PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2014, t. II, s. 481–489

http://dx.doi.org/10.16926/tiib.2014.02.44

Justyna Żywiołek, Ewa Staniewska
Politechnika Częstochowska
al. Armii Krajowej 19, 42-200 Częstochowa
e-mail: staniew@wip.pcz.pl, j.zywiolek@wip.pcz.pl

ROLA POLITYKI BEZPIECZEŃSTWA INFORMACJI W OCHRONIE DANYCH PRZEDSIĘBIORSTWA

Streszczenie. W artykule przedstawione zostały zasady tworzenia polityki bezpieczeństwa informacji. Uwzględniono zarządzanie bezpieczeństwem informacji w przedsiębiorstwie, co jest podstawą planów bezpieczeństwa IT. Opisane w artykule elementy polityki bezpieczeństwa informacyjnego kompleksowo obrazują elementy niezbędne do zapewnienia bezpieczeństwa informacji w przedsiębiorstwie.
Słowa kluczowe: bezpieczeństwo informacyjne, polityka bezpieczeństwa, ochrona danych.

THE ROLE OF INFORMATION SECURITY POLICY THE DATA PROTECTION COMPANY

Abstract. The article presents the principles of creating an information security policy. Includes management of information security in an enterprise which is the basis of IT security plans. Described in the article information security policy elements comprehensively illustrate the elements necessary to ensure the safety of information in an enterprise.
Keywords: information security, security policy, data protection

Wstęp

W warunkach postępującej digitalizacji, gdy coraz więcej danych dostępnych jest w sieci, konieczność ich ochrony wydaje się oczywistością. Można wyróżnić dwa rodzaje danych wrażliwych, które powinny być w szczególności objęte systemem bezpieczeństwa: dane osobowe oraz wszelkie dane przedsiębiorstwa i klientów, dotyczące zakresu i obszaru działań firmy oraz powiąza-

nych z nią podmiotów. Z jednej strony mamy do czynienia z danymi pracowników, z drugiej zaś – strategicznymi informacjami w przedsiębiorstwie.

Ochrona informacji wymaga spełnienia co najmniej trzech warunków, aby można było mówić o jej skuteczności [1, 2]:

1. wysokiej świadomości pracowników, poczynając od najwyższego kierownictwa;
2. efektywnego zarządzania informacjami w taki sposób, aby zapewnić ich bezpieczeństwo;
3. stworzenia odpowiednich rozwiązań technologicznych, które zapewniają realizację tej polityki.

Zasady polityki bezpieczeństwa informacji

W każdej organizacji znajdują się różnego rodzaju informacje, które powinny podlegać ochronie [3]. Informacje te można podzielić na: strategiczne, do których określa się również zakres dostępu poszczególnych użytkowników, oraz informacje chronione z mocy prawa (głównie dane osobowe oraz tajemnice firmy). Kluczowe w tej sytuacji jest spełnienie trzech podstawowych warunków PBI (polityka bezpieczeństwa informacji) [6]: zachowanie poufności, integralności oraz dostępności informacji. Zachowanie poufności oznacza, że do określonych informacji dostęp mają tylko osoby uprawnione. Natomiast zasada dostępności definiuje czas, kiedy osoby upoważnione mogą korzystać z powyższych informacji. Natomiast przez zasadę integralności rozumie się zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.

