PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1122 — 2006
Ekonomia i Międzynarodowe Stosunki Gospodarcze 12

Tomasz Galewski

ROLA BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE W WARUNKACH UPOWSZECHNIANIA SIĘ INTERNETU

1. Wstęp

Termin bezpieczeństwo informacji w ostatnim czasie pojawia się coraz częściej jako główny temat konferencji, monografii, podręczników, publikacji itd. Dzieje się to za sprawą coraz istotniejszej roli, jaką odgrywa informacja w funkcjonowaniu przedsiębiorstwa. Jak wynika z piramidy wiedzy, dane przeradzają się w informacje, a te dzięki umiejętnemu ich wykorzystaniu mogą zaowocować wiedzą. Natomiast zasób wiedzy w przedsiębiorstwie to obecnie najważniejszy komponent przewagi nad rynkowymi przeciwnikami. A Kukliński tak określa znaczenie wiedzy we współczesnej gospodarce: „jedynym pewnym źródłem przewagi konkurencyjnej jest wiedza. Kiedy zmieniają się rynki, eksplodują nowe technologie, mnożą się konkurenci, a produkty starzeją się prawie w ciągu nocy, przedsiębiorstwami mającymi sukcesy są te, które konsekwentnie tworzą nową wiedzę, rozpowszechniają ją szeroko w całej organizacji i szybko przekształcają w nową technologię i produkty. Takie działania określa się jako »przedsiębiorstwo kreowane przez wiedzę«, którego jedynym biznesem są systematyczne innowacje"[1]. Tak więc zapewnienie firmie odpowiednich informacji staje się dla pracowników kluczowym zadaniem. Jako bezpieczeństwo informacji rozumieć tu będziemy za Pipkinem: „ochronę własności intelektualnej wypracowanej w danej instytucji. Ta wartość ma podstawowe znaczenie dla przeżycia instytucji"[2].

Co prawda w teorii ekonomii mamy do czynienia z sytuacją, w której zakłada się, że podmiot rynkowy dysponuje doskonałą informacją, jednakże w praktyce jest to warunek trudny do spełnienia lub wręcz niemożliwy. Tak więc uczestnicy na danym rynku zmuszeni są do podejmowania decyzji w warunkach niedoskonałej informacji. Oczywiście wiąże się to z tym, że nabywcy i oferenci nie uzyskują maksymalnych – możliwych do uzyskania przy pełnej informacji – korzyści. By

[1] A. Kukliński, *Gospodarka oparta na wiedzy*, KBN, Warszawa 2001, s. 23.
[2] D. Pipkin, *Bezpieczeństwo informacji*, WNT, Warszawa 2002, s. XV.

otrzymać lepsze użyteczności zakupionych koszyków dóbr i większe zyski, konsumenci i oferenci mogą zdecydować się na zdobywanie kolejnych informacji. Wymusza to na nich analizę wartości informacji, czyli porównywanie korzyści, jakie by uzyskali bez nowych informacji i korzyści z zastosowaniem większej informacji.

Intuicyjnie aktywność podmiotów w dziedzinie informacji postrzega się jako proces zdobywania nowych danych, mający na celu poprawę jakości podejmowanych decyzji. Jest to jednak jedną stroną możliwej aktywności informacyjnej podmiotu. Drugą jest bowiem przekazywanie informacji (transmisja danych lub sygnalizowanie)[3].

Szczególnego znaczenia nabiera informacja w czasach upowszechniania się Internetu. Znaczna część firm jest podłączona do tej sieci, co jednocześnie jest w ich rękach doskonałym narzędziem wykorzystywanym w procesach informacyjnych i stanowi niemałe zagrożenie, jeżeli chodzi o zapewnienie bezpieczeństwa informacji.

Przykłady różnych rodzajów aktywności informacyjnej można przedstawić za pomocą tabeli (tab. 1).

Tabela 1. Rodzaje aktywności informacyjnej

Aktywna rola		Pasywna rola	
		oferent	nabywca
Nabywca	zaopatruje się w informacje	I. Porównywanie cen, porównywanie jakości	II. Naśladownictwo, zbieranie informacji
	przekazuje informacje	III. Ujawnianie zdolności płatniczej	IV. Lansowanie mody, demonstracyjna konsumpcja
Oferent	zaopatruje się w informacje	V. Badanie konkurencji, szpiegostwo	VI. Badanie rynku, badanie konsumenta
	przekazuje informacje	VII. Fałszywe sygnały, blefy, zmowa	VIII. Ujawnianie jakości, reklama, gwarancja

Źródło: S. Forlicz, *Mikroekonomiczne aspekty przepływu informacji między podmiotami rynkowymi*, WSB, Poznań 1996, s. 10.

W artykule koncentrujemy się na aktywności informacyjnej przedsiębiorstwa, więc nie będzie nas interesował proces informacyjny występujący między nabywcami.

Do potencjalnych zagrożeń dla firmy będziemy zaliczać:
- utratę zasobów informacji,
- zmianę informacji,
- rozpowszechnianie informacji nieprawdziwych wskutek podszycia się (*spoofing*),

[3] S. Forlicz, *Niedoskonała wiedza podmiotów rynkowych*, PWN, Warszawa 2001, s. 49.

- utratę wiarygodności przedsiębiorstwa,
- zdobycie nieodpowiednich informacji.

