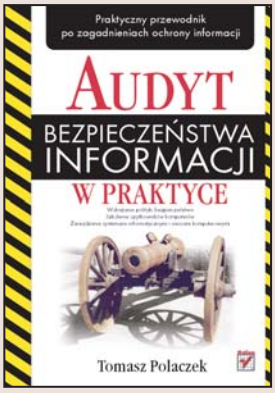
Audyt bezpieczenstwa informacji w praktyce

Autor: Tomasz Polaczek
ISBN: 83-246-0402-2
Format: B5, stron: około 126



Rozpoczęła się era społeczeństwa informacyjnego. Działalność coraz większej liczby organizacji i firm zależy od szybkiego i efektywnego przetwarzania informacji. Informacja stała się cennym, często wykradanym towarem. Zagrożeniem dla bezpieczeństwa danych są nie tylko crackerzy, lecz często także pracownicy firmy, którzy nieświadomie udostępniają zastrzeżone informacje osobom trzecim. Upowszechnienie informacji, będących tajemnicą lub własnością intelektualną i handlową firmy lub instytucji, może oznaczać utratę reputacji, zakończenie działalności na rynku lub nawet wywołać kłopoty natury prawnej. Z tych powodów informację trzeba należycie chronić oraz odpowiednią nią zarządzać.

Książka „Audyt bezpieczeństwa informacji w praktyce" przedstawia praktyczne aspekty wdrażania i realizowania polityki ochrony danych. Opisuje zarówno regulacje prawne, jak i normy ISO traktujące o bezpieczeństwie informacji. Zawiera informacje o odpowiednim zarządzaniu systemami przechowywania danych, fizycznym zabezpieczaniu miejsc, w których znajdują się nośniki danych, oraz szkoleniu użytkowników systemów.

- Normy ISO i PN dotyczące ochrony informacji
- Planowanie polityki bezpieczeństwa
- Umowy o zachowaniu poufności
- Zabezpieczanie budynku i pomieszczeń
- Tworzenie procedur eksploatacji sprzętu i systemów
- Ochrona sieci przed programami szpiegującymi
- Zarządzanie dostępem użytkowników do systemu

Odpowiednio zaplanowane procedury ochrony danych mogą uchronić przedsiębiorstwo przed poważnymi problemami. Wykorzystaj wiadomości zawarte w tej książce i wprowadź podobne procedury w swojej firmie.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

6

Zarządzanie systemami informatycznymi i sieciami komputerowymi

Sieci komputerowe, a właściwie wszelakie systemy informatyczne, stały się już niezbędne zarówno przy wykonywaniu czynności służbowych, jak również w życiu prywatnym. W rzeczywistości bez tego dobrodziejstwa techniki trudno się obyć. Przykładowo, coraz częściej sieci komputerowe służą do dokonywania zakupów. Siecią przesyła się wszelakie informacje i dane — te ważne i te mniej istotne. Systemy informatyczne z kolei dane te przetwarzają i przechowują. Oczywistym jest, że aby służyły one w należyty — i przede wszystkim — w bezpieczny sposób, trzeba zapewnić ich odpowiednią obsługę i poprawnie zarządzać nimi.

Bardzo istotnym elementem systemu bezpieczeństwa informacji jest staranne zabezpieczenie sieci komputerowych i systemów informatycznych przed osobami niepowołanymi. W tym celu — podobnie jak w przypadku innych systemów — trzeba wprowadzić odpowiednie procedury eksploatacyjne.

Procedury eksploatacyjne oraz okres odpowiedzialności

Informacja jest wykorzystywana za pomocą różnego typu urządzeń. Skoro tak się dzieje, oznacza to również konieczność zabezpieczenia tych urządzeń. W tym przypadku oczywistą sprawą jest sprecyzowanie odpowiednich procedur zarządzania tymi urządzeniami oraz zakresów odpowiedzialności za te

urządzenia oraz informacje w nich przechowywane lub przetwarzane. Należy również wdrożyć procedury reagowania na incydenty związane z uszkodzeniem takich urządzeń bądź niewłaściwym ich użytkowaniem, co może się przyczynić do uszkodzenia sprzętu lub utraty przechowywanych danych.