Tak więc PBI ujmuje ogólne zasady bezpiecznego wytwarzania, przetwarzania, przesyłania i przechowywania informacji oraz organizację i zarządzanie tym procesem. Z punktu widzenia prawnego podstawą do opracowania PBI będą wszelkie dokumenty wyższego rzędu (ustawy, rozporządzenia) dotyczące ochrony informacji niejawnych, podstawowych wymagań bezpieczeństwa systemów informatycznych i telefonicznych, wspomnianej już wcześniej ochrony danych osobowych i ochrony praw autorskich. Tak więc stworzenie takiej dokumentacji oraz zarządzania procesem bezpieczeństwa wymaga spojrzenia na przedsiębiorstwo z różnych punktów widzenia, w ujęciu całościowym. Kolejnym ważnym czynnikiem opracowania PBI jest odniesienie się do specyfiki organizacji. Jeśli, przykładowo, organizacja ma charakter korporacyjny i funkcjonuje w łańcuchu dostaw, to dochodzi do dość szerokiej wymiany informacji za pomocą systemów teleinformatycznych zarówno wewnątrz korporacji (między ogniwami „sieci korporacyjnej", na ogół znajdującymi się na różnych kontynentach), jak też między „zewnętrznymi" uczestnikami łańcucha dostaw, a więc klientami, klientami klientów (jeśli organizacja działa na ryn-

kach B2B i B2C), dostawcami, administracją, bankami i innymi interesariuszami, uczestniczącymi w realizowanych transakcjach.

Zasady zarządzania bezpieczeństwem informacji w przedsiębiorstwie

Zarządzanie bezpieczeństwem IT

Zarządzanie bezpieczeństwem IT, zwłaszcza w branżach, w których platforma IT stanowi podstawę do rozwoju biznesu, powinno być wyodrębnione w infrastruktury organizacyjnej i oddzielone od systemów IT. Obecnie każda działalność biznesowa w coraz większym stopniu uwzględnia platformę internetową jako jeden z kanałów docierania do klientów. Branże bankowa, ubezpieczeniowa i logistyczna (w tym: kurierska, ekspresowa i paczkowa – tzw. KEP) traktują ten obszar jako jeden z kluczowych czynników wartości oferowanej klientom. W tej sytuacji kluczowe jest, aby osoba zarządzająca (np. szef bezpieczeństwa informacji) raportowała bezpośrednio do zarządu i miała możliwość niezależnego audytowania systemów IT, jak również mogła koordynować wszelkie funkcje, dotyczące szeroko rozumianego bezpieczeństwa (w tym również bezpieczeństwa fizycznego). Istotnym elementem zarządzania bezpieczeństwem jest stworzenie odpowiedniego dokumentu, w którym są określone zasady polityki, jak również procedury i standardy oraz system raportowania w tym obszarze. Niekiedy, przy rozbudowanych strukturach organizacyjnych i sieciowej organizacji, warto stworzyć i wyszkolić zespół ludzi, który na miejscu dba o bezpieczeństwo informacji, sprawdzając systemy, procedury oraz sam sprzęt IT i oprogramowanie.

Plan bezpieczeństwa IT

Opracowanie planu bezpieczeństwa wymaga zidentyfikowania kluczowych ryzyk związanych z bezpieczeństwem informacji [7]. Ryzyka te mogą być zmienne w czasie i mieć różny aspekt finansowy z punktu widzenia firmy i pozostałych interesariuszy – uczestników łańcucha/sieci dostaw (w tym przede wszystkim klientów i dostawców). Konieczne jest również dokonanie analizy kosztowej takiego planu i zbadanie, jakie są rzeczywiste oczekiwania klientów w tym zakresie. Awaria systemów IT może prowadzić do utracenia części informacji niezbędnych do efektywnego zarządzania danym produktem czy usługą, co wiąże się z powstaniem kategorii „utraconych możliwości" z punktu widzenia klienta lub innych interesariuszy. W tej sytuacji konieczne jest podjęcie decyzji wspólnie z osobami/firmami najbardziej zainteresowanymi, w jakim czasie konieczne jest przywrócenie pełnej funkcjonalności systemu, biorąc pod

uwagę zarówno koszty, jak też efekty. Często decyzja ta może mieć charakter *trade off*, gdzie optymalizacja kosztowa rozwiązania będzie podstawowym czynnikiem wyboru. Można sobie bowiem wyobrazić, że każdy klient/osoba oczekuje natychmiastowej reakcji na awarię systemu, co oznacza bardzo wysokie inwestycje w dublowanie drogiej infrastruktury. Po głębszej analizie okazuje się jednak, że można się zgodzić na czas reakcji na poziomie kilku godzin, a nawet dłużej, co zdecydowanie zmniejsza koszty takiego rozwiązania.

