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