA)

Dekoder haseł, który może ujawniać hasła połączeń telefonicznych przechowywane w systemie Windows

Bezprzewodowy skaner, który zbiera parametry identyfikacji i wydajności w dostępnych urządzeniach Wi-Fi, a także może przechwytywać i dekodować zaszyfrowane pliki 802.11

Skaner SID, który uzyskuje dostęp do zdalnego systemu i wydobywa zabezpieczenia identyfikatora

Filtr VoIP, który rejestruje rozmowy VoIP w formacie WAV

LAN Scanner, który rozpoznaje obecność snifferów sieciowych i systemów wykrywania włamań

Zapory ogniowe

Zapora to kontroler ruchu dla ruchu przychodzącego, wychodzącego lub dwukierunkowego. Oczekiwane korzyści z zapory ogniowej powinny obejmować

• Kontrolowany dostęp do zasobów korporacyjnych

• Zapobieganie nieautoryzowanemu dostępowi do aplikacji lub informacji

• Integracja z mechanizmami uwierzytelniania użytkowników

• Bezpieczne wdrażanie nowych aplikacji

• Ochrona firmowych adresów sieciowych przed Internetem

• Bezpieczny zdalny dostęp do sieci korporacyjnej

• Wykrywanie i zapobieganie włamaniom w całym przedsiębiorstwie

• Mechanizm filtrowania treści

Może to być wyłącznie oprogramowanie lub oprogramowanie zainstalowane na dedykowanym sprzęcie.

W stosie hierarchicznym zapora zwykle znajduje się w warstwie sieci, ale można ją również znaleźć w warstwie transportowej.

Filtrowanie na poziomie pakietów

Ponieważ wszystko w nowoczesnej sieci przenosi się w pakietach danych, filtrowanie odbywa się na poziomie pakietu. Pakiety zawierają liczby binarne lub kody, które zawierają następujące informacje:

• Pochodzenie pakietu - adres IP i numer portu

• Miejsce docelowe pakietu - adres IP i numer portu

• Informacje o protokole

• Znak czasu

• Ładunek - dane, polecenia lub potwierdzenie

• Informacje o wykrywaniu błędów

• Inne - serializacja danych, priorytet itp.

W filtrowaniu na poziomie pakietów, które jest instalowane w warstwie sieciowej, zapory ogniowe odbierają pakiety i oceniają ich potencjalne zagrożenie. Ocena oparta na powyższych trzech pierwszych parametrach (źródle, miejscu docelowym i protokole) zwykle kończy się jedną z dwóch poniższych opcji:

• Pakiety są przekazywane do miejsca docelowego.

• Pakiety są opóźniane, jeśli podejrzewa się atak DoS.

• Pakiety są odrzucane.

Jest to bardzo proste podejście do ochrony, ale można go oszukać za pomocą pakietów o sfałszowanych adresach. Termin sfałszowany odnosi się do fałszowania parametrów pakietu, głównie adresu IP.

Filtrowanie na poziomie obwodu

Ta kategoria zapór ogniowych jest zwykle instalowana w warstwie transportowej, gdzie weryfikuje sesję przed wydaniem oceny wiarygodności pakietów. Kryteriami są powyższe cztery pierwsze parametry (pochodzenie, miejsce docelowe, protokół i znacznik czasu), a także poświadczenia użytkownika - nazwa użytkownika i hasło. Przy takich kryteriach fałszowanie adresów IP nie jest jedynym decydującym czynnikiem w ocenie pakietu.

Brama na poziomie aplikacji

W tym przypadku zapora ogniowa to inteligentny serwer proxy chroniący host przed siecią. Zapora ogniowa dokonuje wymiany danych w sposób przezroczysty dla zdalnego systemu i może kontrolować przepływ pakietów w oparciu o wyrafinowane kryteria ustalone przez administratora sieci. Ten typ zapory często ma możliwość szyfrowania i deszyfrowania danych, co zwiększa bezpieczeństwo. Brama na poziomie aplikacji jest zdecydowanie najbezpieczniejszą zaporą ogniową, ale jednocześnie najbardziej złożoną, wymagającą własnego sprzętu.

Ochrona poczty e-mail

E-mail można chronić na trzy sposoby. Jednym z nich jest potężny klient poczty e-mail, który zapewnia szeroką ochronę, gdy wiadomości przychodzą do przeglądania.

Innym jest oprogramowanie zainstalowane na tym samym hoście z klientem e-mail i praca z klientem e-mail. Trzecie podejście to outsourcing, w którym system poczty elektronicznej organizacji jest rezydentem i jest zarządzany w chmurze. Chmura to termin opisujący korzystanie z Internetu , usługi zlecone na zewnątrz i znajdujące się poza siecią fizyczną organizacji. W chmurze „jest hostowany poza… [siecią organizacji]… sieci, nie wymagając dodatkowego sprzętu, oprogramowania ani zasobów ludzkich do zarządzania codziennymi operacjami bezpieczeństwa". Postępy w technologiach szkodliwego oprogramowania wymagają bezpiecznych systemów pocztowych gdzie oczekiwane funkcje i korzyści obejmują:

• Filtrowanie poczty przychodzącej

• Filtrowanie wiadomości wychodzących

• Filtrowanie antyspamowe w wielu językach

• Blokowanie złośliwego oprogramowania

• Kwarantanna spamu

• Kontrola załączników antimalware

• Usunięcie regulowanych treści

• Szyfrowanie i deszyfrowanie w celu przechowywania lub transportu

• Egzekwowanie zasad korporacyjnych

• Odzyskiwanie po awarii

• Archiwizacja wiadomości e-mail

Zaawansowane systemy filtrowania powiadamiają o rozpoznawaniu obrazów, jeśli treść wiadomości e-mail lub załączniki zawierają obrazy z podpisami cyfrowymi, które spełniają określone cechy. Dodatkowe korzyści zapewniane przez oparty na chmurze system poczty elektronicznej obejmują

• Brak sprzętu lub oprogramowania do zainstalowania lub zarządzania

• Brak nakładów kapitałowych z góry, kosztów instalacji i aktualizacji

• Obsługa klienta 24 × 7

• Automatyczne włączanie i synchronizacja w celu zapewnienia ciągłości

• Zintegrowana internetowa konsola administracyjna dla wszystkich rozwiązań

• Powiadomienia o naruszeniach zasad, zablokowanych treściach i poddanych kwarantannie wiadomości

• Ochrona przed atakami

Typowe ataki na systemy pocztowe obejmują DoS i próby kopiowania katalogów.

Cyberprzestrzeń i prawo

Cyberprzestrzeń jest dziś jedną z wielkich granic prawnych. Stein Schjolber

Wprowadzenie

Gdy tylko cyberprzestrzeń i handel elektroniczny powstały w połowie lat 90., cyberprzestępczość rozkwitła równolegle. Cyberprzestępczość podwaja się każdego roku pod względem liczby incydentów, a także strat pieniężnych. Niemożliwe jest określenie ilościowe cyberprzestępczości, ponieważ większość ofiar widzi dalsze straty w reklamowaniu swojej niezdolności do obrony przed tym współczesnym zagrożeniem. Ciekawe jest to, że spośród złapanych cyberprzestępców zdecydowana większość przyznała się do winy. Wynika to z faktu, że zebrane fakty - zapisy ruchu sieciowego - powodują hermetyczne przypadki. Jeśli chodzi o upowszechnianie przepisów dotyczących walki z cyberprzestępczością, „tekst będzie musiał zachować pewną elastyczność, pozwalając na względnie zmienny charakter różnych form cyberprzestępczości i szybkość, z jaką rozwijają się nowe technologie". Wszelkie traktaty międzynarodowe, które mają być egzekwowane na poziomie krajowym, muszą zostać dostosowane w „odpowiednim i proporcjonalnym ustawodawstwie krajowym". Jednak traktatom międzynarodowym nie jest łatwo ustanowić „wspólne definicje przestępstw, (i)… procedur bezpieczeństwa". Chociaż nikt nie będzie się sprzeciwiał potrzebie ustanowienia skutecznych środków zwalczania cyberprzestępczości, konieczne jest, aby wszelkie takie środki w żaden sposób nie naruszały praw obywateli do prywatności i wolności jednostki.

Prawo międzynarodowe

Ustawodawcy i organy ścigania na całym świecie opowiadają się za potrzebą przepisów prawa cybernetycznego napisanych w języku cybernetycznym. Oznacza to, że przepisy prawne wyraźnie określają cyberprzestępstwa i w pełni popierają akceptację dowodów cybernetycznych. Organy międzynarodowe, odpowiadając na to wezwanie, zwołały i opracowały traktaty i konwencje, które niestety nie dały całkowitej akceptacji państwom członkowskim. Udział kraju w określonej umowie międzynarodowej staje się skuteczny tylko wtedy, gdy zostaną opracowane i zatwierdzone przepisy krajowe, które regulują cel podpisanej umowy międzynarodowej. Oczywiście z biegiem czasu coraz więcej krajów ogłasza prawa cybernetyczne

Europa

W Europie w 2004 r. Rada Europy zaakceptowała projekt Traktatu o cyberprzestępczości, który został zaproponowany krajom na całym świecie. Podczas gdy wiele krajów zostało sygnatariuszami traktatu, tylko kilka faktycznie ogłosiło przepisy krajowe zgodne z traktatem. Interesujące jest, aby traktat w artykule 47 stanowił: „Wypowiedzenie: każda ze Stron może w dowolnym czasie wypowiedzieć niniejszą konwencję w drodze notyfikacji skierowanej do Sekretarza Generalnego Rady Europy". Artykuł 27 stanowi: „Wnioski o wzajemną pomoc na podstawie niniejszego artykułu będą wykonywane zgodnie z procedurami określonymi przez Stronę wzywającą, chyba że jest to niezgodne z prawem Strony wezwanej. Strona wezwana może… odmówić udzielenia pomocy ". Później w 2006 r. Do traktatu dołączono kontrowersyjne uzupełnienie [4], które przyciągnęło mniejszą liczbę krajów sygnatariuszy. Dodatek dotyczył strachu przed pojawieniem się ksenofobicznej troski Internet. Podsumowując, rozpoczęła się inicjatywa Rady Europy sposób na ustawodawstwo krajowe dotyczące cyberprzestępczości w wielu krajach i został wykorzystany jako motywacja do podobnego traktatu w ONZ.

Organizacja Narodów Zjednoczonych

Organizacja Narodów Zjednoczonych (ONZ) w 2010 r. Otrzymała propozycję zalecającą Traktat o cyberprzestrzeni dla członków ONZ. Po długiej debacie propozycja została odrzucona, ponieważ zawierała niedopuszczalne artykuły. Większość kontrowersji wywołały następujące artykuły:

• Artykuł 2 wniosku wskazywał na przewagę takiego traktatu nad przepisami krajowymi, stwierdzając, że „Poważne zbrodnie przeciwko pokojowi i bezpieczeństwu w cyberprzestrzeni powinny być uznawane za przestępstwa na mocy prawa międzynarodowego na mocy traktatu o cyberprzestrzeni na szczeblu Narodów Zjednoczonych, niezależnie od tego, czy były karalne czy nie. zgodnie z prawem krajowym ". Ten fragment został uznany za dwuznaczny i obraźliwy dla suwerenności narodowej.

• W art. 3.8.3, odnoszącym się do odpowiednika traktatu Unii Europejskiej, stwierdzono, że „Dane… danych o ruchu internetowym i danych transakcyjnych, zwykle telekomunikacji, wiadomości e-mail i odwiedzanych witryn [należy zachować] Celem zatrzymywania danych jest analiza danych o ruchu i masowe nadzór danych… " Wniosek sugerował, że dane należy przechowywać „przez okres od sześciu miesięcy do dwóch lat". Artykuł ten spotkał się z sprzeciwem wielu lokalnych i międzynarodowych organizacji działających na rzecz wolności obywatelskich, które uznały to sformułowanie za obraźliwe, szczególnie za „masową inwigilację danych" i wyraźne naruszenie podstawowych praw obywatelskich, których kamieniem węgielnym jest prywatność w komunikacji osobistej.

• Artykuł 4 był najbardziej kontrowersyjny. W efekcie w tym artykule wzywa się państwa członkowskie do zaakceptowania Międzynarodowego Trybunału Karnego jako super-arbitra w cyberprzestępstwach, stwierdzając:

„Każdy, kto popełni którekolwiek z przestępstw… będzie podlegał ściganiu przez sąd… Maksymalny okres pozbawienia wolnościma 30 lat i może zostać nałożony wyrok dożywocia ".

Tak więc ONZ pozostaje idealnym międzynarodowym forum do dyskusji i wymiany pomysłów, ale nie jest idealny do zawarcia międzynarodowego konsensusu. Jednak umowy dwustronne lub regionalne bardzo często wystarczają do podpisania traktatów globalnych. Europol jest przykładem.

NATO

Organizacja Traktatu Północnoatlantyckiego (NATO) , mając na uwadze przede wszystkim obronę i bezpieczeństwo, również obserwuje globalną rolę na arenie cyberbezpieczeństwa. Artykuł pojawiający się na stronie internetowej cyberbezpieczeństwa NATO. Centrum sugeruje, że „Globalne bezpieczeństwo cybernetyczne [może być] Niszą dla NATO". Zainteresowaniem NATO jest cyberterroryzm i cyberwarfare, ale drzwi do cyberprzestępczości pozostały otwarte, jak stwierdzono w polityce bezpieczeństwa cybernetycznego organizacji. Chociaż w wielu państwach członkowskich NATO Internet jest szeroko wykorzystywany, nie odgrywa żadnej roli w ich bezpieczeństwie narodowym, ani nie stanowi absolutnego filaru społecznego ani gospodarczego. Dlatego postawa członkostwa nie będzie jednolita wobec inwestowania przeciwko cyberterroryzmowi lub cyberwarfare, biorąc pod uwagę „dominującą niechęć narodów [członkowskich] do angażowania się w [kosztowne] wiążące inicjatywy międzynarodowe". W sformułowaniu w 2011 r. Strategicznej koncepcji sojuszu na rzecz obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego przyjętej przez szefów państw i rządów w Lizbonie kwestię bezpieczeństwa cybernetycznego rozwiązano w następujący sposób:

Artykuł 12. Cyberataki stają się coraz częstsze, bardziej zorganizowane i bardziej kosztowne w związku ze szkodami, jakie wyrządzają administracjom rządowym, przedsiębiorstwom, gospodarkom, a potencjalnie także sieciom transportowym i dostawom oraz innej krytycznej infrastrukturze; mogą osiągnąć próg, który zagraża dobrobytowi krajowemu i euroatlantyckiemu, bezpieczeństwu i

stabilności. Zagraniczne służby wojskowe i wywiadowcze, zorganizowani przestępcy, grupy terrorystyczne i / lub ekstremistyczne mogą być źródłem takich ataków.

Sojusz utrzymuje Centrum Doskonałości Obrony Bezpieczeństwa Cybernetycznego w Tallinie w Estonii, którego misją jest „zwiększenie zdolności, współpracy i wymiany informacji między NATO, narodami NATO i partnerami w zakresie cyberobrony… [i] być głównym źródłem wiedzy specjalistycznej w dziedzina kooperacyjnej cyberobrony… w ramach NATO, narodów i partnerów NATO ". Na ostatniej konferencji poświęconej cyberbezpieczeństwu w Centrum przedstawiono dziesięć zasad, które stanowią podstawę skutecznej cyberobrony na szczeblu suwerennego państwa. Druga zasada jest jednak całkowicie nie do przyjęcia, ponieważ obwinia sektor publiczny państwa za działanie, które mogło zostać zainicjowane przez nieuczciwą lub tajną organizację działającą w tym państwie.

1. Zasada terytorialności: infrastruktura informacyjna znajdująca się na terytorium państwa podlega suwerenności terytorialnej tego państwa.

2. Zasada odpowiedzialności: fakt, że cyberatak został przeprowadzony z systemu informatycznego znajdującego się na terytorium państwa, świadczy o tym, że czyn można przypisać temu państwu.

3. Zasada współpracy: fakt, że cyberatak został przeprowadzony za pośrednictwem systemów informatycznych znajdujących się na terytorium państwa, stwarza obowiązek współpracy z państwem ofiary.

4. Zasada samoobrony: Każdy ma prawo do samoobrony.

5. Zasada ochrony danych: Dane monitorowania infrastruktury informacyjnej są postrzegane jako dane osobowe, chyba że postanowiono inaczej (powszechna interpretacja w UE).

6. Zasada obowiązku zachowania ostrożności: każdy ma obowiązek zapewnienia rozsądnego poziomu bezpieczeństwa w swojej infrastrukturze informatycznej.

7. Zasada wczesnego ostrzegania: istnieje obowiązek powiadomienia potencjalnych ofiar o znanym, nadchodzącym cyberbezpieczeństwie.

8. Zasada dostępu do informacji: Społeczeństwo ma prawo być informowanym o zagrożeniach dla ich życia, bezpieczeństwa i dobrobytu.

9. Reguła kryminalna: Każdy naród ma obowiązek zawrzeć w swoim prawie karnym najczęstsze cyberprzestępstwa.

10. Zasada mandatu: Zdolność organizacji do działania (i regulowania) wynika z jej mandatu.

INTERPOL

Międzynarodowa Organizacja Policji Kryminalnej (INTERPOL) „jest największą międzynarodową organizacją policji na świecie, z 190 krajami członkowskimi… [z wybitną] zaawansowaną technologicznie infrastrukturą wsparcia technicznego i operacyjnego" . INTERPOL odgrywa wiodącą rolę w szkoleniu organów ścigania na całym świecie w zakresie najlepszych sposobów obrony przed cyberatakami i złośliwym oprogramowaniem, koncentrując się na

•Analiza trendów cyberataków

•Praktyczne wykorzystanie cyfrowych narzędzi kryminalistycznych w incydentach cyberbezpieczeństwa

•Techniki analizy dowodów i odzyskiwania

•Analiza techniczna złośliwego oprogramowania i botnetów

INTERPOL utrzymuje międzynarodowy sojusz cyberbezpieczeństwa na pierwszej linii obrony - organy ścigania - mające na celu

• Promowanie wymiany informacji między krajami członkowskimi poprzez regionalne grupy robocze i konferencje

• Prowadzenie szkoleń w celu budowania i utrzymywania standardów zawodowych

• Koordynacja i wspieranie operacji międzynarodowych

• Ustanowienie globalnej listy oficerów kontaktowych dostępnych przez całą dobę do celów dochodzeń w sprawie cyberprzestępczości

• Pomoc krajom członkowskim w przypadku ataków cybernetycznych lub dochodzeń w sprawie cyberprzestępczości za pośrednictwem usług śledczych i baz danych

• Rozwijanie strategicznych partnerstw z innymi organizacjami międzynarodowymi i organami sektora prywatnego

• Identyfikacja pojawiających się zagrożeń i dzielenie się tymi danymi wywiadowczymi z krajami członkowskimi

• Zapewnienie bezpiecznego portalu internetowego umożliwiającego dostęp do informacji operacyjnych i dokumenty

Utrudnienia dla egzekwowania prawa w cyberprzestrzeni

Międzynarodowe traktaty mogą zostać sporządzone i podpisane, a miejmy nadzieję, że nastąpi po nich publikacja krajowych przepisów, które skutecznie zajmą się cyberprzestępczością. To tylko część pierwsza w niekończącej się walce z cyberprzestępczością. Część druga dotyczy faktycznego usunięcia cyberprzestępców ze społeczeństwa. Obecnie istnieje kilka obszarów, które wymagają definicji lub ulepszenia, a niektóre z nich wymieniono poniżej.