Pierwszy problem to sprawa umiejętnego pozyskania koniecznych informacji, lecz na tym nie kończy się wysiłek prowadzący do zwycięstwa w walce o klientów. Przedsiębiorstwo posiadające nawet najlepsze zasoby informacji może je bardzo szybko stracić na rzecz konkurentów i stracić nad nimi przewagę. Dlatego też równie ważne staje się zapewnienie bezpieczeństwa zgromadzonych danych i informacji. Niestety, problem digitalizacji działalności gospodarczej pozostaje dla niektórych zbyt niezrozumiały i skomplikowany, a tym samym pomijany. Przestępstwa, które zdarzają się w przestrzeni wirtualnej, są w pewien sposób nieuchwytne dla współczesnego laika, więc często się zdarza, że ich istnienie bywa lekceważone. Natomiast ci, którzy są świadomi zagrożeń, z reguły są zatrudnieni w informatycznych działach firmy i, co z żalem należy stwierdzić, mają mały wpływ na podejmowanie istotnych działań w firmie. Do rzadkości należy zasiadanie głównego informatyka w zarządzie przedsiębiorstwa, więc wiedza o potencjalnych zagrożeniach pozostaje w kręgach wyspecjalizowanych pracowników i napotyka mentalną barierę u pozostałych współpracowników[4]. Wynika to po części również z tego, że następuje dynamiczna zmiana w funkcjonowaniu firmy. Biurokratyczne formy rządów odchodzą w niepamięć i na ich miejscu pojawia się nowa forma zwana adhockracją, czyli działaniem w bardzo szybko zmieniającym się otoczeniu i koniecznością coraz większego udziału wszystkich pracowników w zarządzaniu firmą[5]. Menedżerowie nie są w stanie ogarnąć całej wiedzy ze wszystkich dziedzin koniecznych do sprawnego kierowania firmą, więc przynajmniej w części zadań odpowiedzialność za ich wykonanie muszą brać na siebie poszczególni pracownicy. Z takim właśnie przykładem mamy chyba do czynienia, jeżeli chodzi o bezpieczeństwo informacji. Jak pokazują badania w Wielkiej Brytanii, aż 24% firm nie ma zdefiniowanej polityki bezpieczeństwa informacji. A skoro Wielka Brytania wyprzedza Polskę w tempie wykorzystania technologii informatycznych i jest zdecydowanie bardziej zaawansowana w budowaniu tzw. społeczeństwa informacyjnego, wyniki podobnych badań w Polsce nie przedstawiałyby się lepiej[6].

Artykuł ten ma na celu przybliżenie problematyki bezpieczeństwa informacji, przede wszystkim ukazanie źródeł zagrożeń oraz przedmiotów ataku. Podstawowe wnioski tej publikacji mogą zadziwić niejednego menedżera firmy, przyzwyczajonego do kojarzenia ataków na stabilność informacyjną przedsiębiorstwa z istnieniem środowiska hakerów. Mam nadzieję, że zobrazowanie tematu ochrony informacji będzie przyczynkiem do zastanowienia się nad wprowadzeniem zasad polityki bezpieczeństwa informacji w firmie lub do rewizji jej podstawowych zasad, gdyż według S. Kwiatkowskiego: „społeczeństwo informacyjne – to nie tyl-

[4] W. Krusiński, M. Ścibor, *Plusy i wirusy*, „Polityka" 2004 nr 44, s. 88-91.
[5] A. Toffler, *Szok przyszłości*, Zysk i S-ka, Poznań 1998, s. 144.
[6] W. Krusiński, M. Ścibor, wyd. cyt., s. 88-91.

ko społeczeństwo powszechnej dostępności do informacji, ale również społeczeństwo powszechnej możliwości przechwytywania informacji, manipulowania nią, wykorzystywania"[7].

Co roku amerykański Computer Security Institute we współpracy z FBI przeprowadza badania dotyczące przestępstw komputerowych. Dane z 2001 r. oparte na próbie 500 firm i agend rządowych działających w USA potwierdzają, że:

- firmy są poddawane cyberatakom zarówno z zewnątrz, jak i z wewnątrz,
- istnieje szeroki zakres form ataków,
- cyberataki mogą powodować poważne straty finansowe,
- aby skutecznie obronić się przed takimi atakami, nie wystarczy korzystać z informatycznych technologii bezpieczeństwa.

Wyniki tych badań wyraźnie wskazują, że problem cyberprzestępczości jest coraz poważniejszy. W 1998 r. udział respondentów, którzy zanotowali próbę wtargnięcia do ich systemu informatycznego z zewnątrz, wynosił 23%, w 2001 r. – już 40%. Dodatkowo aż 64% procent tych firm poniosło straty finansowe z tytułu tych wtargnięć i 35% nie było w stanie podać wielkości tych strat. Co ważniejsze, 94% firm dokonało po włamaniu takich zmian w systemie, by podobny atak nie mógł już być przeprowadzony, a 40% w ogóle nie zgłosiło tego ataku[8]. Powody takiego działania wydają się oczywiste, gdyż przedsiębiorstwa nie mogą sobie pozwolić na opinię nie zabezpieczonych przed skutkami przestępstw cybernetycznych. Zgodnie z tym należy wziąć poprawkę na wyniki wszelakich badań dotyczących poziomu zabezpieczeń w firmach, ponieważ przedsiębiorstwa mogą się bać podawania takich danych w ankietach w obawie przed ich wydostaniem się na zewnątrz, co groziłoby utratą klientów, niezadowolonych z bezpieczeństwa firmy.