W efekcie oznacza to konieczność zidentyfikowania krytycznych – z punktu widzenia klienta – systemów informatycznych oraz przygotowania kompletnych planów awaryjnych, które można wykorzystać w sytuacji zakłóceń lub też określonych wyraźnie incydentów [6]. Tego typu plany awaryjne, podobnie jak w przypadku systemów bezpieczeństwa osób, powinny być testowane w naturalnym środowisku z określoną częstotliwością, tak aby w przypadku, gdy dojdzie do zaburzeń – procedura była w pełni opanowana. W praktyce często zdarza się, że plany awaryjne, rozpisane profesjonalnie, w rzeczywistością zawodzą, ponieważ zabrakło ćwiczeń w tym zakresie. Zdarza się także, że w planach awaryjnych brakuje informacji, kto podejmuje decyzje w przypadku, gdy awaria odbiega w jakimś stopniu od wcześniej zidentyfikowanej.

Kolejnym istotnym elementem zabezpieczenia systemu jest przegląd planów awaryjnych zaplanowany co najmniej kilka razy w roku. Liczba przeglądów uzależniona jest od dynamiki rozwoju platformy IT, a tym samym zmian, jakie zachodzą w głównych systemach. Przegląd często niesie za sobą konieczność zmiany planów awaryjnych. Warto też pamiętać, że awarie dotyczące systemów IT, jeśli związane są z zawodnością danego systemu, niosą nieco mniejsze ryzyko niż naruszenie bezpieczeństwa IT, którego dokonano świadomie przez ludzi w celu przejęcia określonych informacji (np. konkurencja), pozyskania baz danych (np. pracownicy). Jak wynika z badań, większość włamań do systemów IT jest wynikiem działań pracowników firmy (cel może być różny, jednym z nich jest także pewnego rodzaju zabawa w łamanie systemów).

Jednym z ważniejszych czynników bezpieczeństwa jest opracowanie standardu bezpieczeństwa dla kluczowych platform technologicznych oraz zarejestrowanie standardowej konfiguracji w rejestrze konfiguracji. Warto też się upewnić, że plan obejmuje: kompletny zestaw polityk i standardów, procedury ich wdrożenia i egzekwowania, opis ról i odpowiedzialności, wymagania kadrowe, podnoszenie świadomości użytkowników i szkolenia, opis wymaganych inwestycji w bezpieczeństwo informacji.

Zarządzanie tożsamością

Zarządzanie tożsamością oznacza ustalenie zakresu dostępu i możliwości pasywnego bądź aktywnego wpływania na obowiązujące standardy. W tym celu konieczne jest stworzenie kluczowej dokumentacji (może ona być zarówno w formie papierowej, jak też elektronicznej) oraz listy osób, które mają dostęp do tej informacji na zasadzie przeglądania jej i/lub dokonywania zmian. Dostęp do systemów powinien być możliwy wyłącznie dla uwierzytelnionych użytkowników. Polityka bezpieczeństwa informacji jest ściśle powiązana z zasadami podziału ról i obowiązków w ramach procesów biznesowych, co w praktyce oznacza, że właściciele procesów biznesowych muszą akceptować tworzenie nowych funkcji oraz ich zmianę. Także sam proces przyznawania uprawnień i mechanizmy uwierzytelnienia powinny być oparte na określonych procedurach.