• Biurokracja narodowa. W większości krajów systemy sądowe są przeciążone, a sprawy mają być rozpatrywane rok lub dwa lata po sformalizowaniu i złożeniu oskarżenia. Do tego czasu oskarżeni, jeśli są winni, mogą mieć prawo do popełniania większej liczby cyberprzestępstw.

• Sędziowie o umiejętnościach cybernetycznych. Najczęściej przestępstwa popełnione w cyberprzestrzeni obejmują włamania do sieci i naruszenia bezpieczeństwa, które są częścią wysoce wyrafinowanych programów oszustw. Sędziowie bez specjalnego i ustawicznego szkolenia mogą nie rozumieć, dlaczego oskarżony jest winny lub niewinny zarzutów.

• Uwierzytelnianie dowodów. Jeśli nagłówek wiadomości e-mail zawiera adres e-mail oskarżonego, to samo w sobie niekoniecznie jest dowodem winy lub niewinności.

• Utrata dowodów. Przy dużej luce między popełnieniem domniemanego przestępstwa a sądowym rozpoznaniem sprawy dowody elektroniczne mogą zostać utracone lub zmienione.

• Dostęp do dowodów. Dowody mogą znajdować się na serwerach w obcym kraju i mogą być wymagane specjalne procedury ekstradycji danych.

• Kompleksowe prawodawstwo. Ponieważ programy cyberprzestępczości wyprzedzają organy ścigania o kilka miesięcy, do procesu wprowadzane są dodatkowe opóźnienia.

• śledczy w sprawie cyberprzestępczości. Wraz z eksplozją Internetu i równoległą eksplozją cyberprzestępczości nie ma na świecie kraju, który miałby wystarczającą liczbę pracowników policji cybernetycznej do prowadzenia każdego przypadku domniemanej cyberprzestępczości.

Według wszystkich standardów cyber legalny system jest w stanie embrionalnym. Jednak poprawia się na całym świecie i jest to uzasadnione mam nadzieję, że cyberprzestępczość zostanie powstrzymana w najbliższej przyszłości.

Przepisy dotyczące cyberprzestrzeni w Stanach Zjednoczonych

Przed stworzeniem cyberprzestrzeni, jaką znamy dzisiaj, istniała inna przestrzeń kosmiczna - choć nie została zidentyfikowana jako taka - Dataspace. Dzięki postępom w fizyce i chemii półprzewodników komputery analogowe przekształciły się w cyfrowe, a rozmiar sprzętu zaczął się zmniejszać, stopniowo osiągając dzisiejszy rozmiar i moc obliczeniową. Dataspace - era cyfrowego przechowywania informacji - rozpoczęła się w latach sześćdziesiątych i w połowie lat siedemdziesiątych. Wiele firm zaczęło mieć minikomputery do ich obsługi i rachunkowości , a jednocześnie zaczęły pojawiać się obawy dotyczące prywatności danych i bezpieczeństwo komputerowe, co skutkuje ogłoszeniem przepisów dotyczących ochrony danych, prywatności i bezpieczeństwa narodowego.

Krajowa ustawa o ochronie cybernetycznej z 2014 r

Krajowa ustawa o cyberbezpieczeństwie i ochronie infrastruktury krytycznej z 2014 r. Jest fundamentalnym prawem Stanów Zjednoczonych, które w pełni zajmuje się Internetem i możliwymi zagrożeniami, z którymi się wiąże, mające na celu „Zabezpieczenie Nation Against Cyber Attack. ” Najważniejsze jest to, że prawo zawiera definicję prawną tego, czym jest „incydent cybernetyczny”. Mianowicie „incydent cybernetyczny” jako incydent lub próba spowodowania incydentu, który, jeśli się powiedzie,: (1) zagrozi bezpieczeństwu, integralności, poufności, lub dostępność systemu informacyjnego lub sieci lub jakichkolwiek informacji przechowywane w takim systemie, przetwarzane w nim lub przejeżdżające przez niego; (2) naruszają prawa lub procedury związane z bezpieczeństwem systemu, polityką dopuszczalnego użytkowania lub aktami terroryzmu wymierzonymi przeciwko takiemu systemowi lub sieci; lub (3) odmawiać dostępu do lub degradować, zakłócać lub niszczyć taki system lub sieć, lub porażki w działaniu lub kontroli technicznej takiego systemu lub sieci. Prawo wprowadza National Institute of Standards and Technology (NIST) w celu ułatwienia publiczno-prywatnej współpracy w zakresie bezpieczeństwa cybernetycznego w celu opracowania dobrowolnego, kierowanego przez przemysł zestawu standardów i procesów w celu zmniejszenia ryzyka cybernetycznego infrastruktury krytycznej. Ustawa zmienia również Ustawę o bezpieczeństwie wewnętrznym, dodając przepisy zatytułowane Ustawa o bezpieczeństwie wewnętrznym w zakresie cyberbezpieczeństwa, które rozwijają kategorie zawodowe w zakresie bezpieczeństwa cybernetycznego - po raz pierwszy w rządzie federalnym. W skrócie, prawo uznaje potrzebę stworzenia armii cyberbezpieczeństwa.

Ustawa o ocenie siły roboczej z cyberbezpieczeństwa z 2014 r

Ustawa o ocenie siły roboczej w cyberbezpieczeństwie - kieruje sekretarz Sekretarz Bezpieczeństwa Wewnętrznego, aby przeprowadzić ocenę cyberbezpieczeństwa, personel Departamentu Bezpieczeństwa Wewnętrznego (DHS), który powinien zawierać informacje na temat

• Gotowość i zdolność takiej siły roboczej do wypełnienia misji bezpieczeństwa cybernetycznego;

• Gdzie stanowiska pracowników cyberbezpieczeństwa znajdują się w DHS;

• Które takie stanowiska są wykonywane przez stałych pełnoetatowych pracowników DHS, niezależnych wykonawców oraz osoby zatrudnione przez inne agencje federalne;

• Które z tych stanowisk są wolne

• Odsetek osób w każdej kategorii bezpieczeństwa cybernetycznego i specjalizacji, które zostały przeszkolone w zakresie wykonywania pracy; i

• W jakich przypadkach takie szkolenie nie zostało przeprowadzone, jakie wyzwania napotkano na temat zapewnienia takiego szkolenia.

Ustawa o rekrutacji i zatrzymaniu pracowników w zakresie cyberbezpieczeństwa z 2014 r

Jest to bardzo ważne prawo, ponieważ upoważnia Sekretarza Departamentu Bezpieczeństwa Wewnętrznego w celu ustalenia stanowisk w Departamencie Bezpieczeństwa Wewnętrznego (DHS) niezbędnych do wykonywania obowiązków związanych z cyberbezpieczeństwem. Ponadto wymaga od DHS dostarczenia rządowi wskazówek identyfikujących ostre i pojawiające się niedobory umiejętności w zakresie cyberbezpieczeństwa.

Ustawa o ochronie prywatności w prawie handlowym z 2011 r

Celem tego aktu jest „Ustanowienie ram regulacyjnych dla kompleksowej ochrony danych osobowych osób fizycznych pod egidą Federalnej Komisji Handlu i do innych celów". Zostało to uznane za

• Rozpowszechnianie informacji umożliwiających identyfikację osób (PII) budzi obawy, że może to prowadzić do kompromisów w zakresie prywatności danych, bezpieczeństwa danych i równie ważnej integralności danych.

• Nadużycie w gromadzeniu, przechowywaniu, dystrybucji i wykorzystywaniu danych osobowych spowodowało już wiele różnych przestępstw, głównie cyberprzestępstw, co negatywnie wpłynęło na rozwój wiarygodnego handlu elektronicznego.

• Brakuje, a jednocześnie potrzeba ram prawnych zapewni to jednolite i kompleksowe stanowisko rządu w odniesieniu do postępowania z danymi osobowymi.

Biorąc pod uwagę powyższe, amerykańscy prawodawcy opracowali i uchwalił to prawo, które kieruje prokuratorami generalnymi pięćdziesięciu stanów wraz z Federalną Komisją Handlu (FTC) w celu ustalenia szczegółowych zasady jednolitego systemu prawnego obejmującego cały stan, który będzie chronił informacje osobowe w ramach kompleksowy sposób. Najważniejsze cechy tego prawa są następujące:

• Odpowiedzialność. Wszystkie podmioty objęte tym podmiotem ochrony danych osobowych w trakcie prowadzenia działalności gospodarczej - muszą „ponosić odpowiedzialność zarządczą [za dane znajdujące się pod ich opieką]". W obecnym kontekście odpowiedzialność kierownictwa za dane oznacza istnienie zasad dotyczących gromadzenia, przetwarzania, przechowywania, bezpieczeństwa fizycznego i wirtualnego, dystrybucji na rzecz osób trzecich oraz wykorzystywania danych zaklasyfikowanych jako informacje umożliwiające identyfikację osób.

• Prywatność od samego początku. We wszystkich aspektach przetwarzania danych priorytetem musi być prywatność danych. Można to osiągnąć, stosując „odpowiednie procesy i praktyki zarządzania w całym cyklu życia danych".

• Przejrzystość. Osoby gromadzące dane, zarówno w cyberprzestrzeni, jak i gdzie indziej, muszą „zapewniać jasne, zwięzłe i terminowe zawiadomienie osób fizycznych" w zakresie zarządzania zebranymi danymi PII.

• Indywidualny udział. Posiadacze danych osobowych muszą „oferować osobom fizycznym solidny, przejrzysty i rzucający się w oczy mechanizm", aby umożliwić lub zabronić korzystania z ich informacji osobowych i móc w dowolnym momencie zmienić ten status.

• Minimalizacja danych. Dane dotyczące osoby fizycznej, gromadzone w trakcie świadczenia usługi, muszą zostać zminimalizowane i muszą być „takie, jak jest to uzasadnione".

• Ograniczenia w dystrybucji informacji. Osoby zbierające dane osobowe przekazujące takie dane stronom trzecim muszą „wymagać na mocy umowy, aby taka strona trzecia" w pełni przestrzegała tego prawa w zakresie zarządzania danymi. Ponadto przekazywanie danych osobowych do „niewiarygodnych stron trzecich [jest] zabronione".

• Integralność danych. Osoby zbierające dane osobowe muszą dołożyć wszelkich starań, poprzez odpowiednie zasady, praktyki i mechanizmy, aby zapewnić, że wykorzystywane „dane osobowe […] są dokładne [zwłaszcza, gdy takie informacje]… mogą być wykorzystane do odmowy konsumentom korzyści lub wyrządzenia znacznej szkody".

• Egzekwowanie i kary. Ustawa ta nakazuje FTC ogłaszanie przepisów dotyczących wiedzy i dążenie do ich egzekwowania. Kary będą oparte na skali naruszeń i czasie, przez jaki naruszenia te zostały popełnione.

• Przepisy dotyczące bezpiecznej przystani. Prawo przyznaje FTC uprawnienia do wprowadzania programów „bezpiecznej przystani". Bezpieczna przystań to termin prawny odnoszący się do zmiany, zmniejszenia lub zniesienia zobowiązań strony w stosunku do przepisów określonych przepisów prawa. Takie odstępstwa od zobowiązań prawnych rozciągają się na nazwę większego dobra. Programy takie miałyby zastosowanie do podmiotów zbierających dane, podlegających jurysdykcji tego prawa, dopóki intencja tego prawa pozostaje w mocy, czyli ochrona prywatności jednostki.

Ustawa o ochronie prywatności w prawie handlowym z 2011 r.

Nie przewiduje szczegółowych zasad dotyczących kwestii zarządzania danymi osobowymi, ale upoważniają one FTC, która nadzoruje handel i najlepiej nadaje się do takiego zadania, do opracowywania zasad i środków, które ostatecznie ochronią dane osobowe i zminimalizują nadużycia i cyberprzestępczość.

Ustawa o cyberbezpieczeństwie z 2010 r

Celem tego aktu jest zapewnienie ciągłego swobodnego przepływu handlu w Stanach Zjednoczonych i ze swoimi globalnymi partnerami handlowymi poprzez bezpieczną komunikację cybernetyczną, zapewnienie dalszego rozwoju i wykorzystania Internetu i komunikacji intranetowej do takich celów, aby zapewnić rozwój kadry specjalistów w dziedzinie technologii informatycznych w celu poprawy i utrzymania skutecznej obrony cyberbezpieczeństwa przed zakłóceniami oraz do innych celów.

Zostało to uznane za

• Cyberprzestrzeń jest integralną częścią społeczeństwa amerykańskiego i bardzo ważną infrastrukturą dla wszystkich aspektów życia, przy czym Biały Dom określa ją jako strategiczny atut narodowy.

• Internet nie jest tak bezpieczny, jak powinien, biorąc pod uwagę z jednej strony jego znaczenie i wartość dla Stanów Zjednoczonych, az drugiej rosnące zagrożenia w postaci cyberprzestępczości i ataków terrorystycznych.

• Potrzebna jest kompleksowa strategia bezpieczeństwa narodowego, a także poprawa jakości i ilości cyberbezpieczeństwa

Zainteresowani powyższymi obawami amerykańscy prawodawcy opracowali i uchwalili to prawo, kierując jego wdrażanie raczej do prezydenta USA niż do agencji rządowej, jak w większości przypadków.

Oto główne punkty prawa:

• Certyfikaty. Prawo dotyczy zapotrzebowania na wykwalifikowanych specjalistów ds. Bezpieczeństwa cybernetycznego, czego warunkiem wstępnym jest „akredytacja, szkolenie i programy certyfikacji w zakresie bezpieczeństwa cybernetycznego".

• Stypendia cyberbezpieczeństwa. Prawo nakazuje Narodowej Fundacji Nauki, by „ustanowiła Federalny program stypendiów cybernetycznych służący rekrutacji i szkoleniu nowej generacji specjalistów w dziedzinie technologii informatycznych". Program ma zapewnić 1000 absolwentów i studentów pełnych stypendiów rocznie na programy prowadzące do cyberbezpieczeństwa. Co więcej, talentów należy szukać nawet wśród uczniów szkół średnich, „w celu promowania świadomości bezpieczeństwa komputerowego w klasach średnich i licealnych".

• Konkursy cyberbezpieczeństwa. Prawo nakazuje Narodowemu Instytutowi Standardów i Technologii ustanawiać konkursy z zakresu bezpieczeństwa cybernetycznego i inne wyzwania z nagrodami, aby „przyciągać, identyfikować, oceniać i rekrutować utalentowane osoby do federalnej siły roboczej w dziedzinie technologii informatycznych… [oraz w celu]… stymulować innowacje w podstawowych i stosowanych badaniach w zakresie bezpieczeństwa cybernetycznego. "

• Plan siły roboczej w zakresie bezpieczeństwa cybernetycznego. Uznając, że cyberbezpieczeństwo wymaga cyber-wojowników, prawo uwzględnia potrzebę opracowania planu dla każdej agencji rządowej, który zapewni jakość i ilość w jej cyberobronie. Plan obejmuje „prognozy dotyczące zatrudniania w dziedzinie cyberbezpieczeństwa… długoterminowe i krótkoterminowe planowanie strategiczne mające na celu zaradzenie niedoborom umiejętności krytycznych… strategie rekrutacji… szkolenia związane z cyberbezpieczeństwem", tak aby cyberprzestrzeń była bezpieczna.

• Wskazówki dotyczące bezpieczeństwa cybernetycznego NIST. Prawo uznaje National Institute of Standards and Technology (NIST) za autorytet technologiczny w obszarze cyberprzestrzeni i cyberbezpieczeństwa i zaleca mu „promowanie kontrolowanych, opracowanych przez sektor prywatny technik pomiaru ryzyka cyberbezpieczeństwa, środków zarządzania ryzykiem i najlepszych praktyk", które mogą później służą jako standardy oceny gotowości do cyberbezpieczeństwa.

• Rozwój wiedzy w zakresie cyberbezpieczeństwa. Prawo podkreśla potrzebę ciągłego rozwoju wiedzy, umiejętności i specjalistów posiadających wiedzę specjalistyczną w zakresie projektowania „złożonych systemów wymagających dużego oprogramowania, które są bezpieczne i niezawodne… [które] gwarantują prywatność tożsamości, informacji lub legalnych transakcji. "

• Panel doradczy ds. Cyberbezpieczeństwa. Ustawiając prezydenta jako centralny punkt jego realizacji, prawo wzywa do utworzenia panelu złożonego z wykwalifikowanych „przedstawicieli przemysłu, organizacji akademickich, organizacji non-profit, grup interesu i organizacji rzeczniczych", które będą

doradzać prezydentowi w „sprawach odnoszące się do krajowego programu i strategii bezpieczeństwa cybernetycznego. ”

Ustawa o cyberbezpieczeństwie z 2010 r.

Stanowi punkt wyjścia dla stworzenia planu podnoszenia świadomości w zakresie bezpieczeństwa cybernetycznego, który dzięki polityce, wytycznym i dużym środkom zapewni wykwalifikowanych specjalistów ds. bezpieczeństwa cybernetycznego, którzy będą bronić zarówno sektora publicznego, jak i prywatnego przed cyberprzestępczością i cyberbezpieczeństwem.