Podstawowe aspekty bezpieczeństwa informacji. Analizując poziomy bezpieczeństwa, wyodrębnia się kilka aspektów ochrony danych i informacji. Do najważniejszych należą:

- poufność – równoznaczne to jest z tym, że informacje są dostępne tylko dla uprawnionych osób, może ona dotyczyć wszystkich danych lub tylko ich części,
- uwierzytelnianie – polega na identyfikacji źródła pochodzenia danych i zapewnieniu jego autentyczności,
- integralność – oznacza, że informacje nie były modyfikowane przez osoby do tego nie upoważnione,
- niezaprzeczalność – uniemożliwia próby zaprzeczenia, że komunikat został przesłany, obie strony – nadawca i odbiorca komunikatu – mogą udowodnić, że wiadomość do nich dotarła bądź została wysłana,

[7] S. Kwiatkowski, *Przedsiębiorczość intelektualna a trwały rozwój gospodarczy europejskich krajów posocjalistycznych*, [w:] *Nowa gospodarka i jej implikacje dla długookresowego wzrostu w krajach postsocjalistycznych*, red. G. Kołodko, WSPiZ, Warszawa 2001, s. 99.

[8] www. idg.pl/news/39709.html

- dyspozycyjność – umożliwienie uprawnionym osobom dostępu do danych w każdej chwili,
- rozliczalność – pozwala określić odpowiedzialność za skutki działań przeprowadzonych w systemie informatycznym.

2. Rodzaje ataków skierowanych przeciwko bezpieczeństwu informacji

Zagrożenia dotyczące informacji w przedsiębiorstwie odnoszą się do wszystkich wymienionych uprzednio aspektów. Dalej przedstawiony zostanie wyczerpujący wykaz ataków, z podziałem na podmiot działania, przedmiot oraz cel.

Najczęściej, mówiąc o przestępstwach w cyberprzestrzeni, mamy na myśli działania o charakterze zamierzonym i przegląd tych właśnie ataków zaprezentujemy jako pierwszy. Należą do nich:

- przerwanie,
- przechwycenie,
- modyfikacja,
- podrobienie.

2.1. Przerwanie

Przerwanie ma na celu uniemożliwienie korzystania z systemu informatycznego. Działania atakującego są ukierunkowane na takie obciążenie systemu, by użytkownik nie mógł w dotychczasowy normalny sposób korzystać z zasobów informacji. Wśród tej grupy zagrożeń najpopularniejsze sposoby na przerwanie pracy systemu to: przeciążenie i wprowadzenie wirusów komputerowych.

Przeciążenie systemu informatycznego polega na przesyłaniu do niego olbrzymiej ilości danych, których nie jest w stanie na bieżąco zanalizować. Może to być przesyłanie e-maili, żądania usług sieciowych czy temu podobnych komunikatów z takim natężeniem, że komputery nie będą mogły zrealizować wszystkich zadań, a co za tym idzie, również tych od faktycznych użytkowników. Jeżeli taki atak przeprowadzany jest z jednego komputera, to nazywamy go „odmową usługi" (DoS – *Denial of Service*), natomiast istnieje możliwość wykorzystania w tym celu innych komputerów podłączonych do Internetu. Często jest tak, że użytkownik takiego komputera nie ma pojęcia, że uczestniczy w takim ataku, gdyż wcześniej haker zainstalował na jego terminalu program do automatycznego wysyłania komunikatów pod dany adres i dzieje się to niezależnie od zamiarów „nieświadomego" użytkownika. Taki atak nazywamy wtedy rozproszoną odmową dostępu (DDoS – *Distributed Denial of Service*).

Wirusy komputerowe to fragmenty kodu programu, które są „przyklejone" do oryginalnego programu i mają na celu spowolnienie pracy systemu bądź jego zablokowanie. Wśród wirusów można wyodrębnić następujące ich rodzaje:

- wirusy rekordu startowego – koncentrują swe ataki na programach, które są konieczne do uruchomienia komputera,
- wirusy plikowe – przenoszą się za pomocą programu wykonywalnego, zmieniając strukturę tego programu tak, by uruchamiał się jako pierwszy; wirusy te mogą zainfekować system tylko wtedy, gdy zostaną uruchomione,
- wirusy towarzyszące – podobne do plikowych, z tą różnicą, że nie przyłączają się do programu, tylko tworzą oddzielny plik,
- bakterie – wirusy, które się pomnażają w szybkim tempie, by np. zapełnić miejsce na twardym dysku,
- wirusy makro – infekują pliki, w których można zapisywać makropolecenia,
- robaki – programy, które przenoszą się z komputera na komputer, jako przykład można podać najsłynniejszy chyba wirus „I love you", który spowodował straty na sumę szacowaną na 5-10 mld dolarów[9].

Skutki ekonomiczne przerwania – uniemożliwienie dostępu do danych może spowodować poważne skutki ekonomiczne w przedsiębiorstwie. W zależności od rodzaju prowadzonej działalności będą to np.:

- utrudnienie lub uniemożliwienie obsługi klientów,
- wydłużenie czasu pracy nad nowymi produktami,
- obniżenie wydajności pracy,
- wzrost kosztów w firmie,
- utrudniona reakcja na posunięcia konkurentów,
- uniemożliwienie klientom dostępu do potrzebnych informacji – np. porównywania cen.

2.2. Przechwycenie

Przechwycenie to działanie, które ma na celu spowodowanie utraty poufności danych, czyli sytuacji, kiedy przestępcy mają możliwość przeglądania informacji, do których penetracji nie są upoważnieni. Wyróżniamy dwa główne rodzaje ataków z grupy przechwyceń:

- ujawnienie informacji,
- analizę przesyłu.