Dokumentowanie procedur eksploatacyjnych

Procedury zawarte w polityce bezpieczeństwa informacji powinny być ogólnodostępne dla wszystkich osób w organizacji — jest to warunek sprawnego funkcjonowania całego systemu. Jak wspomniałem we wcześniejszych rozdziałach tej książki, poszczególne procedury powinny być opracowane w sposób ściśle odpowiadający specyfice pracy na danych stanowiskach, jednak istnieją jeszcze procedury ogólnodostępne, skierowane do wszystkich pracowników organizacji. Istnieje przecież wiele urządzeń, wykorzystywanych przez praktycznie wszystkie osoby w firmie do przeglądania, przesyłania, przechowywania czy przetwarzania informacji. Sposób posługiwania się tym sprzętem i zasady ochrony informacji z nim związanej powinny zatem zostać precyzyjnie określone w odpowiednich procedurach. Do takich procedur należą właśnie m.in. procedury eksploatacyjne. Oczywiście, należy je odpowiednio dokumentować i przechowywać. Każda z tych procedur powinna zawierać dokładną instrukcję postępowania z określonymi urządzeniami oraz z informacją w nich zawartą lub przetwarzaną.

Podczas codziennej pracy bardzo często dochodzi do incydentów, które potencjalnie mają wpływ na jakość pracy lub na bezpieczeństwo przetwarzanych danych. Oczywiście, te zdarzenia są spowodowane różnymi przyczynami, np. błędnym działaniem aplikacji lub niepoprawną pracą systemu informatycznego. W takich przypadkach, gdy praca zostanie zakłócona przez np. źle działający system informatyczny, procedury powinny mówić m.in. o obsłudze technicznej i sposobie uzyskania pomocy działu lub firmy zajmującej się utrzymaniem bądź serwisem struktur informatycznych. Poza tym należy również udokumentować procedury ponownego uruchomienia systemu bądź jego odtworzenia w przypadku awarii.

Kontrola zmian w eksploatacji

W przypadku każdego systemu informatycznego na porządku dziennym jest dokonywanie zmian, aktualizacji zabezpieczeń lub innych czynności związanych z podniesieniem wydajności działania sprzętu i oprogramowania. Wszystkie tego typu zmiany powinny być starannie dokumentowane, co ułatwia zapobieganie awariom systemu lub przynajmniej pozwala na odpowiednio szybkie zdiagnozowanie przyczyn jego uszkodzenia. Każda zmiana czy aktualizacja

jest przeprowadzana ze względu na konieczność lub chęć usprawnienia całego systemu czy aplikacji, ale nie zawsze zamierzony cel jest osiągany. Dlatego też w dokumentacji odnoszącej się do dokonywanych zmian, powinny znaleźć się informacje o ewentualnych następstwach danej modyfikacji lub zmiany. Trzeba również uzyskać pisemnie potwierdzone pozwolenie od kierownika działu lub od upoważnionego członka kierownictwa organizacji na dokonanie tego typu czynności. Ponadto należy zdefiniować procedury przywracania systemu do pierwotnego stanu w przypadku problemów występujących w efekcie tego typu zmian.

Procedury zarządzania incydentami związanymi z bezpieczeństwem

Jeśli w organizacji dojdzie do jakiegoś incydentu związanego z naruszeniem prawidłowego funkcjonowania systemu lub zdarzenia mającego bezpośredni wpływ na bezpieczeństwo informacji, należy zastosować wcześniej przygotowane, odpowiednie procedury, które zapewnią szybką reakcję. Przykładem takiego incydentu w przypadku systemów informatycznych są ataki typu DoS (*Denial of Service*), co można przetłumaczyć jako odmowa obsługi. Tego typu ataki na systemy informatyczne powtarzają się coraz częściej. Często również mówi się o błędach w oprogramowaniu, które umożliwiają prowadzenie ataków typu DoS. Dobrze przeprowadzony atak na sieć informatyczną może spowodować jej całkowity paraliż, trwający nawet kilka dni lub tygodni w przypadku rzeczywiście rozległych sieci. Ataki te mają również bezpośredni wpływ na bezpieczeństwo przechowywanych danych. Oczywiście, istnieją techniki zabezpieczania się przed atakami, ale nigdy nie są one w stu procentach skuteczne.