Federalna ustawa o zarządzaniu bezpieczeństwem informacji z 2002 r

W 1987 r. Amerykańscy prawodawcy, widząc wzrost przetwarzania danych i rosnące wykorzystanie komputerów, uchwalili ustawę - Computer Security Act z 1987 r. - która zapewniła pewne podstawowe, według dzisiejszych standardów, wytyczne dotyczące bezpieczeństwa i ogólnego traktowania danych. W 2002 roku uświadomiono sobie, że zagrożenia zostały pomnożone przez kilka rzędów wielkości oraz zarządzanie bezpieczeństwem systemów i danych wymagało zorganizowanego podejścia. Federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) ustanawia standardy, które muszą spełnić agencje federalne i federalni kontrahenci, które są wymierne i mierzalne. FISMA poleca szefom agencji ustanowienie i wdrożenie polityk i procedur w celu zminimalizowania ryzyka i zagrożeń dla rządowych systemów informacyjnych. Odpowiedzialność za stworzenie niezbędnych standardów spoczywała na NIST, w celu zapewnienia jednolitych standardów bezpieczeństwa informacji w całym rządzie, które zapewnią integralność, dostępność i bezpieczeństwo danych. FISMA stanowi kamień milowy w formułowaniu zasad zgodności w zakresie bezpieczeństwa informacji, a jego cel obejmuje następujące cele:

• Zapewnienie kompleksowych ram dla zapewnienia skuteczności kontroli bezpieczeństwa informacji nad zasobami informacji, które wspierają operacje federalne i zasoby

• Zapewnienie rozwoju i utrzymania minimalnych kontroli wymaganych do ochrony federalnych informacji i systemów informatycznych

• Zapewnienie mechanizmu lepszego nadzoru nad programami bezpieczeństwa informacji agencji federalnych

• Uznanie, że wybór konkretnych technicznych rozwiązań w zakresie bezpieczeństwa informacji o sprzęcie i oprogramowaniu należy pozostawić indywidualnym agencjom spośród produktów opracowanych na rynku

Najważniejsze cechy FISMA są następujące:

• Obowiązki. Prawo nakłada na szefa agencji wszelkie obowiązki związane z zapewnieniem bezpieczeństwa wszystkich informacji znajdujących się pod nadzorem agencji, gdzie poziom bezpieczeństwa powinien być „współmierny do ryzyka i wielkości szkody wynikającej z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacja lub zniszczenie ”przechowywanych informacji.

• Planowanie. Agencje mogą opracować własny program bezpieczeństwa w celu ochrony swoich informacji, nawet jeśli ich informacje nie znajdują się w ich własnych lokalach - dotyczy to wykonawców i stron satelitarnych.

• Raportowanie. Zgodność z duchem i listem FISMA zostanie wykazana w rocznym raporcie, który szef każdej agencji przygotuje, wraz z dystrybucją obejmującą:

• Dyrektor FISMA w Departamencie Handlu

• Domowe komisje ds. Reformy rządu i nauki

• Senackie komisje spraw rządowych, handlu, nauki i transportu

• Komisje ds. Środków

• Biuro Generalnego Kontrolera (OCG). OCG poświadczy „na temat adekwatności i skuteczności polityk, procedur i praktyk bezpieczeństwa informacji oraz zgodności z wymogami… [FISMA]".

• Niezależne oceny. Każdego roku każda agencja będzie podlegać niezależnej ocenie przeprowadzonej przez Generalnego Inspektora Agencji „powołanego na podstawie Ustawy Generalnej Inspektora z 1978 r.… Lub przez niezależnego audytora zewnętrznego, zgodnie z ustaleniami Generalnego Inspektora agencji".

Raport FISMA z 2010 r. Komisji Papierów Wartościowych i Giełd (SEC), agencji rządu federalnego, można obejrzeć online]. Raport przygotowany przez niezależnego kontrahenta zawiera ustalenia Generalnego Inspektora ze szczegółowymi zaleceniami dotyczącymi ulepszenia systemu informacyjnego SEC pod względem bezpieczeństwa danych.

US PATRIOT Act z 2001 roku

Cel USA PATRIOT (Zjednoczenie i wzmocnienie Ameryki poprzez zapewnienie odpowiednich narzędzi wymaganych do przechwytywania i

Ustawą o przeciwdziałaniu terroryzmowi, znaną również jako Ustawa o patriocie, jest „Odstraszyć

i karać akty terrorystyczne w Stanach Zjednoczonych i na całym świecie,

ulepszyć narzędzia dochodzeniowe organów ścigania i do innych celów. " Ustawa ta została zaproponowana i uchwalona w następstwie ataków z 11 września na własność publiczną i prywatną w Stanach Zjednoczonych. Jest to bardzo kontrowersyjna ustawa, która ogranicza dotychczasowe swobody obywatelskie w imię bezpieczeństwa narodowego. Poniżej znajdują się kwestie, które to prawo odnosi się do gromadzenia i przetwarzania informacji.

• Krajowa grupa zadaniowa ds. Przestępstw elektronicznych. Uznając potrzebę informacji w walce z przestępczością, a w szczególności z terroryzmem, prawo kieruje tworzeniem „krajowej sieci elektronicznych grup zadaniowych ds. Przestępczości… w celu zapobiegania, wykrywania i badania różnych form elektronicznych przestępstwa, w tym potencjalne ataki terrorystyczne na infrastrukturę krytyczną i systemy płatności finansowych ".

• Przechwytywanie informacji. Prawo przyznaje uprawnienia do rozpoznania amerykańskich agencji rządowych „do przechwytywania przekazów elektronicznych, ustnych i elektronicznych związanych z terroryzmem, oszustwami komputerowymi i przestępstwami polegającymi na nadużyciach". Może wystąpić „przejęcie wiadomości poczty głosowej na podstawie nakazów".

• Ujawnianie zapisów. Dostawca usług internetowych „może ujawnić zapis lub inne informacje dotyczące subskrybenta lub klienta… jeżeli dostawca ma uzasadnione przekonanie, że nagły wypadek, który wiąże się z bezpośrednim zagrożeniem śmierci lub poważnych obrażeń fizycznych, wymaga natychmiastowego ujawnienia informacji".

• Oszustwa telemarketingowe. Prawo dotyczy charytatywnych oszustw telemarketingowych i wymaga pełnego ujawnienia takich działań

„Nazwa i adres pocztowy organizacji charytatywnej, w imieniu której dokonywane jest nagabywanie”.

Ustawa Patriot koncentruje się głównie na środkach pomagających federalnym organom ścigania w walce z terroryzmem i finansowymi przestępstwami. Chociaż grupy wolności obywatelskich twierdziły, że wiele przepisów ustawy jest niezgodnych z konstytucją i że ustawa „rozszerzyła władzę rządu na wtrącanie się w życie prywatne ludzi z niewielkimi lub żadnymi dowodami wykroczeń”, ustawę przedłużono do 1 czerwca 2015 r.

Communications Assistance for Law Enforcement Act z 1994 r.

Ustawa o pomocy prawnej w zakresie egzekwowania prawa z 1994 r (w skrócie CALEA) wymaga, aby firmy z sektora telekomunikacyjnego zapewniały organom ścigania dostęp do prywatnej komunikacji i zapisów takiej komunikacji. Ustawa należy do Federalnej Komisji Łączności (FCC). „W odpowiedzi na obawy, że pojawiające się technologie, takie jak komunikacja cyfrowa i bezprzewodowa, utrudniają organom ścigania wykonywanie autoryzowanego nadzoru, Kongres uchwalił CALEA 25 października, 1994. ” Jednak branża telekomunikacyjna nie zaprojektowała ani nie zbudowała swoich obiektów i usług w sposób konieczny, aby sprostać temu celowi, i potrzebna jest dodatkowa infrastruktura, aby „spełnić określone przez prawo obowiązki CALEA”. Poniżej znajdują się główne punkty aktu

• Wymagania. Firmy telekomunikacyjne świadczące usługi

publiczność musi być w stanie przechwycić „wszelką komunikację przewodową i elektroniczną prowadzoną przez przewoźnika… subskrybenta…”. Stwierdzono, że ta usługa dla organów ścigania musi być „… na podstawie orzeczenia sądowego lub innego zgodnego z prawem upoważnienia…”

• Koszt zgodności. Najwyraźniej instalacja sprzętu, który ułatwi wdrożenie CALEA, wiąże się z wysokimi kosztami, których firmy telekomunikacyjne nie są w stanie ponieść.

• Szyfrowanie. Jeżeli abonent zastosuje własną technologię szyfrowania, „Operator telekomunikacyjny nie ponosi odpowiedzialności

do odszyfrowywania,… chyba że szyfrowanie zostało dostarczone przez przewoźnika, a przewoźnik posiada informacje niezbędne do odszyfrowania komunikacji. ”

• Pojemność. Inną kwestią jest zdolność przechwytywania, którą firma telekomunikacyjna powinna utrzymywać, która „będzie oparta na rodzaju sprzętu, rodzaju usługi, liczbie abonentów, rodzaju lub wielkości lub operatora, charakterze obszaru usług lub jakimkolwiek innym środku; i określa, w maksymalnym możliwym zakresie, pojemność wymaganą w określonych lokalizacjach geograficznych. ”

• Nieuczciwe podsłuchiwanie. Aby chronić rządową bezpieczną komunikację radiową, ustawa zabrania hakerom słuchania komunikacji, która jest „… szyfrowana lub przesyłana przy użyciu technik modulacji, których podstawowe parametry zostały

ukryte przed opinią publiczną w celu zachowania prywatności takiej komunikacji… ”

• Bezpieczny port. Zgodność z dyrektywami CALEA można odstąpić w szczególnych okolicznościach, z upoważnienia Prokuratora Generalnego USA i FCC. Zwykle takie zwolnienia przedłużają jedynie datę zgodności, aby umożliwić firmie telekomunikacyjnej odpowiednie wyposażenie.

• koszty. W telekomunikacji technologie zawsze się rozwijają, w związku z tym zgodność z CALEA spowoduje dodatkowe koszty dla odpowiednich firm, które nie są wspierane przez przychody. „Prokurator generalny może, z zastrzeżeniem dostępności środków, zgodzić się zapłacić operatorom telekomunikacyjnym wszelkie uzasadnione koszty bezpośrednio związane z modyfikacjami

dokonanymi przez przewoźników… (w celu) w celu dostosowania się do [CALEA]. Zatwierdzone środki na lata budżetowe 1995–1998 wyniosły 0,5 mld USD.

• Kary. Wspieranie organów ścigania w ich misji nie jest zadaniem dobrowolnym, ale obowiązkiem prawnym. Ustawa stanowi, że „operator telekomunikacyjny, producent urządzeń do transmisji lub przełączania telekomunikacji lub dostawca usług wsparcia telekomunikacyjnego [uznany za niezgodny z CALEA może zostać ukarany grzywną]… do 10 000 USD za każdy dzień z naruszeniem. ” Grupy wolności obywatelskich czuwające nad CALEA są bardzo zaniepokojone możliwym rozszerzeniem CALEA na telefonię internetową. „Ta ekspansja budzi poważne obawy w zakresie swobód obywatelskich, ponieważ wymagałaby od dostawców VoIP zbudowania wszystkich swoich produktów z backdoorami nadzoru, do których dostęp mają organy ścigania i prawdopodobnie będą niewłaściwie wykorzystywane przez hakerów i przestępców”.

Ustawa o bezpieczeństwie komputerowym z 1987 r.

Prawo to było prekursorem FISMA , a jego celem było poprawić „bezpieczeństwo i prywatność poufnych informacji w federalnych systemach komputerowych… [i stworzyć] sposób na ustanowienie minimalnych akceptowalnych praktyk bezpieczeństwa dla takich systemów…” Niektóre z najważniejszych przepisów prawa były następujące.

• Autorytet. Prawo wskazuje na potrzebę opracowania „standardów bezpieczeństwa komputerowego i minimalnych akceptowalnych praktyk” i przypisuje NIST do zadania z pomocą Narodowej Agencji Bezpieczeństwa.

• Program. Program ustanawia zasady, „standardy, wytyczne oraz powiązane metody i techniki dotyczące systemów komputerowych… [a także] standardy techniczne, administracyjne, fizyczne i administracyjne oraz wytyczne dotyczące opłacalnego bezpieczeństwa i prywatności wrażliwych informacji na komputerze federalnym systemy. ”

• Wcześniejsze powiązane prawo. Ustawa ta zmieniła również federalną ustawę o własności i usługach administracyjnych z 1949 r., Usprawniając ją o praktyki technologiczne i zarządcze z 1987 r.

• Trening. Prawo kładło duży nacisk na szkolenie, stwierdzając, że każda agencja federalna zapewni obowiązkowe okresowe szkolenie w zakresie świadomości bezpieczeństwa komputerowego i przyjętych praktyk bezpieczeństwa komputerowego wszystkich pracowników zaangażowanych w zarządzanie, użytkowanie lub obsługę każdego komputera federalnego system… Takie szkolenie musi być zaprojektowane

1. Zwiększenie świadomości pracowników na temat zagrożeń i podatności systemów komputerowych

2. Zachęcanie do stosowania ulepszonych praktyk bezpieczeństwa komputera

Ustawa o prywatności z 1974 r.

Na początku lat siedemdziesiątych XX wieku zdano sobie sprawę, że powiązane i przekrojone bazy danych mogą bardzo szybko zaowocować szeroką gamą zapisów dotyczących danej osoby i że należy zapobiegać nadużywaniu takiej władzy. Było to zwycięstwo grup wolności obywatelskich, które były bardzo zaniepokojone tym, że technologia bardziej pracuje nad odzyskiwaniem danych, a mniej na ochroną danych. Niektóre z najważniejszych wydarzeń aktu podążać.

• Warunki ujawnienia. Kluczową kwestią jest ujawnienie danych osobowych, a prawo stanowi, że „Żadna agencja nie ujawni żadnych zapisów zawartych w systemie zapisów za pomocą jakichkolwiek środków komunikacji z jakąkolwiek osobą lub inną agencją, z wyjątkiem pisemnego wniosku złożonego

przez, lub za uprzednią pisemną zgodą osoby, której dotyczy dokument… ” Jednak ujawnienie zapisów byłoby dozwolone do oficjalnego użytku. Klauzula ta miała na celu zablokowanie nieoficjalnego ujawnienia danych osobowych.

• Poprawka do wolności słowa. Istnieje bardzo dziwna przyczyna w prawie (zgodnie z wymogami Agencji 7), stwierdzająca, że „Każda agencja, która prowadzi system rejestrów,… nie prowadzi rejestrów opisujących, w jaki sposób poszczególne osoby wykonują prawa zagwarantowane w Pierwszej Poprawce, chyba że wyraźnie zezwalają na to ustawa lub przez osobę, o której prowadzona jest ewidencja, lub o ile nie dotyczy i jest w zakresie dozwolonego działania organów ścigania. ” Luźno wyrażone oznacza, że rząd USA nie powinien oznaczać obywateli na podstawie ich otwartości.

• Dokładność zapisów. Biorąc pod uwagę, że dokładność jest najważniejszym atrybutem zapisów, prawo wyraźnie nakazuje, aby agencje „zachowywały wszystkie zapisy… z taką dokładnością, stosownością, terminowością i kompletnością, jaka jest racjonalnie niezbędna dla zapewnienia uczciwości w ustalaniu”.

• Listy mailingowe. Na początku lat siedemdziesiątych automatyzacja danych ułatwiła tworzenie skategoryzowanych list mailingowych do celów komercyjnych, a prawo chciało upewnić się, że nie dochodzi do nadużywania danych osobowych pod nadzorem rządu. Prawo stanowi: „Nazwisko i adres osoby fizycznej nie mogą być sprzedawane ani wynajmowane przez agencję, chyba że takie działanie jest wyraźnie dozwolone przez prawo. Przepisu tego nie należy interpretować jako wymagającego nieujawniania nazwisk i adresów, które w innym przypadku mogą zostać upublicznione. ”

• Minimum zapisów. Prawo dotyczące kompilacji prywatnych niepowiązanych danych na temat osób fizycznych wyraźnie stanowi: „Każda agencja, która prowadzi system rejestrów,… zachowuje w swoich rejestrach tylko takie informacje o osobie, które są istotne i niezbędne do osiągnięcia celu agencji”.

Cyberprzestępczość

Cyberprzestępczość jest produktem ubocznym cyberprzestrzeni, służąc jako czarne piętno w optymizmie, jaki Internet dał światu. Cyberprzestępczość rośnie w ciągu ostatnich dwóch dekad, osiągając roczny poziom ponad pół miliarda dolarów w 2009 roku. „W rzeczy samej, napędzane perspektywą znacznych zysków, innowacje i techniki cyberprzestępczości wyprzedziły tradycyjne modele bezpieczeństwa i wiele obecnych technologii wykrywania opartych na sygnaturach”. Rozwinął się nowy przemysł podziemny - centra cyberprzestępczości. Są to legalne firmy zatrudniające nawet pięćdziesięciu pracowników, którzy oferują usługi internetowe, od projektowania stron internetowych i reklam internetowych po hosting stron internetowych i rejestrację nazw domen. Stopniowo te firmy zajmujące się cyberprzestępczością zmieniają setki tysięcy Internetowych hostów - komputery podłączone do Internetu – w swoje zombie przez instalowanie złośliwego oprogramowania . Instalacja złośliwego oprogramowania odbywa się pod fałszywymi pozorami. Na przykład mają szereg witryn internetowych, na których odwiedzającym oferuje się prawdopodobnie potrzebne oprogramowanie za darmo. W rzeczywistości to oprogramowanie jest złośliwym oprogramowaniem, które przekierowuje wskaźnik DNS znajdujący się w hoście na nieuczciwy, który źle kieruje interakcjami użytkownika w sieci, co skutkuje naruszeniem poufnych danych użytkownika. Zaskakujące jest to, że znaczna część cyberprzestępczości wciąż nie służy korzyściom finansowym, a jedynie szkodom. Równie zaskakujące jest to, że wiele organizacji wykorzystuje więcej zasobów do wykorzystywania Internetu przez pracowników niż do ochrony cybernetycznej. W stosunku do wymaganych zasobów cyberprzestępczość jest najbardziej opłacalnym i fizycznie bezpiecznym ze wszystkich przestępstw, a nowe zagrożenia są stale rozpoznawane. Nie jest możliwe sporządzenie kompleksowej listy przestępstw, które można popełnić przez Internet. Jeden fakt jest oczywisty, że hakerzy są zastępowani

przez przestępczość zorganizowaną i że zwiększone wydatki na obronę cybernetyczną niekoniecznie prowadzą do zwiększenia bezpieczeństwa cybernetycznego, ale priorytetem jest ryzyko.