Ujawnienie informacji może oznaczać wykorzystanie dokumentacji firmy bezpośrednio lub wydostanie informacji pośredniczących (takich jak hasła dostępu), które w przyszłości mogą umożliwić uzyskanie interesujących danych bezpośrednich.

Ujawnienie informacji może przebiegać za pomocą: sniffingu, koni trojańskich, przeglądania, przenikania. Sniffing to „węszenie", czyli przeglądanie informacji przesyłanych kanałami komunikacyjnymi, adresowanych do innych użytkowników. Można dzięki temu uzyskać numery kart kredytowych, hasła, prywatne dane,

[9] www. micharaf.republika.tezapbdpr.htm

itp. Koń trojański to program, który instaluje się w systemie użytkownika i wykonuje polecenia w nim zapisane, najczęściej bez jego wiedzy. Na przykład może przesyłać hasła do atakującego, w czasie gdy użytkownik będzie je wpisywał do któregoś z programów. Przenikanie to pozyskiwanie informacji, do których normalnie użytkownik nie ma dostępu.

Analiza przesyłu to badanie przechodzących komunikatów pod kątem odnalezienia lokalizacji komputerów w firmie i ich tożsamości. Te informacje tylko z pozoru wydają się mało ważne. W rękach doświadczonego hakera mogą spowodować duże straty w późniejszych etapach ataku.

Skutki ekonomiczne przechwycenia – ataki w postaci przechwycenia mają głównie na celu wydobycie zasobów informacyjnych przedsiębiorstwa, więc skutkiem może być:
- utrata tajemnic handlowych (receptury, *know-how* itp.),
- wyciek bazy klientów,
- ujawnienie informacji zarezerwowanych tylko dla pracowników firmy,
- poznanie sytuacji finansowej przedsiębiorstwa.

2.3. Modyfikacja

Modyfikacja ma na celu dotarcie do informacji zawartych w systemie informatycznym i dokonanie w nim zmian, które spowodują utratę integralności. Różne mogą być przejawy modyfikacji:
- dopisanie do istniejących informacji jakiejś dodatkowej,
- przeformatowanie oryginalnej treści,
- wymazanie niektórych danych zapisanych w systemie,
- umyślne opóźnianie wysłania komunikatu, tak by po jakimś czasie stał się już bezużyteczny.

Skutki ekonomiczne modyfikacji – modyfikacja danych w przedsiębiorstwie oczywiście znacznie utrudnia analizowanie procesów gospodarczych, powodując np.:
- znaczne straty, gdy popyt ulegnie przeszacowaniu lub niedoszacowaniu w wyniku wprowadzenia błędnych danych dotyczących popytu,
- błędne naliczanie wynagrodzeń pracownikom,
- kradzieże pieniędzy z rachunków firmy,
- znaczne koszty odtworzenia prawdziwych danych.

2.4. Podrobienie

Podrobienie to podszywanie się (*spoofing*) pod innych użytkowników, czyli komputer atakującego stara się dostać do systemu, udając inny terminal i wprowadzając tym samym system w błąd. Podczas udanego podszycia się atakujący może zamieszczać w systemie informatycznym firmy swoje dane lub prosić inne komputery znajdujące się w sieci o przesłanie mu pożądanych komunikatów.

Ekonomiczne skutki spoofingu:
- utrata wiarygodności przedsiębiorstwa,
- odpowiedzialność za przeprowadzane nielegalnie transakcje,
- dezorganizacja pracy.

3. Zagrożenia losowe

Oprócz zagrożeń ze strony tzw. cyberprzestępców są również wypadki losowe. W założeniach polityki bezpieczeństwa firmy musi się znaleźć zapis o podjęciu odpowiednich kroków w celu zapobieżenia stratom wynikającym właśnie z takich zdarzeń losowych. Mogą one mieć charakter zewnętrzny, czyli występować z przyczyn mających swe źródło poza terenem firmy, lub wewnętrzny, czyli być związane z systemem zainstalowanym w przedsiębiorstwie lub z pracą użytkowników tego oprogramowania.

Zagrożenia losowe zewnętrzne:
- nieodpowiednia temperatura i wilgotność w pomieszczeniach firmy,
- zakłócenia w dostawie zasilania,
- wyładowania atmosferyczne,
- klęski żywiołowe.

Zagrożenia losowe wewnętrzne:
- błędnie skonfigurowane systemy operacyjne i programy – czasami nawet wyspecjalizowani administratorzy sieci popełniają błędy w konfiguracji, gdyż nowoczesne aplikacje są coraz bardziej skomplikowane,
- błędy w oprogramowaniu – żaden program informatyczny nie jest pozbawiony błędów, nawet wielokrotne testy nie są w stanie wykryć wszystkich uchybień, a hakerzy udostępniają sobie wiadomości o lukach w programach, które znaleźli,
- błędy i zaniedbania użytkowników – wynikają one z niewiedzy lub ze zmęczenia,
- losowe uszkodzenia sprzętu – np. zmęczenie materiału.

