Co to jest polityka bezpieczeństwa informacji?

Czwartek, 2 marzec 2017, 11:14, autor: Fakturowo.pl

W obecnych czasach coraz więcej firm, niezależnie od swej wielkości, wykorzystuje Internet do celów marketingowo – komunikacyjnych. Bardzo ważnym elementem w zarządzaniu i projektowaniu sieci teleinformatycznych jest stworzenie zespołu reguł, które definiowałyby zasady dostępu do zasobów gromadzonych i przetwarzanych przez systemy informatyczne. Nawet najlepsze oprogramowanie czy sprzęt nie zabezpieczą naszych zasobów, jeśli nie będzie przestrzeganych kilka podstawowych zasad przy ich wykorzystaniu. Dokument regulujący tego rodzaju aspekty nazywany jest polityką bezpieczeństwa. Ze względu na wagę podejmowanych tematów, dokument ten ma najczęściej rangę oficjalnego wewnętrznego regulaminu zatwierdzonego przez zarząd firmy.

Politykę bezpieczeństwa organizacji pod wieloma względami moglibyśmy porównać do polityki obronnej państwa. Polityka obronna państwa, zawiera informacje o zagrożeniach dla bezpieczeństwa kraju. Natomiast polityka bezpieczeństwa zawiera różnego rodzaju procedury mające na celu zapewnienie bezpieczeństwa (informatycznego i nie tylko) firmy. Określaniem polityki obronnej państwa zajmują się jego władze (rząd, prezydent, parlament). Z kolei określaniem polityki bezpieczeństwa, zajmuje się zarząd organizacji w współpracy z administratorami systemu informatycznego. Przestrzeganie zasad zawartych w polityce bezpieczeństwa wymagane jest przez wszystkie zatrudnione w firmie osoby, gdyż to głównie od nich zależy, w jakim stopniu będą chronione informacje niezbędne w realizacji podstawowych zadań instytucji (klienci, obroty, wynik finansowy i tym podobne). Widzimy zatem, że poprawnie skonstruowana i przestrzegana polityka bezpieczeństwa, to inwestycja w ochronę wszelkiej informacji niejawnej, której naruszenie mogłoby godzić bezpośrednio w finanse firmy lub dobre imię firmy.

Model polityki bezpieczeństwa będzie w dużej mierze zależał od potrzeb organizacji. Każda firma ma inne wymagania i potrzeby w odniesieniu do pojęcia bezpieczeństwa. Związane jest to z różnymi kombinacjami sprzętu i oprogramowania oraz z różnymi celami i skalą zabezpieczania. Właśnie dlatego polityka bezpieczeństwa będzie indywidualna dla każdej firmy i dlatego nie ma uniwersalnego schematu zabezpieczeń. Jeżeli mamy do czynienia z małą firmą, która wykorzystuje Internet do publikacji na swoim serwerze ogólnodostępnych materiałów marketingowych oraz wysyła i odbiera pocztę elektroniczną o małym stopniu poufności, to dbając o wykonywanie kopii bezpieczeństwa oprogramowania serwera oraz odcinając od sieci komputery zawierające poufne informacje uzyskamy wystarczający poziom zabezpieczeń. W innym zaś przypadku przyglądając się sklepowi internetowemu stwierdzamy, że wszystkie jego serwisy oparte są na interfejsie serwera WWW i to właśnie na serwerze należy skoncentrować uwagę w procesie oceny bezpieczeństwa.