Trendy w cyberprzestępczości

Trendy wskazują, że cyberprzestępczość nie jest jedynym cyberatakiem, a nowe bardzo innowacyjne nielegalne programy pojawiają się codziennie w Internecie. Istnieje wiele aplikacji na telefony komórkowe, które zostały zaprojektowane z myślą o bezpieczeństwie, oraz liczne aplikacje z myślą o cyberprzestępczości. Ogół społeczeństwa w dobrej wierze pobiera i instaluje aplikacje, nie wiedząc, czy są bezpieczne. W rezultacie szkodliwe aplikacje infekują zarówno pierwszy telefon, jak i te, z którymi się komunikują, a także uniemożliwiają dostęp do zawartości telefonu. Tabela 9.3 zawiera listę nadużyć cybernetycznych, które wzrosły.

Zwalczanie cyberprzestępczości

Połączenie z siecią samo w sobie stanowi lukę. Dlatego dobrą praktyką jest łączenie się z Internetem i rozłączanie się z nim w zależności od potrzeb. Łatwość popełnienia cyberprzestępczości sprawiła, że Internet, to cudowne dzieło ludzkie, stał się polem minowym. Jednak świadomość i korzystanie z oprogramowania ochronnego, takiego jak te wspomniane w rozdziale o wtargnięciach, może zminimalizować ryzyko. Filozofią walki z cyberprzestępczością powinno być nie tyle maksymalizowanie bezpieczeństwa, co minimalizowanie ryzyka. Istnieje subtelna, ale ważna różnica w tych dwóch koncepcjach, gdzie pierwsza jest tylko środkiem, a druga jest prawdziwym celem. Na poziomie korporacyjnym cyberbezpieczeństwo nie powinno być postrzegane jako ćwiczenie techniczne, ale jako najwyższe obowiązki kierownicze, które są delegowane na szefa bezpieczeństwa organizacji. W związku z tym cyberbezpieczeństwo powinno być najważniejszym projektem najwyższego kierownictwa. Istnieje wiele programów chroniących przed cyberprzestępczością, które odfiltrowują podejrzane strony internetowe i filtrują tylko wybrane strony internetowe i korespondentów e-mail. Takie oprogramowanie zapewnia „bezpieczeństwo wiadomości przychodzących i wychodzących, (wysoce) skuteczną ochronę antyspamową i antywirusową, zaawansowane filtrowanie treści, zapobieganie utracie danych i szyfrowanie wiadomości e-mail" [34]. Z cyberbezpieczeństwa żadna korporacyjna aktywność cybernetyczna nie może być uznana za nieistotną. Jednak niektóre obszary wymagają szczególnej uwagi ze względu na zwiększoną cyberprzestępczość. Jednym z takich obszarów jest zarządzanie hasłami. Znaczna część ma miejsce przy naruszonych hasłach. Przynajmniej ten rodzaj cyberprzestępczości można zwalczać, wdrażając hasła jednorazowe (OTP) [35]. Tabela 9.4 wymienia cztery obszary - słabe linki - które są na czele cyberprzestępczości. W naszych środkach obrony przed cyberprzestępczością istnieją dwa fronty. Pierwszy to nasza fortyfikacja techniczna. Oznacza to, że instalacja na naszych komputerach najlepszych możliwych programów antywirusowych. Istnieje wiele tak renomowanych programów, nawet dla smartfonów [36], telefonów komórkowych z dostępem do Internetu. Niestety złośliwe oprogramowanie cyberprzestępcze jest liderem w tej technologii, a przemysł bezpieczeństwa złośliwego oprogramowania opóźnia się o trzy do sześciu miesięcy. Drugim frontem obronnym jest nasza świadomość istnienia fałszywych ofert internetowych i powstrzymywanie się od wpadania w pułapki cyberprzestępczości. Na przykład istnieją strony internetowe, które mają fantastyczne oferty produktów lub usług. Niektórzy obciążą Twoją kartę kredytową i nigdy nie dostarczą. W takim przypadku możesz ostrzec wystawcę karty kredytowej i spróbować uzyskać zwrot pieniędzy. Istnieją jednak inne oszukańcze witryny handlu elektronicznego, które po złożeniu zamówienia odpowiedzą, że takiego produktu nie ma na magazynie i że karta kredytowa nie zostanie obciążona. Rzeczywiście, Twoja karta kredytowa nie jest obciążana, ale dane uwierzytelniające karty są sprzedawane cyberprzestępcom. „Technologia może nas do tej pory zabrać, a resztą jest edukacja i czujność użytkowników komputerów". Istnieje wiele organizacji zajmujących się zwalczaniem cyberprzestępczości, a nasza świadomość ich istnienia jest ważna w naszej własnej

walce. Odpowiedzialność za popełnienie przestępstwa, czy to w świecie fizycznym, czy w cyberprzestrzeni, spoczywa na ramieniu ofiary. Na przykład, jeśli ktoś z fałszywą kartą oszuka bankomat i wykradnie pieniądze z konta, odpowiedzialność spoczywa na banku. Jeśli jednak ktoś korzystający ze schematu windykacji za pomocą naciśnięcia klawisza zhackuje Twoje kody bankowe i zaatakuje twoje konto, bank może odmówić „odpowiedzialności za stratę, ponieważ logowanie było autentyczne. Bank nie ponosi odpowiedzialności za integralność komputera klienta ”

Cyberprzestępczość w bankowości

Według różnych informacji prasowych setki banków są codziennie atakowane cybernetycznie, a łączne straty wynoszą prawie miliard dolarów. Tylko jeden bank azjatycki ukradł 101 mln USD, a odzyskano tylko 20 mln USD. Najwyraźniej działania te wymagały rozległych umiejętności w zakresie elektronicznego przesyłania funduszy, a także protokołów internetowych. Nawet niektóre amerykańskie banki były dysfunkcyjne z powodu cyberataków. Ponieważ niepraktyczne jest prowadzenie fizycznych przewodów lub dedykowanych łączy bezprzewodowych, od centralnego centrum IT banku do każdego bankomatu, banki używają sieci jako łącza komunikacyjnego z urządzeniami TM należącymi do kategorii Internetu rzeczy (IoT), z jego plusami i minusami. Wiele przedsiębiorstw, w tym banki, uważa, że cyberbezpieczeństwo można zwiększyć poprzez zakup większej ilości sprzętu. Jednak według urzędnika FBI: „Nie wystarczy budować ściany i hartować systemy, potrzebny jest kapitał ludzki, aby zrozumieć zagrożenie”. § Tam, gdzie ten kapitał ludzki, specjaliści ds. Bezpieczeństwa cybernetycznego, mają doświadczenie i wiedzę specjalistyczną oraz są na bieżąco na co dzień. Dla wszystkich przedsiębiorstw, w tym sektora bankowego, przeznaczanie milionów na bezpieczeństwo cybernetyczne jest nieuzasadnione, ale Royal Bank of Scotland nie wahał się podwoić swojego budżetu na bezpieczeństwo cybernetyczne do pół miliarda dolarów. Potrzeba cyberbezpieczeństwa jest podwójna: doświadczeni strategowie w pakiecie C i technicy w maszynowni IT.

Cyberprzestępczość w handlu elektronicznym

Praktycznie każda działalność komercyjna stara się wykorzystać korzyści płynące z Internetu, jednocześnie narażając się na cyberprzestępczość. Przepisy na całym świecie wyszczególniły cyberprzestępczość na ponad sto rodzajów i podlegały surowym karom, ale nie zniechęciło to przestępców do poszukiwania nielegalnych korzyści. Tak więc, według globalnych statystyk, wielkość handlu elektronicznego podwaja się rocznie. Walka z cyberprzestępczością stała się walką kooperacyjną z kupcami, rządem i konsumentem, której celem jest przynajmniej minimalizacja ta plaga. Osiągnięto konsensus co do środków zapobiegawczych, które muszą stosować konsumenci, które obejmują:

• Zachowaj system operacyjny komputera i zainstalowane aplikacje wszystko na bieżąco.

• Użyj najlepszej możliwej aplikacji antywirusowej. Nigdy nie polegaj na darmowych wersjach

• Używaj bezpiecznych sieci. Unikaj publicznych miejsc Wi-Fi, gdzie w tym samym obszarze fizycznym mogą znajdować się serwery obsługiwane przez cyberprzestępców.

• Kupuj przez zaufane strony internetowe. Cyberprzestępcy zakładają strony internetowe z „zaległymi okazjami”, aby uzyskać parametry karty kredytowej kupujących.

• Unikaj posiadania tego samego hasła do wielu krytycznych zastosowań. W związku z tym, jeśli zostanie naruszony, nie będzie działać na innych stronach internetowych.

• Unikaj wygody automatycznego wypełniania - szczególnie w przypadku finansów dane.

• Unikaj uwięzienia w grach internetowych, nagrodach, loteriach itp. Wiele takich publicznych stron internetowych jest zainfekowanych wirusem.

• Nie daj nikomu znać twoich haseł.

• Często zmieniaj hasła, w zależności od tego, jak ważny jest dostęp.

• Jeśli są dostępne, uczęszczaj na zajęcia uświadamiające na temat cyberbezpieczeństwa.

Cyberbezpieczeństwo na morzu

W dzisiejszej żegludze dostęp do Internetu jest tak samo, jak w dużym mieście. W ten sposób komunikacja online i w czasie rzeczywistym może odbywać się przez całą dobę. Za pomocą odpowiedniego Internetu Rzeczy (IoT) urządzenia centralne biuro może monitorować każdą aktywność na statku, taką jak

• Lokalizacja GPS

• Prędkość

• Skok i ziewanie

• Poziom paliwa

• Status zaciągów

• Zobacz kamery stacjonarne i mobilne na pokładzie

Podobnie jak w przypadku innych działań wspieranych przez cyberprzestrzeń, eksploatacja statku na środku oceanu wymaga morskich usług cybernetyki, które obejmują:

• Testy wytrzymałościowe i wytrzymałościowe

• Testy penetracji i segregacji sieci

• Skanowanie antywirusowe oraz łatki i aktualizacje oprogramowania

• Audyt uwierzytelnienia

• Bezpieczeństwo urządzeń przenośnych i IoT

• Ocena podatności

• Anomalie drogowe

• Monitorowanie urządzeń sieciowych

W kwestii bezpieczeństwa cybernetycznego na morzu Europejska Agencja Bezpieczeństwa Informacji o Sieci (ENISA) zaleca szkolenie uświadamiające na temat bezpieczeństwa cybernetycznego, które obejmuje wszystkich członków w dziedzinie morskiej, od sterników, operatorów terminali i żeglarzy, po głównych inżynierów i kapitanów

Cybernetyczna wojna i bezpieczeństwo wewnętrzne

Zwycięstwo i porażka są dalekie od rozpoznania w cyberprzestrzeni.-Paul Cornish, Chatham House

Wprowadzenie

Cyberprzestrzeń to wyjątkowa instytucja, która wspiera wszystkie aspekty i sektory społeczeństwa, w związku z czym bezpieczeństwo tej przestrzeni ma absolutne znaczenie dla wszystkich rządów dla ich społeczeństw. Kraje, jeden po drugim, tworzą agencje rządowe zajmujące się bezpieczeństwem tej przestrzeni. Podobnie w Stanach Zjednoczonych Departament Bezpieczeństwa Wewnętrznego (DHS), obok wielu innych obowiązków i we współpracy z innymi agencjami rządowymi, otrzymał zadanie cyberbezpieczeństwa. DHS uznał, że istnieje potrzeba stworzenia „odpornego ekosystemu cybernetycznego", co oznacza, że cyberprzestrzeń nie jest izolowanym systemem wsparcia, ale wielowymiarowym ekosystemem, który musi działać w sposób ciągły i odporny, wolny od zagrożeń i możliwości załamania. Ponadto obrona tego ekosystemu musi być dokładna i „zautomatyzowanych działań zbiorowych". Oznacza to, że bezpieczeństwo cyberprzestrzeni musi zostać zautomatyzowane, ponieważ nie może być to proces do zatrzymania, zbadania i podjęcia decyzji z interwencją człowieka - jest po prostu zbyt wolny. System obrony w cyberprzestrzeni musi realizować swoją decyzję działania z prędkością elektroniczną, jeżeli działania te mają charakter zbiorowy są wdrażane w rozproszonych lokalizacjach centrów informacyjnych.

W tym przypadku „sztuczna inteligencja na poziomie węzła sieci rozpoznaje i zapobiega zagrożeniom w czasie rzeczywistym". Cyberprzestrzeń z dnia na dzień staje się coraz ważniejsza w każdym aspekcie życia. Oferuje bezprecedensową i niezastąpioną wygodę, dzięki której społeczeństwo staje się zakładnikiem. Mamy dwie możliwości. Albo odmawiamy użycia cyberprzestrzeni i ponosimy konsekwencje, takie jak izolacja i nieefektywność, lub w pełni cieszymy się z jej nieograniczonych korzyści, wiedząc dobrze, że jej awaria może być katastrofalna, chyba że podejmiemy wszystkie niezbędne środki ostrożności. DHS pojawił się na scenie z pełnym uznaniem tego dylematu i stale zwiększa swoje doświadczenie i wiedzę, starając się dotrzeć do asymptoty - bezpiecznej cyberprzestrzeni.

Cyber Warfare

Cybernetyczna wojna jest spodziewaną wrogą działalnością, którą zrobią przeciwnicy będą próbować wykorzystać, jeśli postrzega się przewagę. „Mówiąc najprościej, wojna cybernetyczna jest nowym, ale nie do końca odrębnym elementem wieloaspektowego środowiska konfliktu". „Dzisiaj w cyberprzestrzeni inteligentni przeciwnicy wykorzystują luki i tworzą incydenty, które rozprzestrzeniają się z prędkością [elektroniczną]… w celu kradzieży tożsamości, zasobów i [tworzenia] przewagi" . W cyberobronie trudno powiedzieć, kto ma przewagę, ponieważ nikt nie wie dokładnie, ile „dziur" znajduje się w cyberprzestrzeni. W kontekście działań wojennych cyberprzestrzeń to przestrzeń elektroniczna, w tym Internet, a także fale radiowe niezależnie od częstotliwości. Miały miejsce liczne cyberataki, ale żadnego z nich nie przypisano wyraźnie przeciwnikowi politycznemu lub wojskowemu. Wszystkie główne mocarstwa - Wielka Brytania, Francja, Niemcy, Rosja i Chiny - na różne sposoby potwierdziły, że włączyły „cyberwarfare jako nową część swojej doktryny militarnej…. Francuzi mogą widzieć uzasadnioną rolę cyberprzestępczości gospodarczej w dążeniu do celów krajowych. " Rosjanie postrzegają „cyberwarfare jako akt wojny, na który każda reakcja… jest uważana za uzasadnioną". Ponadto uważa się, że „Rosja zachowuje prawo do użycia broni jądrowej najpierw przeciwko środkom i siłom wojny informacyjnej, a następnie przeciwko samemu państwu-agresorowi" [6]. Chińczycy postrzegają to jako kolejną wojnę i stworzyli Niebieską Armię [7]. Wydarzenie, które miało miejsce na Syberii, eksplozja gazociągu w 1982 r., jest uważane za pierwszy znany akt cyberbroni. Według zachodnich publikacji wydarzenie było wynikiem sabotażu, w ramach którego system nadzoru i

akwizycji danych (SCADA) systemu rurociągów został źle zaprogramowany w celu spowodowania wybuchu. Jest to skomputeryzowany system, który nadzoruje i kontroluje proces przemysłowy. Jedna strona mówi, że „był to trojan wstawiony [przez CIA] do oprogramowania systemu SCADA, który spowodował masową eksplozję gazu ziemnego wzdłuż rurociągu transsyberyjskiego w 1982 r." Program „resetuje prędkości pompy i ustawienia zaworów, aby wytworzyć ciśnienia znacznie przekraczające wartości dopuszczalne dla połączeń i spoin rurociągów". Druga strona twierdzi, że „było to spowodowane raczej słabą konstrukcją niż sabotażem". Gdyby rzeczywiście był to wrogi akt przypisywany pochodzeniu, jak na przykład bombardowanie, Stany Zjednoczone byłyby winne aktu wojny, ze wszystkimi konsekwencjami prawnymi i moralnymi, jakie Związek Radziecki mógłby ponieść. Ponieważ ofiara wojny cybernetycznej ma trudny przypadek, jeśli nie niemożliwy, do udowodnienia tożsamości cyberatakującego, przyszłość będzie pełna cyberataków. Jeśli w powyższym przypadku rurociągu syberyjskiego urzędnicy byłego lub byłego napastnika twierdzą o odpowiedzialności, kraj będący ofiarą cybernetyczną ma wszelkie prawo do odszkodowania. Dlatego jeśli w momencie wojny cybernetycznej solidne dowody nie wskazują na winnych, nic nie stoi na przeszkodzie prawu do odszkodowania po przyznaniu się do winy lub udowodnieniu pochodzenia czynu przed sądem międzynarodowym. Oznacza to, że po zidentyfikowaniu sprawcy umyślnego szkodliwego działania cybernetycznego ofiara cybernetyczna, zarówno osoba fizyczna, jak i całe państwo, ma prawo do odszkodowania. Uznając ważną rolę, jaką cyberprzestrzeń będzie odgrywać w przyszłości, wszystkie główne potęgi opracowały polecenia cyberprzestrzeni, chcąc stworzyć cyber wojowników gotowych do ataku lub obrony, gdy nadejdzie odpowiedni moment. Mówi się, że cyberprzestrzeń jest korektorem, w tym sensie, że każdy może założyć potężną stronę internetową bez odwiedzającego znającego pełną organizację za fasadą strony. Podobnie wojna w cyberprzestrzeni jest korektorem w tym sensie, że siła militarna, ekonomiczna lub polityczna nie odgrywa żadnej roli, a umiejętności złośliwego oprogramowania są jedynym arsenałem. Jest całkiem możliwe, że dzięki cyberwojnie można osiągnąć niewielkie cele geopolityczne bez konfrontacji militarnej. We wszystkich przypadkach nie ma niepodważalnych dowodów na to, że za suwerenami stoją poszczególne suwerenne państwa. Należy uznać, że ani pochodzenie ataków przez IP, ani osiągnięty cel, jeśli w ogóle, nie mogą absolutnie powiązać ataków z rządami. Większość oskarżeń to uzasadnione spekulacje. Słabym ogniwem w scenariuszu cyberwojny jest telekomunikacja zapadni tworzonej dla organów ścigania, aby ułatwić im misję w walce z przestępczością. Trapdoor jest terminem w kontekście bezpieczeństwa odnoszącym się do mechanizmu, który omija procedury uwierzytelniania i / lub autoryzacji bezpieczeństwa w celu uzyskania nieograniczonego dostępu do zasobów. Jest to odpowiednik klucza głównego w zamkach fizycznych. Biorąc pod uwagę, że żadna informacja o wartości nie może być utrzymywana w tajemnicy, kody zapadni lub inne informacje mogą wyciekać w ręce wroga.

