Celem opracowania jest zwrócenie uwagi czytelnika na złożoność problemu zagrożeń dotyczącego utraty w nie zamierzony sposób danych informacyjnych, wskazanie konkretnych zagrożeń, jak również możliwości ich analizy oraz poprawnego definiowania. Znajduje się w nim odwołanie do podstaw systemowego zarządzania ryzykiem związanym z utratą danych, dotyczące teorii ochrony przed zagrożeniami w branży ICT (*Information and Communications Technologies*) oraz każdej organizacji dostrzegającej wartość i znaczenie informacji oraz danych.

Jacek
ŁUCZAK

Systemy zarządzania bezpieczeństwem informacji (ISMS)

Każda działalność gospodarcza obarczona jest ryzykiem. Zawsze istnieje możliwość pojawienia się praktycznego zagrożenia; w zależności od rodzaju i charakteru prowadzonej działalności będzie ono przybierało różną formę. Zagrożenie może się pojawić w postaci np. opóźnionej dostawy podzespołów od dostawcy, czy też awarii procesora sterującego linią produkcyjną, ale również – napadu z bronią w ręku, a coraz częściej kradzieży wartości intelektualnych firmy – różnego typu danych i informacji gospodarczych.

Zasadnicze przesłanie niniejszego artykułu sprowadza się do zwrócenia uwagi na niedostrzeganą jeszcze sferę zarządzania jakością, której dalsze niedocenianie może sprowadzić katastrofę na producentów i usługodawców, jak również samych klientów. Niewiele sytuacji kryzysowych firmy można porównać z utratą informacji. Tym bardziej, że jak dowodzi praktyka są to przypadki coraz częstsze i niestety trudne do wykrycia. A nawet wykryte i jednoznacznie napiętnowane, powodują nieporównywalne z innymi sytuacjami zagrożenia. Nietrudno wyobrazić sobie następstwa prawne, finansowe, czy utratę wiarygodności przedsiębiorstwa, które dopuściło do niekontrolowanego dostępu osób trzecich do bazy adresowej znaczącego klienta.

Systemowe zarządzanie bezpieczeństwem informacji (Information Security Management Systems – ISMS) nabiera szczególnego znaczenia w dobie informacji, kiedy jest ona najważniejszym aktywem każdej organizacji.

Wprowadzenie

Bezpieczeństwo informacji i danych, w polskich firmach nie należy do grupy zagadnień traktowanych jako podstawowe w kształtowaniu strategii zarządzania, jak również codziennej pracy. Doświadczenia firm światowych w tym względzie nie do końca są znane, skoro podanie do wiadomości faktu związanego z utratą baz danych może w istotny sposób podważyć zaufanie klientów. Można spróbować jednak oszacować straty przedsiębiorstw związane z kradzieżą wartości intelektualnych.

Także w Polsce staje się powszechne zjawisko kradzieży firmowej własności intelektualnej. Rodzime organizacje, w zdecydowanej większości przypadków bagatelizują znaczenie właściwego podejścia w ich zabezpieczenia, kiedy wiodące organizacje światowe traktują systemowe rozwiązania dotyczące bezpieczeństwa informacji, jako podstawę działalności rynkowej. Coraz częściej także klienci domagają się gwarancji bezpieczeństwa powierzanych danych, czy też informacji dotyczących zlecanych do realizacji przedsięwzięć.

Wyłącznie odosobnione polskie przedsiębiorstwa rozwijają politykę bezpieczeństwa informacji, traktując ją jako element systemowego zarządzania jakością. Normy ISO serii 9000 wprost nie stawiają jednoznacznych wymagań w powyższym zakresie, ogólnie określone zostały natomiast, np. przez Wielką Trójkę w standardzie QS-9000 (podobnie VDA 6.1, ISO 16494), w zbiorze wymagań systemowych dostawców na rynek aeronautyki AS9000, czy telekomunikacji TL 9000, bardzo pośrednio w innych standardach.

Można zwrócić uwagę natomiast, że naturalnym dążeniem wielu organizacji jest zapewnienie bezpieczeństwa informacji, bowiem one właśnie stanowią podstawę realizowanej działalności. Obok pytań związanych z zagwarantowaniem satysfakcji klientów, pojawiły się już także pytania o wiarygodność i bezpieczeństwo procedur zarządzania. Można wskazać zaledwie kilka przypadków na polskim rynku, kiedy instytucje finansowe, czy też przetwarzające bazy danych klientów wdrażają systemy zgodne z międzynarodowymi normami ISO serii 9000, stawiając sobie za cel

wiodący, a przynajmniej jeden z celów – bezpieczeństwo danych.