Organizacja powinna przygotować i wdrożyć odpowiednie procedury, które obejmują wszystkie takie potencjalne incydenty, mające wpływ na utratę dostępności, poufności i integralności przechowywanych informacji. Procedury te powinny również uwzględnić plan działania, w tym sporządzenie niezbędnych analiz związanych z rozpoznaniem natury incydentu oraz jego przyczyn. Trzeba również umieć zaplanować i wdrożyć odpowiednie środki zaradcze, aby ograniczyć do minimum możliwość pojawienia się podobnego zdarzenia w przyszłości (warto podkreślić, że nie zawsze można zabezpieczyć system w całkowicie skuteczny sposób).

Następną czynnością jest zebranie wszelkich informacji bądź śladów związanych z zaistniałym incydentem. Ma to na celu zminimalizowanie prawdopodobieństwa wystąpienia podobnego zdarzenia w przyszłości oraz ewentualne wykrycie sprawcy lub przyczyny zaistnienia incydentu.

W przypadku stwierdzenia, że źródłem incydentu było niewłaściwe zarządzanie systemem bądź dostęp osoby nieuprawnionej do określonej jego części, należy wdrożyć bardziej restrykcyjne procedury dostępowe. Przykładowo, każdorazowe uzyskanie dostępu lub praca przy systemie powinny podlegać starannej rejestracji. Oczywiście, można by tu przytoczyć o wiele więcej potencjalnych sposobów dokładniejszego zabezpieczenia przechowywanych informacji, jednak byłoby to niecelowe, gdyż większość z nich wiąże się ze specyfiką działania organizacji oraz innych czynników.

Podział obowiązków

Mówiąc o naruszeniach bezpieczeństwa danych, o utracie poufności, dostępności i integralności chronionej informacji, w większości przypadkach opisuje się zamierzone ataki, spowodowane czy to zemstą zwolnionych pracowników, czy też chęcią uzyskania profitów finansowych bądź innych, przykładowo, wynikających z przekazania informacji konkurencji. Mimo to poza tymi wszystkimi przypadkami, częstą przyczyną incydentów jest również zwykła ludzka nieuwaga lub pomyłka.

Niezależnie od powyższego, ważną częścią polityki bezpieczeństwa informacji jest wprowadzenie podziału obowiązków, gdyż to jest dobra metoda zminimalizowania ryzyka zaistnienia incydentu bądź wystąpienia pomyłek.

Jednym z istotnych zaleceń jest zwracanie większej uwagi na pojedyncze zdarzenia, wynikające z błędów jednej osoby. Nawet niewielkie pomyłki mogą mieć duży wpływ na szereg zdarzeń, których konsekwencją może być, przykładowo, utrata danych.

Oczywiście, nie można wykluczyć zmowy grupy pracowników. Zmowa taka może spowodować utratę chronionej informacji lub duże straty finansowe. Aby zapobiec takim zdarzeniom, należy bardziej rozgraniczyć obowiązki pracowników poszczególnych grup, np. działu zajmującego się wysyłką towaru, działu finansowego itd.

Oddzielenie urządzeń produkcyjnych od znajdujących się w fazie rozwoju

Niektóre organizacje doskonalą swoje systemy informatyczne w celu zwiększenia ich wydajności bądź też zwiększenia swojej konkurencyjności. Jeśli w jednostce funkcjonują działy zajmujące się badaniami rozwojowymi, to ich sprzęt, oprogramowanie, a nawet cała sieć komputerowa powinny zostać

odizolowane od pozostałej infrastruktury informatycznej. Jeśli takie rozgraniczenie nie zostanie wykonane, konsekwencją tego stanu rzeczy mogą być poważne komplikacje w pracy oprogramowania, systemu lub nawet całej infrastruktury.

Celom badawczym powinny służyć osobne domeny lub poddomeny, które zostaną starannie zabezpieczone i oddzielone od pozostałych systemów, niewykorzystywanych podczas badań. W ten sposób można uchronić się przed nieprzewidzianymi sytuacjami, które mogą ujemnie wpływać na funkcjonalność całego systemu.