Konwencja o broni cybernetycznej

Około sto lat temu mocarstwa światowe zdały sobie sprawę, że energia atomowa może być również użyta do celów destrukcyjnych. Trzydzieści lat później eksplozja dwóch głowic atomowych udowodniła światu możliwy poziom zniszczenia. Podobnie dzisiaj światowe mocarstwa - widoczne i niewidzialne - rozwijają defensywne i ofensywne cyber arsenały broni cybernetycznej (CW), nieustannie testując je pod kątem ewentualności. Ponownie, podobnie jak w przypadku broni atomowej, niektóre „chłodne głowy" wskazują na potrzebę Konwencji o broni cybernetycznej (CWC) [13]; konwencja - międzynarodowy traktat o kontroli zbrojeń dla cyberprzestrzeni - do którego sygnatariusze zgodzą się nie wykorzystywać swoich broni w scenariuszach zabronionych [13]. Mówi się, że w otwartych działaniach wojennych pierwsza ofiara jest prawdą. Niewątpliwie drugą ofiarą będzie cyberprzestrzeń. Jednak w przeciwieństwie do wszystkich innych broni, w których początkowy punkt początkowy nie może być ukryty ani zakwestionowany, początkowy punkt początkowy CW może pozostać nieznany na

zawsze. Ostatecznie CWC zostanie sporządzony i podpisany, ale będzie to trudne do wyegzekwowania, podczas gdy wiele pytań pozostaje bez odpowiedzi, takich jak,

• Jak można sprawdzić obecność CW?

• Czy powinna istnieć minimalna liczba CW?

• Jakie udogodnienia należy wykluczyć z takich ataków?

• Czy prawdziwe źródło ataku można zlokalizować bez najmniejszego problemu?

Wojna cybernetyczna ma zaledwie dziesięć lat, w porównaniu do wszystkich innych rodzajów wojny, i nie ma formalnej ani nieformalnej „etyki, norm i wartości".

Cyberterroryzm

Terroryzm jest innym rodzajem wrogiej konfrontacji, często pomiędzy suwerennymi mocarstwami, które anonimowo atakują swoje interesy. Zazwyczaj terroryzm obejmuje bezpośrednie lub pośrednie akty przemocy skierowane przeciwko określonym celom lub przeciwko pewnej niewinnej populacji przez grupy, które nie mają formalnego związku z żadną suwerenną mocą, to znaczy z żadnym krajem.

Terroryści wykorzystali szeroką gamę broni jako środka do osiągnięcia swoich celów, a cyberprzestrzeń nie została pominięta. Jeśli chodzi o definicję, można śmiało powiedzieć, że cyberterroryzm to wykorzystanie cyberprzestrzeni do popełniania przemocy lub grożenia jej popełnieniem. Korzystanie z cyberprzestrzeni może być dodatkiem do przestępstwa. Na przykład organizacja terrorystyczna utrzymuje stronę internetową, aby „zabiegać o pieniądze dla nich z różnych przyczyn lub rozpowszechniać zakodowane wiadomości, jawnie lub steganograficznie ". Stenografia to praktyka ukrywania wiadomości w niepowiązanych plikach. Na przykład wiadomości tekstowe można ukryć w plikach obrazu bez widocznego wpływu na wyświetlany obraz. W przypadku terroryzmu cyberprzestrzeń jest najbardziej opłacalną bronią, a także najbezpieczniejszą z punktu widzenia terrorystów. Cyberterroryzm można określić jako

• Sponsorowane przez państwo. W chwili obecnej żaden kraj nie zaakceptował przeprowadzania wrogich działań wobec kogokolwiek. Tacy aktorzy są zwykle wysoko wykwalifikowani, koncentrując się na konkretnych celach wroga.

• Grupy ekstremistyczne. Takie grupy używają cyberprzestrzeni do promocji, rekrutacji i zbierania funduszy, a także do cyberataków na cele, które uważają za wrogie. Takie grupy należą do następujących ogólnych kategorii:

• polityczny

• religijne

• Etniczne

• ideologiczny

• Przestępczość zorganizowana. Są to grupy, które mają pewną wiedzę specjalistyczną w danym sektorze i popełniają wymuszenia na podstawie zagrożeń szkodą - ekonomiczną lub fizyczną. Ich motywami są zawsze korzyści finansowe.

• Przestępstwa indywidualne. Są to izolowane osoby, które popełniają cyberprzestępstwa lub grożą im. W takim przypadku motywy mogą, ale nie muszą, być zyskami finansowymi.

Jeśli chodzi o narzędzia, minimalne badania w Internecie mogą stworzyć skuteczne narzędzia hackerskie. Specjaliści od zwalczania cyberterroryzmu dokumentują incydenty terrorystyczne poprzez identyfikację sześciu głównych parametrów, które wspólnie definiują incydent. To są

• Sprawca. Osoba lub grupa, która popełniła akt cyberterroryzmu.

• Akcja. Cyberprzestępczość terrorystyczna, która została popełniona lub grożono jej popełnieniem.

• Zasób cybernetyczny. Zwykle składa się z trzech części.

• Wirtualna lokalizacja cybernetyczna zdefiniowana przez adres URL.

• Logiczna lokalizacja zdefiniowana przez tożsamość serwera lub bazy danych.

• Fizyczna lokalizacja, w której znajdują się dane. W przypadku przetwarzania w chmurze określenie tej lokalizacji może być trudne.

• Znaczy. Technika złośliwego oprogramowania lub włamania zastosowana w ataku.

• Luka w cyberprzestrzeni. Słaby punkt cyberbezpieczeństwa atakowanego zasobu.

• Motywacja. Zwykle ma to dwa widoki.

• Upubliczniona „szlachetna" motywacja

• Ukryty motyw ukryty

• Przynależność. Zwykle ma to dwie tożsamości.

• Podmiot powołujący się na odpowiedzialność za działanie

• Podmiot podejrzewany o beneficjenta działania

Powyższe stanowią punkt wyjścia w klasyfikacji incydentu. Takie incydenty obejmują szereg przypadków - od unieważnienia lub tymczasowego rozproszonego ataku typu „odmowa usługi" (DDoS) na oficjalnej stronie internetowej po zniszczenie dostępnych publicznych rejestrów lub ingerencję w sterowanie siecią energetyczną. W przeciwieństwie do ostrzeżeń specjalistów ds. Cyberbezpieczeństwa, wiele infrastruktur krytycznych wykorzystuje Internet jako operacyjny intranet ze względu na wynikające z niego korzyści finansowe, zamiast budować i utrzymywać własną sieć fizycznie i logicznie odizolowaną od Internetu. Obecnie kilka sektorów wytwarzania energii jest narażonych na działanie Internetu, a „Dzięki najnowszym osiągnięciom w dziedzinie inteligentnych systemów sieciowych i coraz większemu wykorzystaniu technologii informatycznych w infrastrukturze elektroenergetycznej takie ataki mogą mieć miejsce, szczególnie na dużą skalę przy użyciu wyrafinowanych technik wtargnięcia". Atak na pokolenie może doprowadzić do zniszczenia dużych turbin, odcięcia zasilania i spowodowania ofiar wśród ludzi. Atak na dystrybucję i kontrolę mocy może pozostawić duże obszary bez usługi zasilania; podczas gdy atak na przetwarzanie danych może zniszczyć ważne, być może niezastąpione zapisy. Eksperci twierdzą, że „kliknięcie myszą może pogrążyć miasto w ciemności" i wezwał przedsiębiorstwa energetyczne do „Odłączenia sieci elektrycznej od Internetu" , stwierdzając, że „infrastruktura krytyczna każdego kraju - komunikacja, sieci energetyczne, zasoby wodne, linie gazowe , wojsko i tym podobne - a ich sieci nie mogą mieć nic wspólnego z Internetem. Taka infrastruktura musi mieć własny intranet, dostępny tylko z wybranych lokalizacji oraz fizycznie i praktycznie bezpieczny ". Co więcej, dowódca amerykańskiego Cyber Command, odnosząc się do słabości cybernetycznych w sieciach elektroenergetycznych, stwierdził, że „cyberataki przez Internet przechodzą z kradzieży danych na ataki fizyczne". Możliwość destrukcyjnego ataku cyberterrorystycznego mieści się w sferze rzeczywistości i należy podjąć wszelkie środki, aby temu

zapobiec. Biorąc pod uwagę, że terroryzm jest zwykle „lewą ręką" suwerennych mocarstw, cyberterroryści są wirtualnymi urzędnikami służby cywilnej, którzy są tak wyszkoleni i równie dobrze wykwalifikowani, jeśli nie więcej, niż uprawnieni agenci ścigania, którzy ich ścigają. Terroryzm w cyberprzestrzeni jest w powijakach, a jego działania w końcu przyćmią działania fizyczne.

Cyberszpiegostwo

Dzięki cyberprzestrzeni szpiegostwo stało się mniej niebezpieczne i bardziej satysfakcjonujące w wielu przypadkach jest to „jedna z najbardziej rozpowszechnionych aktywności cybernetycznych". Organizacje ze względu na wygodę dostępu i pozorną opłacalność bardzo często korzystają z Internetu jako intranetu. W związku z tym dane są narażone na nielegalny dostęp i często są narażone na szwank. Organizacje czasami ustawiają doniczki z miodem, aby zwabić cyberprzestępców i ujawnić ich cyberpochodzenie. Honey pot to termin określający bezpieczeństwo sieci używany w odniesieniu do plików zawierających fałszywe informacje , umieszczone na stronie internetowej w celu wprowadzenia w błąd szpiegów i ujawnienia ich adresu IP. Takie szpiegostwo może mieć charakter polityczny, wojskowy, przemysłowy, handlowy lub osobisty w celu uzyskania informacji w sposób nielegalny lub nieupoważniony. Upubliczniono, że szpiegostwo cybernetyczne po cichu szpiegowało oficjalne zapisy kilkudziesięciu krajów i organizacji, a ingerencje miały miejsce w latach 2006–2011. Kraje rozciągały się od Stanów Zjednoczonych po Wietnam, a wśród organizacji były komitety igrzysk olimpijskich. Zaskakujące było to, że cyber szpiegostwo było dziełem jednego komputera. Zostało to potwierdzone, gdy wszystkie adresy IP ofiar cyberprzestępców zostały przeciwdziałane. Szpiegostwo gospodarcze rośnie, ponieważ wykorzystanie takich informacji może przynieść duże zyski prawne. Zazwyczaj cyberszpiegostwo nie używa haseł, ponieważ takie informacje są trudne do uzyskania, jeśli w ogóle. Cyber-szpiegostwo zaczyna się od wysłania e-maila do powiernika poufnych informacji, takiego jak dyrektor generalny firmy, od nadawcy, który podszywa się pod renomowaną i zaufaną organizację. Wiadomość e-mail zawiera załącznik. Odbiorca, nie podejrzewając oszustwa, wykonuje załącznik, który wyświetla raczej przydatną lub interesującą informację. Podczas wykonywania załącznika na komputerze odbiorcy instalowane jest złośliwe oprogramowanie, które zapewnia nadawcy pełny dostęp do komputera odbiorcy. Mając takie przywileje, nadawca nie tylko przeszukuje komputer, ale również uzyskuje dostęp do stron internetowych, które wymagają nazw użytkowników i haseł, które zwykle pozostawiają cyberprzestępcom dla wygody, zamiast wpisywać je za każdym razem, gdy potrzebują dostępu do poczty e-mail lub innych usług. Szpiegostwo uznano za akt nieprzyjazny, ale nie za akt wojny, podobnie cyberszpiegostwo będzie „tolerowane", co będzie miało konsekwencje dyplomatyczne, a nie działania wojenne. Jednak po rozpoczęciu otwartych działań wojennych między dwoma przeciwnikami cybernetyczne działania wojenne i szpiegostwo cybernetyczne z pewnością nadejdą, jeśli jeszcze nie zostaną wprowadzone.

Bezpieczeństwo wewnętrzne

W Stanach Zjednoczonych, aby zająć się kwestiami bezpieczeństwa innymi niż obrona wojskowa, powołano rządowy departament, 25 listopada 2002 r. Ustawą o bezpieczeństwie wewnętrznym z 2002 r. „Departament Bezpieczeństwa Wewnętrznego [DHS] ma ważną misję: zabezpieczyć naród przed wieloma zagrożeniami… [w tym] cyberbezpieczeństwem…. [Obowiązki] są szerokie, ale nasz cel jest jasny - zapewnienie Ameryce bezpieczeństwa ". DHS został początkowo utworzony przez przeniesienie, z innych departamentów rządowych, różnych agencji, które były bezpośrednio lub pośrednio odpowiedzialne za bezpieczeństwo wewnętrzne kraju

National Cyber Security Division

W ramach DHS działa National Cyber Security Division (NCSD), którego misją jest współpraca „z podmiotami publicznymi, prywatnymi i międzynarodowymi w celu zabezpieczenia cyberprzestrzeni i amerykańskich zasobów cybernetycznych” . Strategią jest

• Zbudowanie i utrzymanie skutecznego krajowego systemu reagowania w cyberprzestrzeni

• Wdrożenie programu zarządzania ryzykiem cybernetycznym w celu ochrony infrastruktury krytycznej

DHS-NCSD jest gospodarzem Zespołu ds. Gotowości na wypadek awarii komputera w Stanach Zjednoczonych (US-CERT), który dostarcza biuletynów bezpieczeństwa związanych z cybernetycznymi, alertów bezpieczeństwa technicznego oraz wskazówek bezpieczeństwa, a także cennych informacji o wydaniach dotyczących luk w zabezpieczeniach dużego oprogramowania. US-CERT jest także miejscem zgłaszania incydentów związanych z cybernetycznymi [28]. Uznając, że nie ma czasu do stracenia, NCSD „agresywnie dąży do zbudowania światowej klasy zespołu ds. Bezpieczeństwa cybernetycznego, a my koncentrujemy się na kluczowych priorytetach, które dotyczą ludzi, procesów i technologii” . Jedną z dyrekcji DHS jest Dyrekcja ds. Nauki i Technologii, która wspiera programy promujące świadomość w zakresie bezpieczeństwa cybernetycznego i zwiększone możliwości zarówno w sektorze publicznym, jak i prywatnym. W ramach tej dyrekcji działa Centrum Badań i Rozwoju w zakresie bezpieczeństwa cybernetycznego, które zapewnia kierunek przyszłych badań i rozwoju w zakresie bezpieczeństwa cybernetycznego. Działalność centrum obejmuje również zapobieganie cyberprzestępczości, bezpieczeństwo sieci bezprzewodowej, niezawodność i integralność systemu nazw domen (DNS) oraz współpracę z innymi zainteresowanymi agencjami rządowymi agencjami. DNS to tablica serwerów rozproszonych na całym świecie z bazami danych, które przekształcają nazwy domen, takie jak www.xyz.com, na adresy IP, takie jak 34.167.86.94. W przypadku zaatakowania tych serwerów cyberprzestrzeń oparta na www upadnie. Utrzymywanie pamięci podręcznej DNS na komputerze może sprawić, że surfowanie będzie szybsze i mniej zależne od serwerów DNS. Pamięć podręczna DNS to dwupolowa baza danych obsługiwana na komputerze PC, która ma nazwy domen i odpowiednie adresy IP odwiedzanych stron internetowych.

Gotowość do cyberbezpieczeństwa

NCSD sponsoruje różne działania i inicjatywy mające na celu poprawę umiejętności i możliwości cyberobrony. Dwie główne to

• Cyber Storm. Jest to odbywające się co dwa lata ćwiczenie w zakresie cyberobrony, które przyciąga międzynarodowy udział i gdzie testowane są nowe umiejętności w zakresie cyberobrony. Pierwsze ćwiczenie Cyber Storm miało miejsce w 2006 r. Dzięki tym ćwiczeniom ocenia się gotowość do reagowania na incydenty cybernetyczne, a także wymianę informacji i koordynację między partnerami. Uczestnikami Cyber Storm w 2010 r. Były inne agencje rządowe USA, stany w ramach związku, liczne kraje i wiele organizacji sektora prywatnego. Cyber Storm IV ma się odbyć w 2012 roku.

• Krajowy system ostrzegania cybernetycznego. Ten program zwiększa świadomość zaniepokojonych mieszkańców cyberprzestrzeni na temat aktualnych zagrożeń i słabości w cyberprzestrzeni. Zainteresowane osoby mogą się zarejestrować [30], aby otrzymywać comiesięczne aktualizacje, a także biuletyny, dotyczące stanu bezpieczeństwa cybernetycznego. Główne inicjatywy są następujące:

• Alerty bezpieczeństwa cybernetycznego - techniczne

• Alerty bezpieczeństwa cybernetycznego - nietechniczne

• Biuletyny bezpieczeństwa cybernetycznego

• Wskazówki dotyczące bezpieczeństwa cybernetycznego

• Uwagi o luce w zabezpieczeniach

• Aktualna działalność

Subskrypcja systemu powiadomień jest bezpłatną usługą publiczną świadczoną przez DHS, a kilka tysięcy subskrybentów korzysta z tych miesięcznych powiadomień.

Wyzwania związane z bezpieczeństwem w cyberprzestrzeni

Każda agencja rządowa odpowiedzialna za bezpieczeństwo cyberprzestrzeni stoi przed licznymi wyzwaniami, które można podzielić na społeczne, gospodarcze, technologiczne i polityczne. Społeczeństwo oczekuje, że władze zapewnią bezpieczeństwo w sposób przejrzysty, skuteczny, skuteczny i w żaden sposób nie narusza wolności obywatelskich, zwłaszcza prawa do prywatności i prawa do wyrażania własnej opinii.