Właśnie takie potrzeby i uświadomienie, że informacja jest jednym z najcenniejszych zasobów każdej organizacji przyczyniły się do wykreowania brytyjskiego standardu BS 7799, oraz podobnych – przede wszystkim szwedzkiego SS 62 77 99.

Podstawy systemowego zarządzania bezpieczeństwem informacji

Na początku lat 90., Brytyjski Instytut Normalizacji BSI (British Standards Institution) przedstawił na forum publicznym opracowanie dotyczące zarządzania bezpieczeństwem informacji w przedsiębiorstwach, określone jako PD0003. Inicjatywa, w której popularność na początku wątpili sami twórcy wzbudziła ogromne zainteresowanie przedstawicieli wielu organizacji. Tezy i przesłanie jakie niosła w sobie powyższa norma, skłoniły BSI do podjęcia nowych prac, w efekcie których opracowano zbiór praktycznych porad, wydany w 1995 roku jako norma BS 7799 Code of practice for Information Security Managemen.

Na poszczególnych etapach opracowania ostatecznej wersji standardu wykorzystywane były doświadczenia i praktyki ochrony informacji stosowane w wielu znanych międzynarodowych firmach, m.in. Shell, Unilever, BT, Midland Bank, Marks and Spencer, Nationwide Building Society.

W obecnej chwili podstawową systemowych rozwiązań w zakresie bezpieczeństwa informacji w skali świata jest właśnie norma brytyjska. Jednak wbrew powszechnej opinii nie dotyczy ona wyłącznie branży ICT (*Information and Communications Technologies*), a zgodnie z założeniami powinna spotkać się ze znacznie szerszym zainteresowaniem.

U źródeł opracowania założeń systemów zarządzania bezpieczeństwem informacji leżał krytyczny stosunek do stosowanych w tym względzie praktyk, w szczególności do ich powszechności. Wiodącą rolę w zakresie kreowania nowych zasad odegrał rząd brytyjski. Przeważającą większością głosów polityków brytyjskich, wszystkie organizacyjne systemy informacyjne powinny zostać objęte systemem zgodnym z BS 7799 oraz zostać poddane certyfikacji do końca marca 2001. E-commerce przestało być teoretyczną koncepcją działalności gospodarczej, staje się aspektem gospodarki rozwijającym się szybciej i intensywniej, niż można było wcześniej przypuszczać. W Wielkiej Brytanii w ostatnim roku zanotowany został 40% wzrost wykorzystania internetu w działalności gospodarczej firm i 37% w zakresie wykorzystania serwisów www (w tym samym czasie odpowiednio 5 i 11% w USA); 38% podmiotów brytyjskich deklaruje zainteresowanie e-biznesem. Rząd Wielkiej Brytanii powziął ambitny cel do osiągnięcia w 2002 roku, dotyczący ustanowienia w UK najlepszego na świecie „środowiska" dla prowadzenia handlu elektronicznego.

Zgodnie ze słowami min. Michaela Willsa, wszystkie organizacje na całym świecie będą wykorzystywały standard BS7799 – standard opracowany przez przemysł dla przemysłu[1].

Norma BS 7799

Norma stanowiąca podstawę systemów zarządzania bezpieczeństwem informacji została opracowana przez BSI-DISC, strukturę BSI funkcjonującą pod nazwą BDD/2 Information Security Management. BDD/2 skupia przedstawicieli wielu organizacji brytyjskich, żywo zainteresowanych rozwojem e-biznesu.

BS 7799:1999 to dwuczęściowa norma:

- BS 7799-1:1999 – standardowy kodeks praktyki, katalog zagadnień, jakie należy realizować dla potrzeb bezpieczeństwa informacji (*Code of practice for Information Security Managemen*);
- BS 7799-2:1999 – standardowa specyfikacja dla systemów zarządzania bezpieczeństwem informacji (ISMS – Information Security Management Systems).

BS 7799-1:1999

BS 7799-1:1999 definiuje 127 elementów kontroli i sterowania bezpieczeństwem informacji, podporządkowanych 10 grupom wymagań, co pozwala użytkownikom na zidentyfikowanie najwłaściwszych zabezpieczeń w kontekście specyfiki działalności, jaką prowadzą oraz otoczenia rynkowego i potrzeb w powyższym zakresie. Wykorzystywane narzędzia sterowania i kontroli zawierają dalsze szczegółowe techniki uznawane jako najlepsza praktyka w tym względzie.