Wiedząc, że firma musi się liczyć z tym, że w przestrzeni wirtualnej czai się na nią wiele zagrożeń, należy poddać wnikliwej analizie ochronę danych i przedsięwziąć odpowiednie kroki. Można zacząć od przeprowadzenia tzw. audytu bezpieczeństwa systemów informatycznych. Umożliwia on ocenę i kontrolę poziomu bezpieczeństwa w firmie. W ramach audytu sprawdza się stronę zarówno techniczną, jak i organizacyjną, a służą do tego m.in. testy penetracyjne i kontrolne. Te pierwsze pozwalają na symulowany atak zarówno z Internetu, jak i z wewnątrz firmy. Oczywiście zdarzenia te w żaden sposób nie powinny uszkodzić systemu, tylko ukazać słabe strony zabezpieczeń. Takie testy dostępne są również na stronach internetowych, można skorzystać z zamieszczonych tam programów, lecz służą one głównie do sprawdzania typowych aplikacji i typowych ich konfiguracji. Jeżeli firma posiada programy pisane specjalnie na jej potrzeby, to takie testy na niewiele się zdadzą. Testy penetracyjne pozwalają śledzić reakcje osób odpowie-

dzialnych za bezpieczeństwo danych i szczelność różnego rodzaju zabezpieczeń. Czasami firmy, które są pewne swoich zabezpieczeń, urządzają konkursy dla hakerów, który z nich podoła zadaniu i np. wyśle wirusa na ich serwer. Wiele firm niestety przegrywa w tej walce i musi przyznać wyższość umiejętnościom „cyberprzestępców". Firma Avecho, świadcząca usługi poczty elektronicznej, podjęła właśnie takie ryzyko i musiała przekazać nagrodę w wysokości 10 tys. funtów za złamanie zabezbieczeń produktu o nazwie GlassWall[10]. Jako ciekawostkę należy odnotować, że umiejętności hakerów czasami służą w słusznej sprawie. Pomogli oni norweskiemu Centrum Kultury i Języka im. Ivara Aasena, którego pracownicy zgubili hasło do bazy danych zawierającej bezcenne informacje o ponad 11 tys. książek. Naukowcy zwrócili się o pomoc do hakerów, by włamali się do bazy danych i odzyskali hasło. Na efekt nie musieli długo czekać. Już po paru dniach dostali ponad 100 maili z propozycjami haseł. W jednym było to prawidłowe i dostęp do informacji został odblokowany[11].

Oprócz testów penetracyjnych stosuje się w audycie testy kontrolne, które wykrywają nieprawidłowości w konfiguracji systemu. Posługując się specjalistycznymi programami, bada się poziom bezpieczeństwa systemu kontroli dostępu, można też wykryć ślady włamań i niewłaściwych działań ze strony użytkowników oraz przeprowadzić kontrolę systemu operacyjnego.

Po zakończeniu audytu firma otrzyma raport o stanie bezpieczeństwa danych zgromadzonych w systemie informatycznym. Jeśli przedsiębiorstwo pozna swoje słabe strony, to może przeprowadzić odpowiednie zmiany w poziomie ochrony informacji. Najlepiej, żeby takie podejście było kompleksowe, czyli zapewniało nie tylko zabezpieczenie dostępu do komputerów, ale też kontrolę przepływu danych, szkolenia pracowników w zakresie bezpieczeństwa informacji itd. W takim wypadku mamy do czynienia z polityką bezpieczeństwa informacji.

Mianem polityki bezpieczeństwa określamy zbiór działań mających na celu osiągnięcie jak najwyższego poziomu bezpieczeństwa. Nie jest to przedsięwzięcie jednorazowe, ponieważ nie da się ustalić raz na zawsze zabezpieczeń systemu. Z dnia na dzień powstają nowe zagrożenia dla stabilnego funkcjonowania firmy i co pewien czas trzeba dokonywać rewizji swej polityki bezpieczeństwa. Organizowaniem i ustanawianiem polityki ochrony danych i informacji powinien zajmować się ktoś z wyższych szczebli kierownictwa, a dotyczyć ona powinna wszystkich pracowników. Bez ich uczestnictwa wszystkie zarządzenia pozostałyby wyłącznie na papierze i ich ustalanie nie miałoby najmniejszego sensu. Oczywiście przygotowanie nawet ogólnych zasad postępowania w celu ochrony informacji nie będzie trwało kilka dni. Jest to proces długotrwały i czasem może się wiązać z dużymi kosztami.

---

[10] S. Górski, *Avecho: kolejne wyzwanie dla hakerów*, „PC World Komputer" 2004, www.pcworld.pl/news/70945.html.

[11] D. Cieślak, *Hakerzy ratują manuskrypty*, „PC World Komputer" 2002, www.pcworld.pl/news/34110.html.

Aby łatwiej było porównywać poziomy bezpieczeństwa systemów informatycznych i móc zaklasyfikować wszystkie standardy bezpieczeństwa, stworzono tzw. standardy bezpieczeństwa. Do najczęściej używanych zalicza się dwa systemy: amerykański – („Pomarańczowa księga") i europejski (ITSEC)[12]. Pierwszy z nich został opracowany przez Narodowe Centrum Bezpieczeństwa Komputerowego w 1983 r. i nazwany „Kryteriami oceny zaufania systemów komputerowych". Wyróżniono w nim cztery poziomy bezpieczeństwa:

poziom D – to całkowity brak zabezpieczeń lub ich najniższy szczebel,

poziom C – zawiera w sobie możliwość rejestracji zdarzeń, możliwe jest także ustalenie uprawnień poszczególnych użytkowników dostępu do plików i przeprowadzania na nich operacji,

poziom B – oznacza wprowadzenie dodatkowych w stosunku do poziomu C zabezpieczeń,

poziom A – oznacza najwyższy stopień zabezpieczenia[13].