Bardzo ważnym czynnikiem w walce z przestępczością jest możliwość spojrzenia w przeszłość. Zdolność do wyszukiwania danych i wydobywania cennych informacji dotyczących kryminalnych nie może zostać zastąpiona informacjami z okresu po popełnieniu przestępstwa. Jednak przechowywanie zapisów cybernetycznych we wszystkich obszarach, na wypadek gdyby cyberprzestępca mógł popełnić przestępstwo w ciągu najbliższych pięciu lat, nie powinno być dopuszczalne w wolnym społeczeństwie. Socjologowie i prawodawcy zawsze będą mieli wyzwanie w dążeniu do znalezienia właściwej równowagi między prawami obywatelskimi a bezpieczeństwem, równowagi, która podlega normom społecznym, które ewoluują wraz z technologią. W związku z tym polityka bezpieczeństwa cybernetycznego może być kompletna tylko wtedy, gdy ma odpowiednią „ocenę wpływu na prywatność". Nie ma przedsięwzięcia, które nie byłoby ekonomicznie trudne. Fundusze trafiające do dowolnego sektora, czy to cyberbezpieczeństwa, czy upiększania ulic, muszą konkurować z wymaganiami innych sektorów. Chociaż więcej zasobów spowoduje lepsze bezpieczeństwo cybernetyczne, odpowiedzialni menedżerowie będą musieli przeprowadzić własną akcję równoważenia, rozkładając dostępne zasoby między różne podsektory bezpieczeństwa cybernetycznego, mając nadzieję na maksymalizację ogólnego bezpieczeństwa. Dzięki „kwantyfikacji wartości ekonomicznej bezpieczeństwa i pewności" menedżer może najlepiej obliczyć zwrot z inwestycji w bezpieczeństwo cybernetyczne. Biorąc pod uwagę, że cyberbezpieczeństwo wymaga wysoko wykwalifikowanych cyber wojowników lub cyberobronców, dostępne fundusze mogą odegrać zasadniczą rolę w programach edukacyjnych i specjalistycznych szkoleniach, a ciągłe kształcenie jest kamieniem węgielnym sukcesu. Ważnym wyzwaniem w ramach cyberekonomii są wskaźniki bezpieczeństwa cybernetycznego. Metryki są wynikiem uzyskanym po przetworzeniu powiązanych pomiarów. Wyzwanie polega na tym, jakie powinny być pomiary i jak należy przetwarzać wyniki. Zarządzanie przedsiębiorstwem i administracja rządowa nie wahają się zatwierdzać środków na bezpieczeństwo cybernetyczne, ale ponieważ same nie są technikami, szukają namacalnego, choć parametrycznego sposobu pomiaru zwrotu z inwestycji. Pomiar skuteczności lub skuteczności środka bezpieczeństwa, który stał na straży, ale nigdy nie został skonfrontowany, jest wyzwaniem samym w sobie. W kontekście cyberprzestrzeni odpowiedź na pytanie: czy jesteśmy wystarczająco bezpieczni? zawsze jest nie. Wynika to z faktu, że sieć jest nie tylko narażona na znane i nieznane zagrożenia cybernetyczne, ale każdy członek organizacji poprzez surfowanie, wysyłanie e-maili i tworzenie sieci społecznościowych stwarza dodatkowe podatności, przed którymi środki bezpieczeństwa cybernetycznego przedsiębiorstwa nie muszą koniecznie chronić. Oznacza to, że „stopień zrozumienia problemów bezpieczeństwa wśród użytkowników komputerów" w organizacji jest głównym czynnikiem w ocenie poziomu cyberbezpieczeństwa w systemie. Efektywne wykorzystanie technologii jest najważniejszym czynnikiem w praktycznie każdym sektorze, zwłaszcza w cyberbezpieczeństwie. Internet jest bardzo złożonym systemem, a identyfikacja źródła cyberataku może nie zawierać

marginesu błędu. Wyzwanie polega na opracowaniu ergonomicznego bezpieczeństwa cybernetycznego; oznacza to, że wykorzystuje zautomatyzowane procesy i procedury, które najlepiej wspierają specjalistów w ich misji. Po absolutnym zidentyfikowaniu źródła cyberataku wyzwaniem politycznym jest jego sklasyfikowanie. Taka klasyfikacja może wahać się od uciążliwych do cyberwarfare, ze wszystkimi powiązanymi konsekwencjami. W większości przypadków odwet będzie dokonywany raczej w naturze niż w innym trybie.

Rozproszona obrona

Ponieważ cyberprzestrzeń staje się integralną częścią praktycznie każdego aspektu współczesnego życia, zagrożenia dla jej bezpiecznego i niezawodnego działania rosną. Dzięki kryptografii zawartość komunikacyjna jest stosunkowo bezpieczna, a szybkie dostarczanie komunikacji może być utrudnione przez ataki typu „odmowa usługi" (DoS). Cyber-antimalware skutecznie chroni przed wirusami. Jednak ataki DDoS wydają się pozostawać poza kontrolą. Takie ataki przychodzą w dużych seriach tysięcy żądań, które przytłaczają możliwości obliczeniowe hostów internetowych. Zazwyczaj tak się dzieje

• Poprzez powtarzające się żądania, które obezwładniają zasoby serwera, atakują serwery, sieć lub urządzenia końcowe

• Poprzez wstrzyknięcie fałszywych komunikatów, takich jak komunikaty o połączeniach, rozłączeniach lub błędach, które dezorientują operacje serwera.

Internet nie został zaprojektowany z myślą o cyberprzestępcach i jest całkowicie podatny na wyrafinowane ataki DDoS, które stały się główną troską wszystkich funkcjonariuszy ds. Bezpieczeństwa cybernetycznego. Bardzo zaniepokojeni są także opiekunowie serwerów DNS. Nasycenie lub nieprawidłowe działanie takich serwerów spowoduje niedostępność tysięcy stron internetowych. Ataki DDoS zwiększały częstotliwość i siłę, osiągając poziom blisko 50 Gb / s w jednym ataku.

Środki zaradcze w zakresie cyberbezpieczeństwa

Środki zaradcze DDoS rozpoczynają się od wykrycia potencjalnego ataku, następnie oceniają potencjał ataku, a kończą koniecznymi działaniami, które należy podjąć. Takie działania obejmują opóźnienie lub odrzucenie podejrzanych pakietów oraz, jeśli to możliwe, powiadomienia węzłów internetowych do przodu i do tyłu o podejrzeniu ataku DDoS. Zwiększona prędkość sieci w połączeniu z równie zwiększonym rozmiarem pamięci i pamięci komputera pozwala teraz na włączenie zaawansowanych algorytmów w węzłach sieci, w których można monitorować, oceniać i kontrolować ruch. W ten sposób „funkcje bezpieczeństwa są wbudowane w urządzenia cybernetyczne w sposób, który pozwala na koordynację działań zapobiegawczych i obronnych w obrębie społeczności urządzeń i pomiędzy nimi". Wdrożenie takich algorytmów w węzłach internetowych może wspólnie stworzyć system prognozowania ruchu, w którym serwery docelowe będą informowane o zbliżającym się ruchu, jego natężeniu i, co równie ważne, jego pochodzeniu. Obecnie nie ma takiego systemu. Trwają jednak znaczące badania, które wskazują na potrzebę opracowania SCADA przez Internet. Każdy internetowy system SCADA musi mieć ściśle określony zakres, mierzalną skuteczność, możliwą do kontrolowania złożoność oraz praktyczną skalowalność, koncentrując się na wczesnym ostrzeganiu typu wykrywania DoS

Ekosystem Cyberobrony

Liczne działania badawcze w zakresie cyberobrony wskazują na jeden konkretny kierunek, to znaczy stworzenie specjalnego oprogramowania sztucznej inteligencji , które zostaną osadzone w każdym węźle internetowym, gdzie będą zbierać informacje o ruchu. Wspólnie i we współpracy ze sobą, takie

oprogramowanie będzie służyć jako SCADA internetowa, która będzie w stanie wykrywać potencjalne ataki DoS i zapobiegać im.

Obecnie Internet jest jedynie globalną siecią połączonych routerów, które ułatwiają kompleksową komunikację między klientami internetowymi a serwerami internetowymi, bez żadnego potencjału cyberbezpieczeństwa. Zarządzając tym ruchem, węzły internetowe uzyskują dostęp do danych, które łącznie mogą dać najbardziej cenne informacje. Na podstawie ocen statystycznych i innych obserwacji pakietów, internetowy SCADA - ekosystem cyberobrony - będzie w stanie monitorować powiązany ruch i dynamicznie ustalać kryteria, które będą w stanie rozpoznać podejrzane ataki DDoS. Wszystkie usługi wspierane technologią mają minimalny rozmiar i funkcjonalność i stopniowo stają się potężnymi i użytecznymi zasobami społecznościowymi. Podobnie Internet zaczął się jako platforma do wysyłania wiadomości tekstowych i stał się integralną częścią życia każdego. Obecnie poziom funkcjonalności węzłów internetowych można porównać do poziomu telefonów komórkowych z lat 90. - minimalnego i inteligentnego. W przypadku węzłów internetowych następnym krokiem jest wyjście poza etap przekazywania pakietów i wspólne stworzenie infrastruktury, która wspiera bezpieczeństwo serwera i ładuje projekcje, przynajmniej na początek. Jako system, węzły internetowe są niewykorzystanym zasobem. Po wprowadzeniu do nich danych wywiadowczych dotyczących bezpieczeństwa powstanie ekosystem cyberobrony.

Szkolenie w zakresie cyberbezpieczeństwa

Szkolenie w zakresie bezpieczeństwa cybernetycznego jest obowiązkiem wszystkich osób, które je ujawniają, ich komputery do cyberprzestrzeni. Stopień szkolenia będzie się różnić w zależności od zaangażowania. Jeśli spojrzymy na dwa końce spektrum, widzimy użytkowników cyberprzestrzeni z jednej strony i specjalistów ds. Cyberbezpieczeństwa na drugim końcu. Użytkownicy cyberprzestrzeni ponoszą odpowiedzialność za siebie i społeczność cyberprzestrzeni za utrzymanie zdrowego komputera, wolnego od złośliwego oprogramowania, które może infekować innych za pośrednictwem cyberprzestrzeni. Co najmniej komputer musi mieć aktywne oprogramowanie antywirusowe, które sprawdza każdy plik przed jego otwarciem lub zainstalowaniem na komputerze. Użytkownicy cyberbezpieczeństwa muszą mieć świadomość bezpieczeństwa, zwłaszcza, że dotyczy to akceptacji plików i aplikacji z nieznanych źródeł, ponieważ akceptacja użytkownika może zastąpić zaporę ogniową lub program antywirusowy w celu ochrony komputera. Tę świadomość należy wzmocnić poprzez częste seminaria - seminaria internetowe, jeszcze lepsze - oraz wiedzę na temat ryzyka związanego z sieciami społecznościowymi. Specjaliści ds. Cyberbezpieczeństwa muszą mieć szerokie spektrum umiejętności i wiedzy specjalistycznej, koncentrując się na co najmniej jednej specjalizacji. Specjaliści od cyberbezpieczeństwa wybrali karierę, która charakteryzuje się intensywnym uczeniem się przez całe życie i monitorowaniem prawodawstwa technologicznego.

Cyber-symulacja i ćwiczenia

Duża ilość zasobów jest stale przeznaczana na cyberbezpieczeństwo i potężne twierdzenia co do poziomu gotowości. Nie ma jednak wiarygodnych danych pozwalających ocenić i skalibrować siłę cyberobrony. Nie było prawdziwej cyber wojny, która przetestowałaby możliwości obronne i ofensywne potencjalnych przeciwników. Zamiast tego istnieje możliwość symulacji cyber wojny. Przez lata przeprowadzano symulacje przy użyciu dużych tablic cyber hostów - komputerów - i serwerów. Botnetowanie dużej liczby hostów w celu bombardowania określonego serwera i utworzenia DoS nie jest łatwym atakiem. Na szczęście było oprogramowanie do symulacji cyberwojennego opracowania, które mogą naśladować ataki w milionach. Biorąc pod uwagę zależność nowoczesnego społeczeństwa od Internetu,i jak „cyberwojna jest subtelna i dewastująca” , rządy były bardzo zaniepokojeni lukami w sieci. W rezultacie cyberćwiczenia są ważnymi mechanizmami przeprowadzanymi w celu]

• Oceń środki gotowości w stosunku do

• Cyber-zagrożenia

• Klęski żywiołowe

• Awarie technologii

• Umożliwić organom zaradzenie określonym słabościom

• Zwiększenie współpracy między odpowiednimi zainteresowanymi stronami

• Zidentyfikuj współzależności

• Stymuluj planowanie ciągłości

• Trenuj i edukuj ludzi

• Stwórz poziom pewności co do cyberbezpieczeństwa

Cyber ćwiczenia wymagają obszernych

• Planowanie ataków i kontrataków, fałszowania i włamań, zakłóceń i degradacji

• Testowanie [oceny] różnych strategii i taktyk ograniczania szkód, identyfikowania słabych punktów i tworzenia redundancji

• Szkolenie personelu w zakresie rozpoznawania problemów oraz skutecznego dostosowywania się i reagowania

• Cyber Endeavour, rząd USA, przemysł i środowisko akademickie

• Cyber Storm, międzynarodowe ćwiczenie zorganizowane przez Stany Zjednoczone

• Cyber Europe, ćwiczenie regionalne zorganizowane przez Unię Europejską

Cyber Endeavour to coroczne wydarzenie organizowane przez podmioty wojskowe rządu Stanów Zjednoczonych, które „zapewnia oddolną, poziom pracy i środowisko dla operatorów, myślicieli i praktyków, aby wspólnie dyskutować i identyfikować potencjalne rozwiązania najbardziej krytycznych, palących wyzwań cybernetycznych oraz zestawy problemów stojące przed… ”cyberbezpieczeństwem. Wydarzenie obejmuje Sympozjum Cyber, Cyber Gry i Konkursy oraz Cyber Wystawy. Cyber Storm jest ćwiczeniem cybernetycznym, które odbywa się co dwa lata od 2006 roku. Jest organizowane przez National Cyber Security Division Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych i zapewnia ocenę gotowości Stanów Zjednoczonych na wypadek wojny cybernetycznej. Uczestniczą w nim organizacje sektora publicznego i prywatnego, a także podmioty międzynarodowe [39]. Cyber Europe to pierwsze europejskie ćwiczenie cyberbezpieczeństwa, którego celem było stworzenie społeczności cyberobrony wśród członków państwa. Uczestniczyło w nim siedemdziesiąt organizacji sektora publicznego z dwudziestu dwóch krajów, a niektóre dodatkowe uczestniczyły jako obserwatorzy. Ćwiczenie zostało zorganizowane przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), agencję Unii Europejskiej. Jednym z zaleceń było, aby takie ćwiczenia odbywały się również na poziomie krajowym w celu zdobycia doświadczenia i wiedzy specjalistycznej [40]. Wspólne cele ćwiczeń były następujące

• Twórz, testuj i ulepszaj zasady i procedury komunikacyjne dla różnych scenariuszy cyberataków

• Zidentyfikuj obszary wymagające poprawy i oceń wartość polityki zagadnienia

• Oceń mechanizmy wymiany informacji

• Zidentyfikuj krytyczne współzależności między infrastrukturą cybernetyczną a fizyczną

• Zwiększenie świadomości roli cyberbezpieczeństwa w bezpieczeństwie narodowym i gospodarce

• Rozwijanie znajomości dostępnych narzędzi i technologii dla cyberbezpieczeństwa

Informacje o działaniach wojennych w obszarze informacji o działaniach wojennych W wojnie informacyjnej najcenniejszą informacją o działaniach wojennych jest wiedza o istnieniu luk w zabezpieczeniach zero-day. To znaczy, wiedząc, jakie dziury istnieją w cyberprzestrzeni przeciwnika i jak zadać maksymalne obrażenia poprzez ich wykorzystanie. Jest już stara wiadomość, że każde ministerstwo obrony narodowej ma dział walki cybernetycznej, a każde ministerstwo spraw zagranicznych ma dział cyberinformacji. Obecnie jest otwarte, że cyberwojna wojna jest rzeczywistością. 20 stycznia 2017 r. Strona internetowa Białego Domu opublikowała: „Cyberwarfare to nowe pole bitwy i musimy podjąć wszelkie środki, aby zabezpieczyć nasze tajemnice i systemy bezpieczeństwa narodowego. Priorytetem dla nas będzie rozwój defensywnych i ofensywnych zdolności cybernetycznych w naszym amerykańskim Cyber Command oraz rekrutacja najlepszych i najbystrzejszych Amerykanów, którzy będą służyć w tym kluczowym obszarze.

Ta publikacja w witrynie mówi światu, aby zrobiła to samo. Różnica między umowami o wojnie konwencjonalnej a umowami o nierozprzestrzenianiu polega na tym, że rozmiary sił zbrojnych i zdolności są dobrze znane lub można je rozsądnie oszacować. Dokładniej mówiąc, nie można poznać wielkości siły cybernetycznej w kraju lub siły informacyjnej, ponieważ cyberwojna jest ograniczona do cyberprzestrzeni, czyli przestrzeni internetowej, natomiast w wojnie informacyjnej cała przestrzeń elektroniczna jest uwzględniona.

Fałszowanie sygnałów GPS, które może wprowadzać w błąd działania wspierane przez GPS, takie jak nawigacja, jest potężnym środkiem obronnym przeciwko dronom wroga. Doskonałym przykładem jest to, że „[rząd] Iranu ogłosił, że amerykański bezzałogowy samolot, wykryty w irańskiej przestrzeni powietrznej, został zestrzelony przez jednostkę cyberwojną stacjonującą w pobliżu Kaszmaru i sprowadzony z minimalnymi uszkodzeniami". Na poziomie stanu cyberbezpieczeństwo nie jest tak bardzo zagrożone przez samouków cyberprzestępców i cyberterrorystów, ale przez dobrze finansowanych, dobrze wykształconych i dobrze wykwalifikowanych sponsorowanych przez państwo cyber-aktorów. W rezultacie „… istnieje pilna potrzeba, aby wszystkie sektory i rządy (w celu stworzenia państwowego podmiotu cyberobrony / przestępstwa) zapobiegały cyberatakom, wykrywały je, odzyskiwały i broniły się przed nimi. Przy tworzeniu państwowego podmiotu cyberobrony / przestępstwa istnieją cztery główne wyzwania, a mianowicie:

• Jak odróżnić misję nominalną od prawdziwej misji przedsięwzięcia.

• Jak określić najbardziej efektywny jakościowo i ilościowo rozmiar i struktura.

• Jak przyznać mu autonomiczny, ale uzasadniony autorytet

• Jak wybrać agencję rządową, w której ma być, bez naruszania istniejącej wewnętrznej równowagi politycznej władzy w kraju. Główną różnicą między wojną konwencjonalną a cyberwoją jest to, że w wojnie konwencjonalnej napastnicy i ich lokalizacje są dobrze identyfikowalne, podczas gdy w wojnie cybernetycznej praktycznie niemożliwe jest ustalenie lokalizacji lub tożsamości atakującego.