Przy tworzeniu polityki bezpieczeństwa powinna być zachowana odpowiednia kolejność postępowania. Należy zaplanować kroki, jakie będą niezbędne w celu usprawnienia i uwiarygodnienia podjętych działań. Pierwszym krokiem w procesie tworzenia polityki bezpieczeństwa jest przeprowadzenie oceny funkcjonalnej firmy.. W ocenie takiej powinny się znaleźć wszystkich istotne informacje, dzięki którym możliwe będzie stworzenie polityki bezpieczeństwa. Zatem między innymi będą to informacje: o firmie, o jej działalności, o procesach w niej zachodzących, a także o współpracy pomiędzy określonymi działami. Po fazie oceny i zebraniu odpowiednich informacji, doszliśmy do etapu tworzenia polityki bezpieczeństwa. Polityka bezpieczeństwa określa zasoby, które powinny być zabezpieczone, ale nie wskazuje na zastosowanie konkretnych metod. Dokument taki może mówić na przykład o konieczności szyfrowania informacji, ale nie wskaże on jakiej konkretnie metody szyfrowania powinniśmy w tym celu użyć. Powodem takiego stanu rzeczy jest fakt, że w momencie zmiany przez firmę stosowanej technologii całą polityką także należałoby zmieniać. Jeżeli na przykład, w stosowanym przez firmę algorytmie szyfrującym odkryte zostałyby jakieś wady, które umożliwiłby jego złamanie, wówczas polityka bezpieczeństwa takiej firmy, odnosząca się do metod szyfrowania byłaby bezużyteczna. Właśnie dzięki temu, że polityka bezpieczeństwa jest w pewnym stopniu "ogólna", pozostawia ona szczegóły dotyczące stosowania konkretnych rozwiązań, w rękach tych, którzy będą bezpośrednio odpowiedzialni za działanie systemu zabezpieczeń. Dzięki tej właściwości polityki bezpieczeństwa, nieodpowiednie rozwiązania nie będą narzucane z góry przez osoby, które nie mają praktycznego doświadczenia w kwestiach bezpieczeństwa (jest to ważne, bo często osoby tworzące taki dokument, zagadnienia bezpieczeństwa znają tylko teoretycznie). Polityka bezpieczeństwa jest przeważnie dokumentem wielostronicowym i w praktyce wielu pracownikom, do których jest ona

skierowana, nie będzie chciało się jej czytać (jak już wcześniej pisałem, przestrzeganie polityki bezpieczeństwa przez pracowników jest jednym z najważniejszych elementów w całym procesie zapewniania bezpieczeństwa). Praktycznym rozwiązaniem tego problemu, stosowanym przez wiele instytucji jest tworzenie, pewnego dokumentu na kształt wzorca polityki bezpieczeństwa, w którym zamieszczone są pewne obszary odpowiedzialności. Następnie na podstawie takich wzorców tworzona jest bardziej zwięzła forma dokumentu, która jest specjalnie przystosowana i przeznaczona dla wybranych grup: kierowników, przeciętnych pracowników czy pracowników działu informatycznego. Takie właśnie rozwiązania sprawdzają się najlepiej. Kolejnym ważnym elementem w procesie tworzenia polityki bezpieczeństwa jest tworzenie procedur i dokumentów operacyjnych. Ten element polityki bezpieczeństwa wskazuje już określone procesy, systemy i implementacje, które powinny być użyte. Przykładowo może wskazywać on metody archiwizacji danych i częstotliwość z jaką archiwizacja taka powinna być przeprowadzana. Kolejnym etapem jest ocena techniczna. Na tym etapie dokonywane są testy penetracyjne, które pokazują, czy system poradzi sobie z atakami dokonywanymi od wewnątrz lub z zewnątrz sieci. Celem takich testów jest sprawdzenie istniejącej infrastruktury przedsiębiorstwa i ustalenia tego, co w chwili obecnej sprawia największe zagrożenie i co należy poprawić w pierwszej kolejności. Taki test również istniejącą politykę bezpieczeństwa, a także jej przestrzeganie przez pracowników organizacji. Konieczne jest więc powołanie zespołu którego zadaniem będzie identyfikacja i wskazanie obszarów zagrożeń. Zespół taki (złożony przeważnie ze specjalistów do spraw bezpieczeństwa) symuluje ataki, jakby były one przeprowadzane przez hakerów, czyli wykorzystuje wszystkie dostępne środki, by osiągnąć cel.