Dodatkowo wszystkie poziomy podzielono na klasy, którym przypisano numery w ten sposób, że wraz ze wzrostem bezpieczeństwa zwiększa się numer klasy. Przy klasyfikowaniu do poszczególnych klas i poziomów bierze się pod uwagę:

- politykę bezpieczeństwa,
- identyfikację, kontrolę i sprawdzanie podmiotu,
- ubezpieczenie eksploatacyjne i okres trwałości ubezpieczenia,
- testy sprawdzające system i opis idei bezpieczeństwa systemu.

Europejski system oceny poziomu bezpieczeństwa systemów informacyjnych opracowany został w 1991 r. i jest rozwinięciem wspomnianej „Pomarańczowej księgi". Oprócz poprzednio sprawdzanych cech dodano:

- wierność, która jest rozszerzeniem integralności o wykrywanie i prewencję,
- niezawodność pracy, która gwarantuje dostęp do zasobów systemu w wymaganym czasie,
- wymianę danych, która wiąże się z bezpieczeństwem transmisji[14].

4. Plany i procedury działania w celu bezpieczeństwa informacji

Przedsiębiorstwo musi przygotować komplet planów i procedur, by zabezpieczyć się przed cyberprzestępstwami i ustalić, jakie posunięcia należy wykonać w razie ewentualnego ataku. Takie działania muszą być kompleksowe i zawierać procedury organizacyjne, techniki programowe i zabezpieczenia fizyczne.

W kwestiach organizacyjnych przede wszystkim należy określić zakres kompetencji i odpowiedzialności. Wszyscy użytkownicy muszą być zaznajomieni z procedurami użytkowania systemu informatycznego oraz z konsekwencjami, jakie na nich czekają, gdy naruszą zasady bezpieczeństwa. Szczególną formą ochrony

[12] www. micharaf.republika.tezapbdpr.htm.
[13] Tamże.
[14] Tamże.

należy objąć te informacje, które są kluczowe do funkcjonowania firmy. Gdyby atak na takie dane się powiódł, wówczas konsekwencje dla przedsiębiorstwa mogłyby być naprawdę poważne. Wśród następnych procedur koniecznych do ustalenia jest przekazanie pracownikom odpowiednich reguł wyboru haseł. Jest to jedno z najpowszechniejszych zabezpieczeń przed nieupoważnionym dostępem do danych, więc nacisk na ten aspekt powinien być szczególny.

4.1. Polityka dotycząca haseł dostępu

Hasło dostępu do informacji musi spełniać dwa postulaty: musi być trudne do złamania dla osób postronnych i jednocześnie powinno być łatwe do zapamiętania dla użytkownika. Szczególnie ważne jest to w obecnych czasach, gdy każdy człowiek musi zapamiętać wiele kodów, szyfrów, haseł itp. Pamięć każdego człowieka jest ograniczona i niestety zawodna, dlatego niektórzy użytkownicy systemów informatycznych zapisują sobie hasła dostępu na kartkach i przypinają w pobliżu swoich stanowisk pracy. Jak łatwo się domyślić, takie postępowanie jest bardzo niepożądane ze względu na politykę bezpieczeństwa firmy. Wystarczy wskazać na to, że wiele haseł dostępu do informacji jest wykradanych przez osoby zatrudnione w firmach sprzątających. Kiedy wszyscy pracownicy firmy opuszczą już budynek, to pracę zaczynają sprzątacze i przyklejone pod klawiaturą lub pod podkładką pod myszkę karteczki łatwo padają ich łupem. Ale nie tylko takie działanie jest naganne. Większość haseł jest łatwa do odgadnięcia, ponieważ stanowią je imiona bliskich osób, ulubione miejsca pobytu na wakacjach, nazwy przyrządów znajdujących się na biurku, obraźliwe epitety pod adresem szefa.

Aby hasło spełniało warunek trudności do odgadnięcia przez nieupoważnione osoby, musi charakteryzować się następującymi cechami:

- nie może być za krótkie, gdyż kombinacji takich słów jest niewiele i łatwo będzie można wykorzystać metodę siłową polegającą na próbowaniu kolejnych kombinacji liter, aż do znalezienia tej odpowiedniej (wraz ze wzrostem mocy obliczeniowej ten sposób staje się coraz prostszy),
- przy wpisywaniu go nikt nie może go podejrzeć,
- najlepiej jeżeli hasło będą stanowić kombinacje liter i cyfr (jeszcze lepiej gdy w haśle pojawią się dodatkowo znaki, które znajdują się na klawiaturze, np. „^", „*", „#"),
- w żaden sposób hasło nie powinno zawierać naszych osobistych danych, które można było zdobyć w inny sposób (np. data urodzenia, numer rejestracyjny samochodu),
- powinno być w miarę często zmieniane, gdyż z czasem prawdopodobieństwo wykrycia hasła się zwiększa.

Aby się upewnić, czy użytkownicy mają bezpieczne hasła, można zastosować różne narzędzia. Po pierwsze, można uruchamiać własny tzw. łamacz haseł i wykrywać tych pracowników, którzy nie dobrali odpowiednich haseł. Lepszym

sposobem jest zainstalowanie programu, który sprawdza każde hasło przy pierwszym logowaniu do systemu i nie pozwala na wybranie „słabego hasła".