Zarządzanie urządzeniami przez firmy zewnętrzne

Ostatnimi czasy zlecanie usług informatycznych firmom zewnętrznym stało się częstą praktyką. Jest to dobry sposób zmniejszania kosztów oraz odpowiedzialności związanych z utrzymaniem własnego systemu informatycznego. Firma, która zleciła obsługę informatyczną innemu przedsiębiorstwu, nie musi się martwić o awarie, zabezpieczenia przed wirusami, krakerami oraz o naprawę i wdrażanie sprzętu i oprogramowania. Jest to wygodna forma pracy, lecz również niebezpieczna, jeśli chodzi o zachowanie poufności, dostępności i integralności chronionych informacji. Zlecanie obsługi informatycznej zewnętrznej firmie stanowi potencjalnie duże ryzyko, przed którym trzeba się należycie zabezpieczyć. Oczywiście, jednym z możliwych zabezpieczeń jest starannie sporządzona umowa między firmami, ale umowa nie daje stuprocentowej pewności bezpieczeństwa chronionych danych ani nie zagwarantuje uczciwości strony pracowników firmy świadczącej usługę. Dlatego też należy m.in. zdefiniować czynności, które mogą i powinny być wykonywane przez pracowników organizacji, który sprzęt powinien być serwisowany w firmie, a jaki może zostać przeniesiony poza siedzibę jednostki. Oczywiście, przedstawiciele firmy zewnętrznej, tacy jak serwisanci, inżynierowie systemowi oraz inne osoby wchodzące w skład obsługi technicznej, powinni zostać zapoznani z obowiązującymi procedurami bezpieczeństwa informacji. Należy też opracować i wdrożyć procedury zgłaszania oraz przyjmowania zgłoszeń przez pracowników.

Planowanie i odbiór systemu

Aby zminimalizować ryzyko awarii systemów informatycznych, należy zaplanować oraz zapewnić odpowiednie zasoby sprzętowe (np. niezbędną przestrzeń dyskową). Oczywistą sprawą jest możliwość przeciążenia systemów informatycznych, sieci oraz urządzeń przechowujących i przetwarzających dane.

Aby uniknąć takich incydentów, należy dobrze sprecyzować potrzeby firmy w zakresie potrzeb sprzętowych: liczby, rodzaju i wielkości dysków twardych, liczby serwerów, szybkości sieci komputerowej. Przemyślane zaplanowanie konfiguracji sprzętowej pozwoli na zminimalizowanie ryzyka wystąpienia awarii i częściowej lub całkowitej utraty chronionej informacji.

Należy też pamiętać, że w przypadku wprowadzania dodatkowych usprawnień, takich jak nowe urządzenia, aplikacje czy nawet rozbudowa sieci komputerowej, przed ich wdrożeniem należy dokładnie przetestować każdą z tych modyfikacji.

Planowanie pojemności

Jak już wcześniej wspomniałem, aby móc dobrze zaplanować konfigurację sprzętową systemu informatycznego, trzeba dokładnie znać wymagania organizacji dotyczące przechowywania danych. W przypadku funkcjonujących systemów informatycznych jest konieczne bieżące monitorowanie zwiększającej się ilości przechowywanych danych, aby w odpowiednim czasie móc zwiększyć dostępną przestrzeń dyskową bądź inne niezbędne zasoby sprzętowe. Niedopełnienie tych zadań może spowodować przeciążenie systemu, a w konsekwencji — jego zatrzymanie bądź nawet uszkodzenie.

Istotną kwestią jest zaznajomienie się kierownictwa organizacji z podstawowymi zagadnieniami dotyczącymi potrzeb sprzętowych, aby w odpowiednim czasie zapewniono rozbudowę systemu informatycznego w niezbędnym zakresie.

Odbiór systemu

Przed przekazaniem systemu informatycznego do eksploatacji po jego utworzeniu bądź po wykonaniu napraw czy aktualizacji należy przeprowadzić odpowiednie testy, co pozwoli na uniknięcie poważniejszych skutków ewentualnej awarii. Zanim system zostanie włączony do całej infrastruktury informatycznej, należy spełnić pewne warunki i wykonać dodatkowe czynności. Obostrzenia te powinny odpowiadać istotności informacji przechowywanej i przetwarzanej w tym systemie. Warunki przekazania do eksploatacji zmodyfikowanej części systemu informatycznego należy określić na etapie planowania systemu bezpieczeństwa informacji. Trzeba się tu odnieść m.in. do takich zagadnień jak:

- sposoby ponownego rozruchu systemu;
- opisanie wszystkich wdrożonych zabezpieczeń;

- potwierdzenie zgodności nowego systemu z całą infrastrukturą informatyczną;
- szkolenia kadry technicznej i pracowników z użytkowania nowego systemu;
- pozostałe czynniki, wynikające ze specyfiki działalności organizacji bądź potrzeb samego systemu.