Zatem działania takie nie koncentrują się tylko na aspektach technicznych, czasami wykorzystywane są również metody inżynierii społecznej (tak zwany social engineering). W metodzie tej wykorzystuje się pozatechniczne środki do uzyskania dostępu do informacji lub systemów informatycznych. Zamiast wykorzystywać słabe punkty zabezpieczeń czy skomplikowane programy, można posłużyć się naturą ludzką. Mając miły głos czy umiejąc dobrze kłamać również można wiele osiągnąć (chodzi mi oczywiście o dostęp do systemów informatycznych). Można na przykład udawać pracownika, zadzwonić do serwisu informatycznego i poprosić o hasło w celu "naprawienia drobnej usterki w systemie pracownika". Wiele takich przypadków kończyło się sukcesem.

Wracając do tematu, w poszukiwaniu słabych punktów pierwszym wykonywanym testem jest skanowanie sieci. Tego rodzaju testy wykonywane są przy użyciu zautomatyzowanych narzędzi, które skanują komputery znajdujące się w sieci lokalnej. Celem takiego testu jest sprawdzenie zabezpieczeń pod kątem znanych luk programowych lub systemowych (przy pomocy takich programów znajdziemy na przykład komputery, w których nie zainstalowano niezbędnych pakietów Service Pack lub uaktualnień). Na podstawie wyników uzyskanych z testów, przygotowane są specjalne raporty, które zawierają informację o zaobserwowanych nieprawidłowościach.

Kolejny rodzaj testów penetracyjnych jest już bardziej zaawansowany. Tego typu testy wykonywane są przeważnie przez firmy, które profesjonalnie zajmują się zapewnianiem i oceną stanu bezpieczeństwa. Do testów wykorzystywane są komercyjne skanery zabezpieczeń lub specjalistyczne narzędzia, tworzone właśnie przez te firmy. Testy pozwalają sprawdzić możliwości dalszej penetracji systemu po włamaniu się do niego, reakcje administratorów na próby włamania czy poprawności działania systemów wykrywania włamań. W ramach przeprowadzanych testów sprawdzana jest również odporność na ataki między innymi systemów firewall. Testy takie, mają za zadanie sprawdzić poprawność konfiguracji systemu firewall oraz jego odporność na ataki z Internetu. Sprawdzane jest również, czy przypadkiem na zewnątrz nie wydostają się informacje o strukturze chronionej sieci (na przykład informacje o adresach wewnętrznych), które ułatwiłyby działanie włamywaczom. Za pomocą testów penetracyjnych sprawdzane są również serwery stron WWW, które w obecnych czasach posiada każda większa firma czy instytucja. Zadaniem testu jest wykrycie podatności serwera WWW na znane ataki oraz sprawdzenie poziomu jego zabezpieczeń przed kradzieżą bądź modyfikacją zawartych w nim danych.

Jednak należy pamiętać, że narzędzia wykorzystywane w takich testach, nie są doskonałe i mogą być jedynie jednym z elementów pomocnych w badaniu zabezpieczeń. Na przykład jedną z wad skanerów sprawdzających zabezpieczenia jest to, że są one uaktualniane co pewien czas, a zatem nie mogą odkryć najnowszych luk czy słabości testowanego systemów. Niestety nie wszyscy o tym pamiętają, w rezultacie wiele przedsiębiorstw polega wyłącznie na tego rodzaju testach i nie wykonuje dodatkowych szczegółowych badań zabezpieczeń systemu.

W dzisiejszych czasach proces zapewniania bezpieczeństwa nie jest jednorazowym wydarzeniem, nie wystarczy zakupić i skonfigurować odpowiedni system firewall. Bezpieczeństwo zależy nie tylko od zastosowanych, często bardzo drogich i wyrafinowanych technologii, ale przede wszystkim od świadomości całego personelu firmy. Często zastosowanie podstawowych zasad bezpieczeństwa wystarcza dla spełnienia założeń polityki bezpieczeństwa.