Nawet najlepsze hasło nie spełni swojego zadania, jeśli pracownik nie będzie znał wagi polityki bezpieczeństwa. Podstawową procedurą są ustawiczne kształcenia użytkowników w kierunku ochrony poufnych danych firmy. Dotychczasowe badania przeprowadzone w Wielkiej Brytanii wskazują, że 70% pracowników jest w stanie wyjawić hasło za czekoladki, a 34% podaje hasło, gdy ich się po prostu o to poprosi. Badania te przeprowadzono na jednej z londyńskich sieci metra. Pocieszające jest to, że rok wcześniej aż 90% badanych podało hasło za tandetny długopis. Najsłynniejszy haker na świecie – Kevin Mittnick – stwierdził, że w większości przypadków nie łamał zabezpieczeń, tylko ludzi. Metodami tzw. inżynierii społecznej można dostać się do systemu informatycznego szybciej i bez wysiłku[15].

Oprócz haseł dostępu przedsiębiorstwo ma jeszcze klika innych technik programowych do wyboru. Są to m.in.:

- kryptografia, czyli stosowanie różnego rodzaju szyfrów w celu uniknięcia nieupoważnionego dostępu do informacji, odbiorca wiadomości, by ją odczytać musi znać kod odszyfrowujący,
- programy antywirusowe,
- podpisy cyfrowe pozwalające zidentyfikować nadawcę komunikatu, co chroni przed wiadomościami od podszywających się pod innych użytkowników,
- bezpieczne protokoły przesyłu uzupełniające powszechne protokoły transmisji i zwiększające bezpieczeństwo podczas przesyłania danych, najpopularniejsze to: SSL (Secure Socket Layer), PGP (Pretty Good Privacy), S-HTTP,
- kontrola dostępu do systemu obejmująca oprócz haseł wprowadzenie kart identyfikacyjnych, systemy biometryczne, ściany zaporowe itd.

Karty identyfikacyjne przypisuje się do konkretnych pracowników i tylko oni mogą przedostać się przez system barier. Z kolei systemy biometryczne wykorzystują charakterystyczne cechy ludzkiego organizmu. Najczęściej jest to badanie linii papilarnych, oka, głosu, twarzy. Systemy te są bardzo skuteczne, ponieważ prawdopodobieństwo, że dwie osoby mają takie same cechy, jest minimalne. Drugą ich zaletą są coraz niższe ceny instalacji takiego systemu w firmie.

Ściana zaporowa (*firewall*) – jest to punkt między dwoma urządzeniami, który kontroluje całość ruchu między nimi i może blokować niektóre ataki ze strony nieupoważnionych osób.

Jak już wspomniałem na początku tego artykułu, polityka bezpieczeństwa kojarzy się głównie z bezpieczeństwem fizycznym. I o nim nie należy zapominać, gdyż obecność na terenie firmy osób nie związanych z nią może spowodować również duże straty. W trakcie pobytu w budynku firmy mogą one ukraść pewne elementy systemu informatycznego, wymienić jego części, zainstalować programy

[15] www. zsi.pwr.wroc.pl/~kazienko/ochrona/.

szpiegujące, fizycznie zniszczyć np. serwer lub urządzenia przesyłowe itp. W celu ochrony przed zniszczeniem najważniejszych danych firma powinna przechowywać ich kopie w miejscu, które jest oddalone od budynków przedsiębiorstwa.

Ważna z punktu widzenia bezpieczeństwa informacji jest również polityka niszczenia dokumentów. Często zdarza się, że aby zdobyć interesujące informacje, wystarczy przetrząsnąć śmieci, które pochodzą z firmy. Dlatego ustalenie mechanizmu niszczenia dokumentów i wyznaczenie do tego odpowiednich osób stanowi ważny punkt ochrony informacji.

5. Wyzwania, jakie stoją przed polityką bezpieczeństwa informacji

W związku z przemianami, jakie dokonują się we współczesnej gospodarce, a związanymi z rozwojem Internetu i procesem globalizacji, firma musi nieustannie modyfikować swoje procedury ochrony informacji i dopasowywać je do nowych ram działalności.

Jeden z ważniejszych problemów to kwestia przenoszenia produkcji do krajów, gdzie koszty są niższe. Grozi to utratą np. zastrzeżonych receptur bądź innych tajemnic handlowych. W innym kraju mogą być odmienne zwyczaje dotyczące bezpieczeństwa informacji i w związku z tym to, co u nas jest uznawane za zachowanie krzywdzące interesy firmy, gdzie indziej wcale nie musi być tak samo postrzegane.

Niebezpieczeństwo wycieku informacji zwiększa się również wraz z popularnością outsourcingu. Przy korzystaniu z takich rozwiązań zmniejszają się koszty działania firmy, dzięki przekazaniu niektórych prac podwykonawcom. Niekiedy wiąże się to z udostępnianiem im niektórych informacji, a to może oznaczać zagrożenie, że nasi partnerzy wykorzystają je kiedyś przeciwko nam. Może się również zdarzyć tak, że jakaś firma na jednym polu działania będzie naszym partnerem, a na drugim – konkurentem.

Coraz popularniejsze staje się również zatrudnianie czasowe, więc w firmie może występować problem nadmiernej rotacji zatrudnionych. Przyjmując ich do pracy, należy na wstępie w umowie zaznaczyć, że pracownik zobowiązuje się do ochrony informacji firmy także po wygaśnięciu umowy o pracę. Nikogo nie dziwi już obecność ochroniarzy przy pakowaniu się zwolnionych pracowników, a cały proces wypowiedzenia pracownikowi umowy o pracę odbywa się jak najszybciej, gdyż taki pracownik stanowi duże zagrożenie dla bezpieczeństwa informacyjnego firmy. Jak wskazują statystyki, pracownicy są powodem największych strat w firmie pod względem niezachowania bezpieczeństwa danych.