Wprowadzenie nowego systemu bądź modyfikacja istniejącego wiąże się również z przeprowadzeniem rozeznania wśród pracowników szczebla administracyjnego oraz obsługi technicznej. Celem tego rozeznania jest zebranie informacji dotyczących samego systemu, czy spełnia on wymagania użytkowników, czy jest łatwy w obsłudze, czy też nie trzeba czegoś zmienić bądź poprawić. Są to ważne informacje, ponieważ system skomplikowany, trudny w obsłudze i niespełniający oczekiwań użytkowników jest z zasady systemem niebezpiecznym. Należy stale mieć na uwadze, że niewiedza osób korzystających z systemu może doprowadzić do nieumyślnego uszkodzenia lub utraty danych.

Ochrona przed szkodliwym oprogramowaniem

W dobie powszechnego wykorzystywania internetu największym zagrożeniem dla systemów informatycznych jest szkodliwe oprogramowanie. Pod tym terminem należy rozumieć oczywiście wszelkiego rodzaju wirusy komputerowe, robaki internetowe, konie trojańskie oraz inne złośliwe programy-skrypty. Złośliwe oprogramowanie może nawet zniszczyć system informatyczny czy dane. Coraz to nowsze generacje złośliwego oprogramowania powodują problemy różnego typu. Twórcy takich programów wkładają wiele wysiłku, by ich zachowanie było coraz bardziej inteligentne. Znane są już takie wirusy czy robaki, które są zdolne do reprodukowania się lub też do samoistnego zmieniania swojej postaci, dzięki czemu są coraz trudniejsze do unieszkodliwienia. Znane są przypadki, gdy infekcja wirusowa przyczyniła się do zatrzymania pracy dużych korporacji na wiele dni lub nawet tygodni, mimo że owe przedsiębiorstwa uchodziły za organizacje dobrze zabezpieczające się przed tego typu atakami. Z tego wynika, że złośliwe oprogramowanie coraz częściej jest w stanie rozprzestrzeniać się mimo coraz doskonalszych mechanizmów antywirusowych. Sprawa jest bardzo poważna, gdyż prawdopodobieństwo, że infekcja wirusem może doprowadzić nie tylko do poważnych strat finansowych, ale także do upadku całej firmy, jest znaczące. Oczywiste jest, że organizacje starają się zabezpieczyć przed podobnymi zdarzeniami, nawet kosztem ogromnych środków finansowych. Wyspecjalizowane przedsiębiorstwa opracowują coraz bardziej wyrafinowane — i często bardzo kosztowne — mechanizmy zabezpieczające przed atakami złośliwego oprogramowania, podczas gdy liczni twórcy takich programów piszą coraz to nowsze

ich odmiany, które coraz sprawniej pokonują coraz to nowsze zabezpieczenia. I tak koło się zamyka — ten swoisty „wyścig zbrojeń" trwa. Obecnie stuprocentowe wyeliminowanie plagi złośliwego oprogramowania jest niemożliwe i zapewne taki stan rzeczy jeszcze potrwa jakiś czas. Wirusy oraz inne szkodliwe oprogramowanie trzeba zatem uznać za tzw. *ryzyko akceptowalne*. Termin ten oznacza ryzyko, którego nie można całkowicie wyeliminować. A skoro nie można go wyeliminować, trzeba się przed nim jak najlepiej zabezpieczyć, aby je zminimalizować.

Przede wszystkim trzeba wdrożyć mechanizm wykrywania wirusów i względnie szybko reagować na ich działanie. Wykrywalność złośliwego oprogramowania zwiększy się na pewno, jeśli personel techniczny będzie na bieżąco prowadził monitoring nie tylko zachowania systemów, ale również gdy będzie śledził najnowsze informacje ze świata na temat powstających wirusów.