Zarządzanie kontami użytkowników

Zarządzanie kontami użytkowników wymaga, podobnie jak inne czynności z zakresu zarządzania, wyraźnie określonych procedur oraz zasad ich weryfikacji, jak również kontroli uprawnień do systemów. Dość często zdarza się, zwłaszcza w dużych organizacjach, że zmiany organizacyjne, rozwiązanie umowy o pracę czy też zwolnienia nie znajdują odzwierciedlenia w weryfikacji uprawnień. W przypadku dobrze prowadzonej polityki bezpieczeństwa informacji, tego typu sytuacje są jednoznacznie opisane w ramach procedur i w momencie wystąpienia którejś z nich – następuje uruchomienie danej procedury. Sprowadza się ona najczęściej do realizacji określonej liczby działań w określonym porządku, co ma istotne znaczenie dla zachowania bezpieczeństwa.

Zdarza się także, że uprawnienia do korzystania z systemów otrzymują również osoby z zewnątrz, przykładowo: klienci w pewnym zakresie korzystają z udostępnionego im miejsca na serwerze usługodawcy czy też producenta (operatora logistycznego itp.). Za pomocą haseł mogą oni sprawdzić status swojej przesyłki albo stopień zaawansowania realizacji zamówienia. Ten sposób, wygodny dla klienta, stwarza jednak określone zagrożenia:

- może nastąpić nawet przypadkowa awaria systemu i klient będzie miał dostęp do całości informacji (w tym również utajnionych informacji firmy – producenta lub usługodawcy);
- włamanie do systemu firmy może spowodować nie tylko naruszenie danych firmy, ale również dostęp do danych firm, z którymi prowadzone są działania biznesowe.

W związku z powyższym również w tym obszarze należy zadbać o stworzenie właściwej ochrony danych, przy czym systemy, aplikacje i dane powinny być sklasyfikowane według kryterium ważności i ryzyka.

Testy bezpieczeństwa i monitorowanie

Ten obszar wymaga pełnej inwentaryzacji wszystkich urządzeń sieciowych oraz ich okresowej weryfikacji. Każde z tych urządzeń powinno mieć przypisany poziom ryzyka z punktu widzenia krytyczności systemów wykorzystywanych w firmie i systemów użytkowanych wspólnie przez kilka firm w ramach łańcucha/sieci dostaw. Na tej podstawie tworzone są standardy bezpieczeństwa dla wszystkich wykorzystywanych technologii. Pewnym problemem może być brak opisów aplikacji, co często występuje w firmach, gdzie działy IT są rozbudowane i nie ma wyraźnych procedur dotyczących zasad tworzenia aplikacji. Członkowie zespołów IT, często uzdolnieni informatycznie, tworzą aplikacje zgodnie z oczekiwaniem klienta biznesowego, prawie na poczekaniu, nie zajmując się faktycznym opisem aplikacji. W efekcie w momencie powstania zakłócenia w działaniu danej aplikacji nikt, oprócz autora, nie jest w stanie usunąć powyższego zakłócenia. Ten sposób działania znacznie utrudnia zarządzanie polityką bezpieczeństwa informacji.

Zdarza się również, że członkowie zespołów IT nie przywiązują wagi do wykonywania – przed ostatecznym uruchomieniem aplikacji – testów bezpieczeństwa, traktując je jako zbędną czynność, niepotrzebnie wydłużającą całą procedurę. W tym przypadku może dochodzić do konfliktu między szefem bezpieczeństwa a szefem IT. Aby zminimalizować tego typu sytuacje, konieczne jest budowanie świadomości bezpieczeństwa wśród wszystkich pracowników, w szczególności jednak wśród pracowników IT. Dodatkowe zagrożenie może powstać w sytuacji, gdy część działań IT będzie realizowana przez firmę zewnętrzną. Stąd też kluczowe dla utrzymania systemu bezpieczeństwa jest właściwe określenie systemów, które są najważniejsze z punktu widzenia podstawowej działalności biznesowej danej firmy, i ustanowienie dla nich szczególnej ochrony.