Przestępstwa komputerowe są wynikiem:

- błędów człowieka – 50%,
- nieuczciwości pracowników – 10%,
- działań osób niezadowolonych – 9%,
- programów złośliwych – 6%,
- ataków zewnętrznych – 5%.

Następne zagrożenie to rozwój telepracy, czyli pracy wykonywanej w domu, dzięki możliwościom, jakie daje Internet. Podczas pracy w domu dochodzi do zagrożenia, że dane firmy nie będą dostatecznie zabezpieczone przed kradzieżą. To samo dotyczy laptopów. Przenoszenie danych na twardych dyskach komputerów przenośnych naraża na utratę tych danych (oczywiście razem z zapisanymi danymi traci się sprzęt i oprogramowanie).

6. Podsumowanie

Sprawa bezpieczeństwa informacji nabiera coraz większego znaczenia. Straty wynikające z niedostatecznie zabezpieczonego systemu informatycznego mogą być niewspółmiernie duże w porównaniu z nakładami, jakie trzeba ponieść, by zapewnić odpowiedni poziom zabezpieczeń.

W kwestii ochrony informacji nie można nigdy być przekonanym o całkowitym bezpieczeństwie. Działa tu zasada sprzężenia zwrotnego, nigdy nie będziemy mogli zakończyć prac nad zapewnianiem bezpieczeństwa informacji, gdyż osoby zainteresowane atakiem na nas będą próbować innych sposobów, by dopiąć celu. Również pod względem kosztów nie opłaca się likwidować wszystkich dziur w systemie, gdyż pochłonęłoby to zbyt wiele pieniędzy. Nie można zlikwidować ryzyka, ale należy je minimalizować.

Przedsiębiorstwo powinno prowadzić defensywną politykę zgodnie z ogólnymi jej zasadami, czyli zapobiegać wszelkim atakom, dzięki metodom wymienionym w tej publikacji. Należy również odstraszać potencjalnych przestępców zapowiedziami kar za ewentualne próby ataku (lub wywieraniem wpływu na organy rządzące, które mogą odstraszać przestępców, wprowadzając wysokie kary za ataki na systemy informatyczne firm). Kolejna procedura w obronnej polityce to wskazywanie i ostrzeganie, czyli zbieranie informacji o atakach na inne podmioty rynkowe. Nie trzeba się uczyć tylko na własnych błędach, wiadomości o atakach na systemy innych firm mogą przedsiębiorstwu przynieść wymierne korzyści w postaci szybciej zabezpieczonego zasobu informacji. Następny element defensywnej wojny informacyjnej to wykrywanie ewentualnych ataków. Zastosowane techniki muszą pozwolić na ujawnienie ataku, na tyle sprawnie, żeby na nie zareagować. Po tym całym zbiorze działań przychodzi czas na refleksje i zreorganizowanie obrony systemu informatycznego pod kątem ostatnich ataków. I trzeba zawsze pamiętać, że siła systemu informatycznego jest mierzona odpornością jego najsłabszego ogniwa.

Literatura

Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003.

Cieślak D., *Hakerzy ratują manuskrypty*, „PC World Komputer" 2002, www.pcworld.pl/news/34110.html.

Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.
Forlicz S., *Niedoskonała wiedza podmiotów rynkowych*, PWN, Warszawa 2001.
Forlicz S., *Mikroekonomiczne aspekty przepływu informacji między podmiotami rynkowymi*, WSB, Poznań, 1996.
Górski S., *Avecho: kolejne wyzwania dla hakerów*, „PC World Komputer" 2004, www.pcworld.pl/news/70945.html.
Krusiński W., Ścibor M., *Plusy i wirusy*, „Polityka" 2004, nr 44.
Kukliński A., *Gospodarka oparta na wiedzy – wyzwania dla Polski*, KBN, Warszawa 2001.
Kwiatkowski S., *Przedsiębiorczość intelektualna a trwały rozwój gospodarczy krajów posocjalistycznych*, [w:] *Nowa gospodarka i jej implikacje dla długookresowego wzrostu w krajach postsocjalistycznych*, red. G. Kołodko, WSPiZ, Warszawa 2001.
Pipkin D., *Bezpieczeństwo informacji*, WNT, Warszawa 2002.
Rattray G.J., *Wojna strategiczna w cyberprzestrzeni*, WNT, Warszawa 2004.
Toffler A., *Szok przyszłości*, Zysk i S-ka, Poznań 1998.
www.idg.pl/news/39709.html.
www.micharaf.republika.tezapbdpr.htm.
www.zsi.pwr.wroc.pl/~kazienko/ochrona/.

THE ROLE OF INFORMATION SECURITY IN A COMPANY IN TERMS OF INTERNET SPREADING

Summary

The article takes up the problem of information security, which is crucial for companies nowadays. This issue has a big importance in terms of Internet spreading. Wide range of Internet appliances results in many changes in company's activities. The global network is a facilitation for information processes, but it also poses a threat for information security. The article mentions the most important aspects of information security and types of threats that appear in companies' information systems. Different kinds of attacks are divided into groups depending on their source and attacker's intentions. The author also assigns economical consequences of every mentioned type of attack.

The last part of the article introduces basic rules of information security policy in a company.

Mgr Tomasz Galewski jest pracownikiem Katedry Ekonomii Matematycznej Akademii Ekonomicznej we Wrocławiu.