Opracowanie krajowej strategii na rzecz bezpieczeństwa cybernetycznego

Gdy cyberprzestrzeń narzuciła się światu, rządy uznały jej nieunikniona dominacja i jedna po drugiej uświadomiły sobie potrzebę opracowania krajowej strategii bezpieczeństwa cybernetycznego. To musi być strategia, która się równoważy na potrzeby ochrony krajowej i ochrony praw obywatelskich. Mianowicie prawa obywateli do wypowiedzi i prawa obywateli do prywatności. Ponadto należy przyjąć, że nie będzie absolutnej ochrony i że strategia ta będzie musiała zostać zaktualizowana w miarę ewolucji społeczeństwa i technologii. Ogólnie rzecz biorąc, taka strategia powinna obejmować:

* Stwórz grupę roboczą ds. Bezpieczeństwa cybernetycznego ze scentralizowanym zespołem wsparcia w sytuacjach kryzysowych, służącym jako zaufany punkt kontaktowy i jako krajowy koordynator ds. Cyberprzestrzeni.

* Ustanowienie programu edukacyjnego dotyczącego świadomości w zakresie bezpieczeństwa cybernetycznego, rozpowszechnianie najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego i budowanie kultury bezpieczeństwa cybernetycznego

* Zbuduj bezpieczną i niezawodną agencję rządową udostępniającą informacje w cyberprzestrzeni.

* Daj obywatelom i organizacjom możliwość wniesienia wkładu w dialog krajowy.

* Wyszczególnij narodowe priorytety, zasady, polityki i programy.

* Określ role i misje każdej zaangażowanej agencji rządowej i organizacji pozarządowej.

* Określ cele, kamienie milowe i wskaźniki, aby mierzyć i komunikować zakres postępów w rozwiązywaniu problemów.

* Wspieranie międzynarodowej współpracy w zakresie bezpieczeństwa cybernetycznego.

Podobnie jak w przypadku każdej współczesnej strategii, każda krajowa strategia bezpieczeństwa cybernetycznego musi rozpoznać odpowiednie potrzeby i wskazać drogę ,że należy się tym zająć. W takim przypadku strategia musi spełniać następujące zasady:

* Oparte na ryzyku. Cyberprzestrzeń jest pełna różnych rodzajów ryzyka.

* Modelowanie zagrożeń. Zajmij się wszystkimi możliwymi zagrożeniami, niech to będzie cyberprzestępczość lub szpiegostwo.

* Zorientowany na wyniki. Wyartykułuj i skup się na pożądanym wyniku końcowym.

* Priorytetowo. Ustal jasne priorytety wśród celów strategii.

*Pełen szacunku. Obejmują ochronę prywatności i swobód obywatelskich.

Chociaż w wielu krajach przyjęto narodową strategię bezpieczeństwa cybernetycznego, Austria przyjęła „samoregulację" w celu zachęcania sektora prywatnego do ustanowienia własnych standardów w zakresie bezpieczeństwa cybernetycznego, a państwo tworzy niezbędne ramy regulacyjne. Podsumowując, celem krajowej strategii bezpieczeństwa cybernetycznego jest służyć jako centralny punkt obrony narodu przed tym niewidzialnym, choć realnym zagrożeniem dla interesów narodowych kraju.

Cyfrowe waluty

Wprowadzenie

Zazwyczaj waluty cyfrowe to prywatne wartości pieniężne, które istnieją tylko w księgach rachunkowych. Oznacza to, że cyfrowa waluta - oferowana i administrowana przez prywatną organizację - omija konwencjonalny system bankowy i waluty rządowe, pozwalając wartości pieniężnej na zmianę własności zakupu towarów i usług. Ponieważ waluty te nie mają fizycznego aspektu do ochrony, ich ochrona i integralność są chronione za pomocą ciężkich środków kryptograficznych i dlatego nazywane są kryptowalutami. Równolegle do miękkich kryptowalut, czyli walut, które istnieją tylko w księgach bazy danych, istnieją również twarde kryptowaluty, czyli waluty posiadające fizyczną reprezentację. Przykładami takich walut są peercoin. Podczas gdy najbardziej znaną kryptowalutą jest Bitcoin z jej Rynkiem , istnieje wiele innych takich walut dostępnych publicznie lub prywatnie§. Korzystanie z kryptowalut umożliwia anonimowość w transakcji, a tym samym zapewnia prywatność podczas przeprowadzanej transakcji.

Koncepcja Blockchain

Fizyczne jednostki pieniężne, takie jak pieniądz papierowy, są ponumerowane w celu wskazania ich wyjątkowości i względnie trudno je powielić. Podobnie mają metalowe jednostki monetarne, takie jak złote i srebrne monety ich własną wartość wewnętrzną, a ich powielanie jest niepraktyczne. Z drugiej strony, jednostki waluty cyfrowej są śledzone według ich wykorzystania, ponieważ są wykorzystywane, zmieniając właścicieli w tym procesie. Śledzenie jest wdrażane za pomocą wysoce bezpiecznej otwartej księgi - bazy danych - która rejestruje wszystkie transakcje, które przechodzą cyfrowe jednostki walutowe. Każda transakcja jest określana jako blok, a księga rejestruje każdą transakcję, która ma miejsce w określonym systemie kryptowalut. Każda transakcja, czyli każde użycie pieniądza cyfrowego, ma znacznik czasu i łącze do źródła tego pieniądza cyfrowego. Organizacje zarządzające kryptowalutami twierdzą, że „Z założenia łańcuchy bloków są z natury odporne na modyfikację danych". Ponieważ bloki są ze sobą połączone - są powiązane łańcuchem - koncepcja nazywa się blockchain. W ogólnym ujęciu koncepcja tworzenia łańcucha bloków, czyli rejestrowania sekwencji zdarzeń trwale zapisanych w bazie danych, ma zastosowanie w wielu obszarach, w tym w dziedzinie medycyny i wojsku.

Kryptowaluty

Istnieje wiele organizacji, które wydają kryptowaluty. Uważali, że jest to ponad siedemset organizacji emitujących waluty cyfrowe. OneCoin twierdzi, że „Wyzwania prawne związane z kryptowalutami są głównie związane z anonimowością transakcji i decentralizacją transakcji finansowych. " Monero twierdzi, że „... to bezpieczna, prywatna, niemożliwa do wykrycia waluta". Wiele takich organizacji stosuje zewnętrzny nadzór audytowy w celu ustalenia reputacji w zakresie zachowania integralności, a przede wszystkim prywatności. Władze są zaniepokojone przede wszystkim dwoma głównymi kwestiami dotyczącymi branży kryptowalut, jeśli możemy to tak nazwać. Pierwsza polega na tym, że za anonimowymi transakcjami kryje się możliwość ukrywania przestępczych / nielegalnych działań. Uważa się, że kryptowaluty „... były dość dyskusyjnym narzędziem płatności z powodu złych przepisów i wysokiej atrakcyjności dla międzynarodowej działalności przestępczej." Federalne Biuro Śledcze USA jest bardzo zaniepokojone wykorzystywaniem kryptowalut do celów przestępczych działania, po wielu aresztowaniach za takie przestępstwa. Drugi dotyczy integralności kryptowaluty, przy czym bicie odpowiedniej waluty odpowiada dostępnym konwencjonalnym aktywom pieniężnym. W przypadku nieuregulowania kryptowaluty mogą stać się niewypłacalne, niezdolne do konwersji kryptowaluty na konwencjonalne pieniądze - dolary, euro itp. W odpowiedzi na takie możliwości firmy ubezpieczeniowe

oferują ochronę przed stratami w kryptowalutach wynikającymi z cyberprzestępczości, takimi jak kradzież, włamanie lub niewypłacalność. Istnieje wiele kryptowalut, a nowe pojawiają się stale.

Bitcoin

Bitcoin jest najbardziej znaną z kryptowalut. Według organizacji Bitcoin „... podaż Bitcoin jest matematycznie ograniczona do dwudziestu jeden milionów bitcoinów, których nigdy nie można zmienić ”i„… sieć Bitcoin jest nie do powstrzymania i nie do zniesienia ”. Ostatnie oświadczenie dotyczy agencji zapobiegania przestępczości na całym świecie, podczas gdy jest wyraźnym zaproszeniem do nielegalnych działań. To oświadczenie nie jest unikalne dla monet Bitcoin, ale dotyczy wszystkich walut cyfrowych, które prowadzą konta nie podlegające wymianie. Kancelaria specjalizująca się w sprawach cybernetycznych stwierdza: „Ta cyfrowa waluta (Bitcoin) przetwarzana przez Internet nie podlega nadzorowi centralnego organu wydającego”.

Przekształcenie tradycyjnej przestępczości w cyberprzestępczość

Wkład generała Emmanuela Sfakianakisa, dyrektora Wydziału Anty Cyberprzestępczości greckiej policji.

Wprowadzenie

Celem tej części jest wykazanie, w jaki sposób cyber i inne technologie elektroniczne są obecnie w służbie przestępcom, których działania wymagają śledczych z zaawansowanymi umiejętnościami cybernetycznymi. Powoli i konsekwentnie musimy zdawać sobie sprawę z tego, że w nadchodzącym stuleciu i za pośrednictwem Internetu nasze życie stanie się piękniejsze, przyjemniejsze, bardziej produktywne i dzięki wyjątkowym doświadczeniom, wbrew coraz bardziej wyrafinowanemu i rosnącemu cyberprzestępstwu. Musimy zdać sobie sprawę, że przestępcy - złodzieje, włamywacze, rabusie, terroryści itp. - powoli porzucają narzędzia epoki kamienia i wkraczają w erę zaawansowanych technologii, w której za pośrednictwem mediów elektronicznych będą mogli zaatakować nasze życie i osiągnąć swoje cele, tym razem online. Aby zrozumieć wagę możliwych nadużyć w cyberprzestrzeni, zadajmy sobie następujące pytania:

• Popełniania morderstw lub szantażu i zbierania pieniędzy na wymuszenia, nie pozostawiając po sobie śladu?

• Ingerować w operacje organizacyjne (samoloty, pociągi, metro, instytucje bankowe itp.)?

Niestety, dzisiaj przez Internet jest to możliwe i jest realizowane,codziennie. Obecna era online zmieniła wszystko wokół nas. Internet daje nam wiedzę, informacje, komunikację, ekonomię rozwój, dobre samopoczucie i wiele więcej. Może również sprawiać nam ból poprzez przestępstwa. Dzisiaj wiele osób demonizuje Internet, zamiast akceptować fakt, że jest on jak elektryczność. Energia elektryczna ułatwia nam życie, ale może być również śmiertelna. Jeśli nie będziemy przestrzegać zasad korzystania z Internetu, możemy stać się ofiarami zachowań przestępczych, które różnią się stopniem surowości i niebezpieczeństwem. Ludzie muszą zrozumieć, że dziś przestępczość zmieniła się z tradycyjnej na elektroniczną. Smutne jest to, że na całym świecie prawodawstwo nie dogoniło tej mutacji. W rezultacie w sądach toczą się obecnie tysiące spraw karnych i cywilnych, które są przestępstwami czysto elektronicznymi lub zawierają elementy wymagające dochodzenia w sprawie cyberprzestępczości. Należy zauważyć, że stopniowo każde przestępstwo będzie wymagało dochodzenia elektronicznego. Wszystkie dochodzenia policyjne w sprawie poważnych przestępstw (terroryzm, zabójstwo, szantaż, porwanie, zapobieganie samobójstwom, zaginięcia itp.) Obejmują element elektroniczny. W rezultacie rozpaczliwie potrzebna jest nowa rasa śledczych policji. W związku z tym wszyscy kuratorzy sądowi, śledczy, prokuratorzy, a także sędziowie zajmujący się sprawami, które posiadają dowody na istnienie elementów elektronicznych, muszą znać podstawowe zasady przestępczości elektronicznej. Od 1995 roku, jako policyjny śledczy cyberprzestępczy, obsłużyłem ponad dziesięć tysięcy spraw z łącznej liczby około dwudziestu tysięcy spraw mojego Departamentu. Jak pamiętam, w 1995 r. Mieliśmy od dwóch do trzech spraw miesięcznie. Obecnie w 2017 r. Skargi dotyczące cyberprzestrzeni wynoszą średnio osiemdziesiąt dziennie. Typowym cyberprzestępczością jest oprogramowanie ransomware, w którym wirus instaluje się na komputerze ofiary. Blokuje wszystkie funkcje, wyświetlając na ekranie komunikat żądający okupu w zamian za odblokowanie komputera. Poniżej znajdują się dwa typowe przypadki ransomware, z jakimi często spotykają się władze.

Przypadek pierwszy: Wirus ransomware uderza w komputery ofiar, blokując wszystkie funkcje i wyświetlając komunikat o wymuszeniu. Wiadomość ma logo jednostki ds. w alki z cyberprzestępczością w policji danego kraju, twierdząc, że ten komputer - komputer ofiary - odwiedził witryny o

zabronionych treściach i że został ukarany grzywną w wysokości X euro. Wiadomość o wymuszeniu zawiera także instrukcje i linki do stron internetowych, na których ofiara może kupić e-gotówkę i zapłacić okup.

Przypadek drugi: Podobny wirus ransomware, który uderzył w wiele komputerów, szyfruje wszystkie pliki komputera, wyświetlając wiadomość o wymuszeniu wymagającą kwoty X euro, którą można zapłacić w e-walucie BitCoin. W obecnych okolicznościach transakcje BitCoin są niemożliwe do wykrycia.

Faktem jest, że niewykrywalne e-waluty uniemożliwiły władzom na całym świecie właściwe prowadzenie dochodzeń i ściganie przestępstw. Warto przeczytać oficjalne dokumenty przedstawiające cyberprzestrzeń w przyszłości. Jednym z takich dokumentów jest biała księga: prognoza i metodologia Cisco VNI, 2015-2020 , która przewiduje i analizuje rozwój i trendy w Internecie. W przeciwieństwie do tej wykładniczej ewolucji, która ma miejsce w cyberprzestrzeni, opracowanie nowych ram prawnych dotyczących przestępczości elektronicznej jest znacznie opóźnione. Prognozy Cisco są ogólnie konserwatywne i niezwykle dokładne, pokazując światową tendencję do szybkiego dostosowywania się do nowych technologii. Smutne jest to, że dostępność zaawansowanych technologii zwiększa stopień zaawansowania przestępczości.

Przestępczość elektroniczna

Najpierw zdefiniujmy, co rozumiemy przez przestępczość elektroniczną, której cyberprzestępczość jest w przeważającej części. Zasadniczo przestępczość elektroniczna to przestępstwa popełnione przy użyciu technologii

• W przypadku samodzielnych komputerów, fałszowanie pieniędzy lub tworzenie fałszywych dokumentów. Lub,

• Z wykorzystaniem niepewności w cyberprzestrzeni, gdzie istnieje szerokie spektrum przestępstw, od piractwa własności intelektualnej po cybernękanie.

Przypadek trzeci: Przestępcy elektroniczni posiadający wysokiej jakości sprzęt do produkcji kart kredytowych we współpracy z kasą sklepu „zgromadzili" dane paska magnetycznego ważnych kart i następnie osadzili je na fałszywych kartach noszących nazwy użytkowników. W związku z tym wyświetlanie ważnego dowodu tożsamości ze zdjęciem dawało wiarygodność karcie kredytowej, ponieważ obie miały tę samą nazwę. Jednak natychmiastowe powiadomienie o użyciu podrobionej karty doprowadziło policję do sklepu, w którym była używana, i do aresztowania przestępcy elektronicznego.

Cyberprzestępczość jest szybka, popełniana w milisekundach i często nie jest rozpoznawana przez ofiary. Szybkość i łatwość przeprowadzania cyberprzestępczości przyciągnęła wykwalifikowanych cyberprzestępców, co stanowi poważną wadę i niepokój dla organów ścigania na całym świecie. Powody rozpowszechnienia się cyberprzestępczości mogą być następujące:

• Specjalistyczna wiedza nie zawsze jest wymagana.

• Można popełnić na odległość i anonimowo.

• Umożliwia przestępcom szybkie i niedrogie komunikowanie się z osobami o podobnych poglądach, nawet w czasie rzeczywistym, bez konieczności przeprowadzki.

• Trudno jest ustalić rzeczywiste pochodzenie cyberprzestępczości.

• Jest bez granic. Bardzo często wymaga wielonarodowej współpracy w celu prowadzenia dochodzeń i prześladowań.

• Ścigane i ścigane cyberprzestępstwa stanowią wierzchołek góry lodowej.

• Dochodzenie policyjne jest stosunkowo trudne i wymaga doskonałego szkolenia i specjalistycznej wiedzy.

Dla osób zaangażowanych w funkcjonariuszy policji, prokuratorów okręgowych, sędziów i prawników zajmujących się przestępczością elektroniczną wymagana jest specjalistyczna wiedza, doświadczenie i umiejętności. Ponieważ jednak wszystkie przestrzegają litery prawa, nie mogą skutecznie wykonywać swoich obowiązków, jeżeli nie są wspierane przez odpowiednią infrastrukturę prawną.

Formy cyberprzestępczości

Według sondażu przeprowadzonego przez McConnell International w 52 krajach przestępstwa popełnione w cyberprzestrzeni są w większości następujące:

• Utrudnianie ruchu (cyber)

• Modyfikacja i kradzież danych

• Inwazja i sabotaż w sieci

• Nieautoryzowany dostęp

• Zastrzyki wirusa

• Traktowanie przestępstw

• Plagiat i oszustwo

Najczęstsze cyberprzestępstwa, które utrzymują organy zajmujące się zwalczaniem cyberprzestępczości, są następujące:

• Oszustwa przez Internet

• Przestępstwa związane z moralnością

• Pękanie i hackowanie

• Przejmowanie oprogramowania i piractwo

• Karty kredytowe

• Handel narkotykami

• Przestępstwa za pośrednictwem czatów

• Naruszenie - wprowadzenie w błąd danych osobowych (media społecznościowe itp.)

Badanie przestępstw elektronicznych

Podczas nawigacji w cyberprzestrzeni wszyscy użytkownicy Internetu pozostawiają unikalne ślady swojej tożsamości elektronicznej. Każdy ślad elektroniczny składa się co najmniej z trzech części, które zapewniają wyjątkowość tożsamości:

• Adres IP (adres połączenia internetowego przyznany dla tej konkretnej komunikacji)

• Data (na podstawie położenia geograficznego używanego urządzenia)

• Strefa czasowa lokalizacji urządzenia.