Zabezpieczenie przed szkodliwym oprogramowaniem

Aby odpowiednio zabezpieczyć się przed wirusami komputerowymi oraz innym szkodliwym oprogramowaniem, należy wprowadzić szereg usprawnień, procedur oraz odpowiednio przeszkolić i uświadomić użytkowników systemów informatycznych w tym zakresie.

Przede wszystkim polityka bezpieczeństwa informacji powinna jasno określać, kto ma dostęp do poszczególnych elementów systemu, na jakich zasadach i z jakimi uprawnieniami. Należy wystrzegać się przyznawania większości lub nawet wszystkim użytkownikom uprawnień administratora systemu, ponieważ wtedy stanowią oni największe — po internecie — zagrożenie dla całego systemu informatycznego. Jeśli użytkownicy posiadają konta ze wszelkimi możliwymi uprawnieniami, z pewnością będą posługiwali się oprogramowaniem z niepewnych źródeł (takim jak np. różnego rodzaju gry), a to znacząco zwiększa ryzyko nieświadomego zainfekowania komputera wirusami. Jeśli taki komputer jest podłączony do sieci, oznacza to groźbę rozprzestrzenienia się złośliwego oprogramowania.

Oto kilka praktycznych zaleceń, które powinny okazać się przydatne podczas wprowadzenia systemu zabezpieczeń przed złośliwym oprogramowaniem:

- korzystanie tylko z legalnego oprogramowania, ponieważ aplikacje skopiowane nielegalnie mogą zawierać ukryte wirusy, robaki lub konie trojańskie. Poza tym legalne oprogramowanie pozwala na bieżące aktualizowanie systemu, co w przypadku nielegalnych kopii jest niemożliwe;
- wykonywanie na bieżąco aktualizacji wydawanych przez producenta oprogramowania;

- zainstalowanie na serwerach oraz na każdej stacji roboczej oprogramowania antywirusowego oraz innego oprogramowania chroniącego przed np. robakami;
- pilnowanie regularnej aktualizacji baz sygnatur wirusów i innego oprogramowania zabezpieczającego;
- dokonywanie systematycznych przeglądów oprogramowania;
- podczas instalowania nowego oprogramowania należy zawsze skanować pliki instalacyjne w celu sprawdzenia, czy nie zostały zainfekowane;
- przeszkolenie użytkowników w zakresie zasad ochrony przed złośliwym oprogramowaniem (użytkowanie oprogramowania antywirusowego, podstawowe techniki unikania wirusów, takie jak ignorowanie wiadomości e-mail pochodzących z nieznanych źródeł, unikanie odwiedzania pewnych witryn WWW itp.).

To są tylko podstawowe wymagania, które mogą posłużyć jako punkt wyjścia do w miarę skutecznego zabezpieczenia organizacji przed złośliwym oprogramowaniem.

Procedury wewnętrzne

Procedury wewnętrzne, mające na celu zapewnienie sprawnego funkcjonowania systemów informatycznych, mogą być bardzo liczne. W tym podrozdziale przedstawię pewne zasady sporządzania kopii zapasowych, częstotliwości ich wykonywania, ich liczby oraz kwestie weryfikacji gotowych kopii.

Kopie zapasowe ważnych danych

Kopie zapasowe można porównać do polisy ubezpieczeniowej, nieocenionej w przypadku nieprzewidzianych awarii, włamań do systemu informatycznego, utraty informacji, czyichś celowych działań na szkodę organizacji też lub klęsk żywiołowych. Dzięki posiadaniu aktualnych kopii zapasowych można uchronić organizację przed ogromnymi nieraz stratami finansowymi, konsekwencjami prawnymi spowodowanymi utratą pewnych informacji czy też nawet przed upadłością firmy. Niejednokrotnie kopie zapasowe okazywały się ratunkiem dla reputacji jednostki.

Aby uzyskać pewność, że operacje sporządzania kopii zapasowych są należycie przeprowadzane, trzeba spełnić kilka warunków. Przede wszystkim trzeba wskazać odpowiednie miejsce przechowywania kopii zapasowych. Nie powinno