Konieczne jest również opracowanie systemów monitoringu urządzeń o krytycznym znaczeniu z punktu widzenia możliwości wystąpienia incydentów bezpieczeństwa. Jeśli organizacja zarządzana jest projektowo, warto pamiętać o wbudowaniu w metodykę projektową już w momencie ustalania podstawowych elementów projektu – również analizy bezpieczeństwa informacji. Sam proces zarządzania incydentami powinien obejmować [4]:

- wykrywanie zdarzeń,
- korelację zdarzeń i ocenę zagrożenia,
- wyeliminowanie zagrożenia lub eskalacji i uruchomienie innych procedur,
- ustalenie kryteriów uruchomienia procedur obsługi incydentu,
- weryfikację i wymagany poziom dokumentacji incydentu i jego rozwiązania,

- analizę po rozwiązaniu incydentu,
- procedury zamknięcia incydentu.

Ochrona technologii bezpieczeństwa

Właściwy system ochrony technologii stanowi ważny czynnik prewencji w przypadku polityki bezpieczeństwa informacji. W tym celu konieczne jest zbadanie, jak dalece procedury, opisane w polityce, uwzględniają konsekwencje naruszenia bezpieczeństwa informacji. Kolejnym krokiem jest analiza dokumentacji, na podstawie której jest przyznawany i akceptowany dostęp do systemów oraz dzienników systemowych pod kątem nieudanych prób dostępu, blokady kont, dostępu do wrażliwych zasobów oraz dostępu do pomieszczeń. Jednym z ważniejszych, często niedocenianych (zwłaszcza przez użytkowników) elementów jest wdrożenie i przestrzeganie polityki haseł (długość, kompozycja, ważność itp.). Sam dostęp do systemów powinien być przyznawany po odpowiedniej akceptacji, a weryfikacja mechanizmów bezpieczeństwa logicznego i fizycznego systemów i danych oraz uprawnień użytkowników powinna być dokonywana przynajmniej raz w roku. Warto również dokonywać analizy raportów bezpieczeństwa systemów pod kątem istniejących podatności i systematycznie wprowadzać nowe rozwiązania. Ta zasada działa podobnie jak aplikacje chroniące przed wirusami. W krótkim czasie (do miesiąca) definicje wirusów stają się przestarzałe i wymagają odświeżenia. Podobnie systemy zabezpieczeń, w kontekście bardzo szybko rozwijających się systemów IT, stają się mało skuteczne.

Zarządzanie kluczami kryptograficznymi

Klucze kryptograficzne są narzędziem pozwalającym zwiększać poziom bezpieczeństwa przechowywanych i wymienianych informacji poprzez zapewnienie szyfrowania i deszyfrowania informacji (w kryptografii symetrycznej). Do obu czynności używa się tego samego klucza, co oznacza, że powinien on być znany tylko uczestnikom wymiany informacji. Klucz przypisany jest do danej komunikacji. W przypadku kryptografii asymetrycznej występują dwa rodzaje kluczy: publiczny i prywatny. W pierwszym przypadku mamy do czynienia z jawną informacją, w drugim – jest w pełni utajniona. W celu lepszej ochrony konieczne jest zatem zdefiniowanie procesu zarządzania cyklem życia kluczy kryptograficznych. Klucze prywatne powinny podlegać odpowiedniej ochronie przed utratą poufności i integralności.

Ochrona, wykrywanie i usuwanie złośliwego oprogramowania

Tak jak wcześniej wspomniano, najbardziej skutecznym narzędziem zabezpieczenia informacji jest zwiększenie poziomu świadomości pracowników,