• Prawdopodobnie numer seryjny podłączonego urządzenia (komputer, telefon itp.)

• Prawdopodobnie numer seryjny używanej aplikacji (przeglądarka, serwer itp.)

W każdym dochodzeniu online podejmowana jest próba zlokalizowania elektronicznego śladu przestępcy, który jest unikalny dla każdej wymiany danych i jest bardzo ważnym dowodem w każdym postępowaniu sądowym. Oprócz korzystania z ich prawdziwej tożsamości można uzyskać dostęp do Internetu, publikując i podpisując jako anonimowe lub nawet używając pseudonimu. Ten stan domniemanej anonimowości w Internecie ułatwia i motywuje sprawców, którzy myślą, że zawsze pozostaną anonimowi, aby popełniać przestępstwa online. Anonimowość utrudnia ich zlokalizowanie, ale gdy organy ścigania dysponują odpowiednimi narzędziami i doświadczeniem, sprawcy nie będą w stanie uniknąć prawa. Jeśli anonimowa osoba popełni cyberprzestępczość, organy ścigania, w drodze postanowienia sądu, mogą otrzymać cyber ślady od dostawcy usług internetowych (ISP). Często proces ten wymaga czasu, co utrudnia proces ścigania. Podsumowując, w Internecie nie ma anonimowości, ale zdarzają się przypadki, w których aktor online korzystał z różnych elektronicznych programów unikania śledzenia lub bezpłatnych sieci bezprzewodowych. Jednak w takich przypadkach przestępstwa są badane za pomocą specjalnych technik prowadzących do identyfikacji sprawcy.

Przypadek czwarty: odrzucony kochanek opublikował anonimowo zdjęcia byłego partnera z numerem telefonu i zaproszeniami erotycznymi. Jednak z powodu braku doświadczenia w protokołach internetowych kochanek pozostawił wiele śladów, które doprowadziły do udanego ścigania.

Przypadek piąty: śledczy policji stwierdzili istnienie cyberprzestępcy, który handlował nielegalnymi / niemoralnymi materiałami online działającymi w kafejkach internetowych, które zapewniały anonimowość użytkownika. Jednak za pomocą specjalnych programów policja była w stanie rozpoznać ślady własności intelektualnej, które doprowadziły do aresztowania podejrzanego.

Hakerzy i crackerzy

„Zabójców cyberprzestrzeni" można podzielić na dwie kategorie, w zależności od ich intencji, sposobu ich penetracji i pożądanego rezultatu.

Hakerzy: zwykle hakerzy „atakują" komputer bez wyrządzania jakichkolwiek szkód lub pozostawiania śladów. Ich motywem może być przyjemność lub ciekawość, bez szukania korzyści ekonomicznych. W niektórych przypadkach hakerzy identyfikują słabość cyberbezpieczeństwa i zgłaszają ją właścicielowi komputera w nadziei na uznanie lub inną korzyść.

Crackerzy: Zwykle crackerzy „atakują" komputer, próbując zidentyfikować słabość cyberbezpieczeństwa i wykorzystać ją. Oznacza to, że szukają korzyści finansowych lub powodują cyfrowy wandalizm. Mówiąc prościej, crackerzy to cyberprzestępcy, którzy „atakują" swój system, aby uczyć się lub zdobywać coś w celu późniejszego popełnienia czynu niezgodnego z prawem.

Przypadek szósty: muły finansowe. Właściciele dużych sum pieniędzy, którzy chcą przenieść je z konta na konto, anonimowo zabiegają o posiadaczy rachunków, którzy mogą „przenieść" swoje pieniądze za bardzo wysoką „opłatą". W ten sposób tacy właściciele działają w sposób niewidoczny dla władz.

Dochodzenie w sprawie cyberprzestępczości

Dochodzenie w sprawie cyberprzestępstw jest dość trudnym i bardzo czasochłonnym zadaniem. Śledczy działają na zasadzie, że „przestępca zawsze pozostawia ślady. " Dochodzenia w sprawie

cyberprzestępczości obejmują identyfikację śladów elektronicznych. Dochodzenie może potrwać kilka minut do lat. Może to być czasochłonne, ponieważ cyberprzestępcy czerpią korzyści z braku ustawodawstwa, które zapewnia śledczym szybki dostęp do historycznych danych z komunikacji cybernetycznej. W każdej ankiecie internetowej próbuje się zidentyfikować ślady online przestępcy, które są unikalne, gdy każdy użytkownik Internetu porusza się po Internecie. Każdy rekord śladu może zawierać kilka parametrów, takich jak data, znacznik czasu i numery seryjne powiązanych aplikacji (przeglądarka, edytor tekstu, procesor obrazu itp.). Zbiór takich parametrów faktycznych służy jako ważny i niepodważalny dowód sądowy w ściganiu podejrzanego przestępstwa.

Cyberoszustwa finansowe

Podstawową zasadą oszustwa internetowego jest przekonanie ofiary, że płacąc teraz niewielką kwotę, czeka znacznie większa kwota. Oszustwa internetowe rosną wykładniczo, a jednocześnie wyrafinowanie oszustów. Zakres cyberprzestępstw finansowych osiągnął punkt, w którym powstały takie kategorie, jak opisano poniżej.

List Nigeryjski

Jest to wiadomość e-mail, która informuje potencjalną ofiarę, że ktoś, prawdopodobnie „były wysoki urzędnik wysokiego szczebla" w rządzie Nigerii, potrzebuje pomocy w przekazaniu - pod przykryciem - dużej kwoty (np. 30 mln USD) i jest skłonny uiścić „wysoką" opłatę w zamian za taką usługę. Odbiorca tego listu proszony jest o pomoc, działając jako „muł pieniężny", tymczasowo otrzymujący tę kwotę na swoim koncie. W liście podkreślono poufność, której należy przestrzegać. W pierwszej kolejności cyberprzestępcy proszą kandydata będącego ofiarą o zgodę i podanie informacji dotyczących jego kont bankowych oraz wszelkich informacji „uznanych za niezbędne" do przeprowadzenia transakcji. Wiele razy i na prośbę niczego niepodejrzewającej ofiary przedstawiane są dokumenty, które wydają się autentyczne i oficjalne, w celu wyeliminowania wszelkich wątpliwości, jakie mogła mieć naiwna ofiara. Gdy ofiara odpowiada, niekończący się proces wymiany maili, e-maili i połączeń telefonicznych zaczyna sprawiać, że potencjalna ofiara uważa, że proces otrzymywania dużych pieniędzy jest bliski. Tuż przed domniemanym „ostatecznym transferem pieniędzy" cyberprzestępcy informują ofiarę o nieoczekiwanym problemie. Takim problemem może być zapłata podatku, nieoczekiwana opłata lub potrzeba przekupienia pracownika banku, który autoryzuje przekaz pieniężny. Tutaj zaczyna się „haczyk". Cyberprzestępcy twierdzą, że nie są w stanie pokryć tych nieoczekiwanych kosztów, ponieważ duże pieniądze są zablokowane w transferze, i proszą potencjalną ofiarę o zapłatę tej kwoty, która, jak powiada ofierze, zostanie zwrócona po zakończeniu transakcja. Niektóre ofiary przekonuje się nawet do udania się do Nigerii, aby zapłacić kwotę w celu „sfinalizowania" transakcji. Co więcej, ofiara jest wprowadzana w błąd, że nie potrzebuje wizy, trafia nielegalnie do kraju, wpadając głębiej w sieć nigeryjskich przestępców. Takie przestępstwa nie są nowe. Odbywały się one za pośrednictwem listów i faksów. Dzisiaj kontynuują, z tą różnicą, że Internet jest infrastrukturą przestępców.

Przypadek siódmy. Pani o najwyższym poziomie wykształcenia została przekonana do wyjazdu do europejskiej stolicy w celu otrzymania „nagrodzonych" funduszy. Po przybyciu została potraktowana poważnie, prawdopodobnie w oczekiwaniu na transfer środków nastąpi. Pani została zabrana do banku, gdzie spotkała ją na korytarzu, prawdopodobnie wysokiego „urzędnika bankowego", który zapewnił ją o swoich funduszach. „Urzędnik" zwrócił uwagę, że bank natychmiast zwolni „nagrodę" w wysokości 12 milionów euro, jak tylko zostanie zapłacony podatek w wysokości 0,5 miliona euro. Pani przekazała swoje środki „urzędnikowi bankowemu". Przestępcy zostali w końcu złapani, ale fundusze zostały utracone na zawsze.

Hiszpańskie Lotto

Ta forma oszustwa odbywa się poprzez masowe wysyłanie e-maili do losowych użytkowników Internetu. Te wiadomości informują ich, że w loterii internetowej zarobili dużą ilość pieniędzy, rzędu milionów dolarów. Jednak odbiorcy nigdy nie brali udziału w lotto. Sprawcy, aby uwierzyć, używają nazwisk od dużych firm (np. Microsoft, Yahoo itp.) I towarzysząc wiadomościom wysyłają fałszywe certyfikaty dotyczące rzekomego losowania elektronicznego. Oszustwo polega na tym, że prosi domniemanych zwycięzców o dokonanie przedpłaty niektórych podatków, zwykle w wysokości kilku tysięcy dolarów. Co zaskakujące, ta kategoria cyberprzestępstw pochłania setki ofiar.

Phishing danych

Wyłudzanie informacji jest zwykle przeprowadzane przez wysyłanie masowych wiadomości e-mail ze spamem, które powinny być wysyłane przez istniejącą i legalną korporację (bank, sklep internetowy, usługa płatności elektronicznych itp.) W celu wprowadzenia odbiorcy w błąd i pobrania prywatnych danych osobowych i dane finansowe. Następnie sprawcy tego rodzaju oszustwa wykorzystują te dane do popełnienia przestępstwa. Zazwyczaj proszą o numery kart kredytowych z terminem płatności i numerem zabezpieczającym. Dzięki tym informacjom powstają fałszywe karty bankowe do nieuczciwego użytku.

Piractwo oprogramowania

Piractwo komputerowe oznacza nieautoryzowane powielanie i / lub usuwanie programów komputerowych chronionych prawem autorskim. Dystrybucja odtwarzanego materiału rozpoczęła się od obsługi płyt CD lub dyskietek. Jednak rozprzestrzenianie się Internetu otworzyło drogę do nowej formy przestępczości, w której materiał jest sprzedawany za pośrednictwem poczty e-mail, czatu lub aplikacji peer-to-peer.

Przypadek ósmy. Pakiet oprogramowania - własność intelektualna International Welding Corporation (IWC) - został nielegalnie wprowadzony na rynek i rozpowszechniany w Europie za pośrednictwem Internetu, co spowodowało stratę wielu milionów euro dla twórców oprogramowania. Nielegalne reklamy przyciągnęły uwagę IWC, a w ciągu kilku minut przestępcy zostali zlokalizowani i postawieni przed sądem.

Karty kredytowe

Zjawiska oszustw związane z używaniem kart kredytowych na rynkach internetowych rosną w szybkim tempie. Szacuje się, że banki liczą miliony euro strat poniesionych przez osoby, które robią podróbki, przechwytują numery kart kredytowych lub inne osoby, które dokonują zakupów online przy użyciu numerów kart znalezionych na przykład przez phishing lub wyprodukowanych za pomocą analogicznych algorytmów komputerowych.

Przypadek dziewiąty. Przestępca reklamuje dostępność określonego produktu w bardzo atrakcyjnej cenie, prosząc o niewielki procent zamówienia za pomocą karty kredytowej - z góry, a resztę należy zapłacić po otrzymaniu produktu. Wielu się na to zgadza, podając wszystkie dane swojej karty, aby zapłacić za niską „zaliczkę". Na podstawie tych informacji przestępcy dokonują nieuczciwych zakupów, a następnie sprzedają je za gotówkę.

Pokoje czatowe

Współczesny styl życia nie pozwala rodzicom poświęcać niezbędnego czasu na nadzór i prowadzenie dzieci, co prowadzi do stopniowego braku komunikacji. Ze swojej strony dzieci uwielbiają wysyłać i odbierać wiadomości oraz korzystać z czatów. W pokojach czatowych dzieci szukają ciepła, towarzystwa i wygody, których nie znajdują w rodzinie. Jednak nie ma czatu bez drapieżnika, który

będzie próbował wykorzystać niewinność młodzieży. Niestety, drapieżniki, udając nastolatków, korzystają z czatów, serwisów społecznościowych i innych witryn komunikacji online, aby przyciągać i wykorzystywać dzieci. Zaskakujące jest to, że drapieżnikami są zwykle ludzie podejrzani, społecznie szanowani, wykształceni - naukowcy, nauczyciele, przedsiębiorcy i tak często wybitni, zamożni ekonomicznie i zwykle mający własną rodzinę. Takie osoby rozpoczynają rozmowy z potencjalnymi ofiarami dzieci w celu nawiązania przyjaznego związku i uzyskania jak największej ilości informacji o ich życiu osobistym - miejscu zamieszkania, zainteresowaniach, hobby itp. Dyskusje mogą trwać kilka dni, tygodni, a nawet miesięcy, do drapieżnik zyskuje zaufanie dziecka. Następnie drapieżnik powoli angażuje się w rozmowy w nadziei, że doprowadzą do znęcania się nad dzieckiem-ofiarą.

Trendy w cyberprzestępczości

Cybernękanie

Są to działania, które mają miejsce przez Internet i mają na celu zastraszenie i poniżenie osoby od jednej lub więcej osób. Cybernękanie zwykle występuje wśród nieletnich, odbywa się za pośrednictwem wszystkich nowoczesnych mediów komunikacji internetowej - e-maili, mediów społecznościowych, czatu, wiadomości błyskawiczne itp. Zasadniczo jest to mutacja tradycyjnego szykanowania. Niestety, wersja cybernetyczna przeżywa ostatnio światowy wzrost, a incydenty mają miejsce głównie w środowiskach szkolnych. Cybernękanie może przybierać różne formy, z których większość jest następująca:

• Wysyłanie SMS-ów, wiadomości e-mail lub komunikatorów internetowych z obraźliwymi treściami (w komunikatorach internetowych lub na czatach)

• Złośliwe publikowanie zdjęć w serwisach społecznościowych, blogach lub innych witrynach wyłącznie w celu nękania

• Rozpowszechnianie plotek i fałszywych faktów w celu

zniesławianie osób trzecich w mediach społecznościowych, blogach, witrynach internetowych itp.

• Anonimowe zastraszające rozmowy i wiadomości.

Cybernękanie nie powinno być postrzegane jako niewinny żart dzieci, ale jako poważny negatywny wpływ na życie dziecka. Takie konsekwencje, które powinny ostrzec rodziców i nauczycieli obejmują

• Nieobecność w szkole

• Nagły spadek wyników w nauce

• Wykonanie czynu niezgodnego z poprzednim zachowaniem

• Zaangażowanie w działania niezgodne z prawem

• Chęć dziecka do zmiany własnego imienia

• depresja psychiczna

• Myśli lub próby samobójcze.

Przypadek dziesiąty: w szkole podstawowej uczennica pierwszej klasy, A, była zastraszana przez kolegę z klasy, B, który groził opublikowaniem w Internecie nagiego zdjęcia ucznia A. Poważnie wpłynęło to na wyniki akademickie ofiary, przyciągając uwagę władz szkolnych, które zbadały incydent i odpowiednio ukarały ucznia B.

Badanie przeprowadzone przez organizację non-profit N.EO.I na próbie 422 dzieci w wieku 13–18 lat (275 chłopców i 147 dziewcząt) wykazało, że:

• 16% chłopców i 22% dziewcząt w wieku 13–18 lat twierdziło, że padło ofiarą cybernękania.

• 32% twierdziło, że zastraszyło ich publikacja osobistych zdjęć w Internecie.

• 10% chłopców odpowiedziało pozytywnie na pytanie, czy byli zastraszani przez kolegę z klasy, przyjaciela lub znajomego za pośrednictwem Internetu lub innych nowych technologii.

• 42% odpowiedziało, że wie lub słyszało o kimś, kto padł ofiarą prześladowania przez Internet i / lub nowe technologie.

Chociaż powyższe statystyki odzwierciedlają środowisko młodzieżowe Grecji, gdzie te dane były dostępne, światowa rzeczywistość jest znacznie gorsza.

Samobójstwa i zaginięcia

Ogólny niepokój związany z rolą Internetu w życiu jego użytkowników wynika z przypadków samobójczych, w których Internet działał jako czynnik. Typowe przypadki to samobójstwa związane z uzależnieniami od hazardu online.

Przypadek jedenasty: W Grecji znaleziono 18-letniego studenta martwego obok jego komputer, gdy komputer był online na czacie. Na ekranie w e-mailu znajdował się przepis na śmierć od osoby o imieniu żeńskim, który zawierał szczegółowe instrukcje na temat tego, jakiego leku użyć, aby zakończyć życie.

Na szczęście istnieje całodobowy internetowy czat służący zapobieganiu samobójstwom, który w ostatnich latach najwyraźniej zapobiegł ponad tysiącowi możliwych samobójstw. Warto wspomnieć, że dzięki Internetowi i pozostawionym śladom rozwiązano liczne przypadki zniknięć.

Wniosek

W ostatnich dziesięcioleciach technologia poczyniła duże postępy, wprowadzając nowe urządzenia, nowe techniki i nowe funkcje. Do tej pory komputery i Internet stały się integralną częścią naszego codziennego życia, ulepszyły nasze życie w nieskończony sposób i sprawiły, że nasze działania były znacznie szybsze i łatwiejsze. To samo dotyczy działań przestępczych - stały się one znacznie szybsze i łatwiejsze. Ponieważ Internet stał się cenną i niezbędną częścią naszego codziennego życia, błędem byłoby demonizowanie go pod pretekstem, że ułatwia on działania przestępcze. Dzięki szkoleniom uświadamiającym w zakresie cyberbezpieczeństwa możemy chronić się przed pułapkami kryminalnymi i być dodatkowymi podejrzliwy wobec wspaniałych ofert. Faktem jest, że uniknęlibyśmy wielu hacków internetowych, gdybyśmy wiedzieli kilka podstawowych rzeczy na temat korzystania z nich. Na zakończenie nawigacja w zakresie bezpieczeństwa cybernetycznego jest jak nawigacja na otwartym morzu, gdzie wymagane są specjalistyczne umiejętności. Podobnie wszyscy musimy przeprowadzić pewną formę szkolenia w zakresie cyberbezpieczeństwa, aby mieć bezpieczną i przyjemną nawigację w sieci.