klientów oraz innych interesariuszy, którzy uczestniczą w łańcuchu/sieci dostaw. Jednym z częściej występujących zakłóceń jest tzw. złośliwe oprogramowanie, często samoinstalujące się na danym komputerze, przekazywane czy też podczepiane do plików, otrzymywanych nawet z wiarygodnych (sprawdzonych) adresów. W związku z powyższym konieczne jest opracowanie polityki ochrony przed złośliwym oprogramowaniem, udokumentowanie i zakomunikowanie jej wszystkim pracownikom firmy. Jednocześnie niezbędne jest wdrożenie systemów, które wykrywają złośliwe oprogramowanie i zabezpieczają przed jego instalacją. W efekcie prowadzi to do ograniczenia adresów internetowych, które mogą być wykorzystane w pracy. W niektórych firmach zablokowane są również możliwości przegrywania plików na zewnętrzne nośniki informacji oraz wgrywania plików do komputera. To w znaczący sposób zmniejsza zagrożenie związane z przeniesieniem wirusa, choć z drugiej strony ogranicza swobodny dostęp do zewnętrznych źródeł wiedzy. Oprogramowanie antywirusowe powinno być dystrybuowane i zarządzane centralnie, przy czym kluczowe jest określenie jego skuteczności operacyjnej. Na ogół funkcjonują już filtry w postaci *firewall*, które nie pozwalają przedostać się do środka systemu niepewnym informacjom, jednocześnie sam użytkownik może zdefiniować, które adresy czy też słowa użyte w temacie wiadomości powinny być automatycznie wysyłane do kosza.

Wymiana wrażliwych informacji

W dobie łączenia się za pomocą różnych protokołów transmisji z zewnętrznymi podmiotami i/lub udostępniania miejsca na własnym serwerze innym użytkownikom konieczne jest wykorzystanie specjalnych metod szyfrowania w celu ochrony danych. W praktyce zdarza się, że nawet audytorzy z wielkiej czwórki nie mają opracowanych zasad wykorzystania wrażliwych danych i w ramach audytu proszą o przekazywanie kopii w formie papierowej, którą następnie chcą wykorzystywać już w siedzibie własnego przedsiębiorstwa. Tego typu praktyki powodują powstawanie dodatkowego ryzyka po stronie audytowanego i narażenie klientów na utratę poufnych danych.

W kontekście coraz częściej pojawiających się zagrożeń w zakresie zarządzania bezpieczeństwem informacji, a także zagrożeń wynikających z podejmowania działań niezgodnych z prawem i obowiązującymi regułami/procedurami w organizacjach zaczęto wprowadzać, zgodnie z ustaleniami Komisji Europejskiej, politykę w zakresie zgodności (ang. *compliance*).

Podsumowanie

W warunkach globalizacji, powszechnej digitalizacji i swobodnego dostępu do informacji wzrastają zagrożenia związane z cyberatakami, przypadkową utratą wrażliwych informacji wszystkich uczestników sieci/łańcucha dostaw. W tym kontekście ochrona bezpieczeństwa informacji staje się coraz istotniejszą funkcją przedsiębiorstwa. Z kolei naruszenie zasad działania, brak monitoringu zagrożeń, uchybienia prawne i proceduralne, które były przyczyną spektakularnych upadków znaczących korporacji międzynarodowych, spowodowały, że zaczęto rozwijać politykę w zakresie przestrzegania i systematycznego audytowania procedur określaną jako *compliance*. Można się spodziewać, że w przyszłości funkcja bezpieczeństwa informacji zostanie włączona do szerokiej działalności działów operacyjnych realizujących politykę w zakresie *compliance*.

Literatura

[1] D. Brink, Beyond Demonstrating Compliance, The Reinvention of Internal Audit, Aberdeen Group, August 2009.
[2] Dziennik Ustaw z 1993 r. Nr 47, poz. 211.
[3] R. Kaczmarek, Przegląd procesu zarządzania bezpieczeństwem informacji w pigułce [w:] Computerworld z dn. 10.03.2009 r.
[4] S. Kosielinski, W kręgu pięciu żywiołów [w:] Computerworld z dn. 10.02.2009 r.
[5] M. Kowalewski, A. Ołtarzewska, Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego, Telekomunikacja i Techniki Informacyjne, nr 3.4/2007.
[6] Rządowy Program Ochrony Cyberprzestrzeni, marzec 2012 r.
[7] B. Zdanowicz, Compliance – nowa funkcja banków, www.nbp.pl