Aktualne, drugie wydanie normy kładzie szczególny nacisk na zarządzanie ryzykiem, wskazuje także, że użytkownik nie jest zobowiązany do wdrażania wszystkich technik przywołanych w części pierwszej standardu, tylko uznanych za najistotniejsze i zapewniające realizację celów. Katalog dotyczy wszystkich form informacji, w tym także ustnych i graficznych, powstających z wykorzystaniem telefonów komórkowych i faksów. Standard uwzględnia najnowsze formy działalności gospodarczej, np. e-commerce, internet, outsourcing, teleworking, mobile computing. Międzynarodowe aspiracje brytyjskiej normy podkreśla fakt, że specyfika rynku brytyjskiego została przywołana w załączniku, a nie w treści samej normy. Na przełomie października i listopada 1999 roku rozpoczęły się formalne prace zmierzające do opracowania adekwatnego, międzynarodowego standardu (ISO).

BS 7799-2:1999

Zawarte w normie BS 7799-1 wymagania znalazły uznanie w wielu firmach brytyjskich. W oparciu o nabyte doświadczenie w BSI rozpoczęto prace nad kolejnym dokumentem normalizacyjnym BS 7799-2 Specification for Information Security Management Systems. Celem przyświecającym twórcom drugiej części standardu było stworzenie formalnych podstaw dla uruchomienia mechanizmu certyfikacji istniejących sy-

[1] z wypowiedzi ministra Michaela Willsa na Infosec`99

Etap	Opis
1.	Opracowanie polityki bezpieczeństwa informacji i danych.
2.	Określenie zakresu projektowanego systemu zarządzania bezpieczeństwem informacji (ISMS).
3.	Ocena ryzyka – identyfikacja zagrożenia utraty aktywów informacyjnych i danych, słabości oraz nastawienia organizacji dla określania ryzyka.
4.	Zarządzanie ryzykiem z wykorzystaniem przystających elementów z BS 7799-2.
5.	Opracowanie bilansu adekwatności (Statement of Applicability) – zapisy wskazują na wybór określonych elementów BS 7799 oraz przyczyny uznania za nieodpowiednie pozostałych.
6.	Udokumentowanie procedur dotyczących zarządzania i elementów operacyjnych ISMS wskazujących na odpowiedzialności oraz podstawowe działania.

Tab. 1. Etapy projektowania i wdrażania ISMS. Źródło: opracowanie na podstawie BS 7799-2

stemów ochrony bezpieczeństwa informacji. Przewiduje się, że w ramach procesu certyfikacji sprawdzany będzie aktualnie działający w danej firmie system ochrony bezpieczeństwa informacji na zgodność z sugestiami zawartymi w normie BS 7799.

BS 7799-2:1999 ilustruje, w jaki sposób zaprojektować, wdrożyć i poddać certyfikacji system zarządzania bezpieczeństwem informacji (ISMS – Information Security Management Systems). Norma wskazuje na sześcioetapowy proces kreowania i wdrożenia zaprojektowanych rozwiązań (tab. 1); odwołuje się do konieczności określenia wszystkich aktywów informacyjnych i oszacowania ich istotności dla organizacji.

Standard zawiera także dodatkowe wymagania dotyczące struktury, zarządzania i administrowania ISMS.

Przewodniki związane z BS 7799

Jednocześnie w ostatnim czasie dokonana została rewizja przewodników związanych z normą BS 7799:

- PD 3001 – Przygotowanie do certyfikacji BS 7799;
- PD 3003 – Czy jesteś gotowy do auditu BS 7799?;
- PD 3004 – Przewodnik do auditowania BS 7799.

Do rodziny dokumentów związanych z normą BS 7799 należy zaliczyć także wcześniej opracowane przewodniki i pozostające bez zmian:

- PD 3000 Zarządzanie bezpieczeństwem informacji. Wprowadzenie;
- PD 3002 Przewodnik do BS 7799. Ocena i zarządzanie ryzykiem;
- PD 3005 Przewodnik wyboru elementów BS 7799.

Organizacja i wymagania BS 7799

Norma BS 7799-1 została podzielona na dziesięć podstawowych części tematycznych odnoszących się do polityki i organizacji bezpieczeństwa IT w firmie. Kolejne rozdziały przedstawiają konkretne propozycje rozwiązań w następujących obszarach:

- polityka bezpieczeństwa informacji w firmie;
- organizacja systemu bezpieczeństwa informacji;
- klasyfikacja oraz nadzór środków i zasobów wykorzystywanych dla realizacji polityki bezpieczeństwa;
- polityka bezpieczeństwa w odniesieniu do polityki kadrowej i metod rekrutacji pracowników;
- techniczne środki ochrony i kontroli dostępu do obiektów i pomieszczeń w odniesieniu do bezpieczeństwa danych i infrastuktury IT;
- formy i zasady korzystania z sieci i komputerów w firmie w odniesieniu do polityki bezpieczeństwa;
- zasady kontroli i monitorowania dostępu do systemów i informacji;
- utrzymanie, rozwój i rozbudowa systemu w odniesieniu do polityki bezpieczeństwa;
- planowanie strategii firmy wobec zagrożeń krytycznych;
- ochrona danych, a regulacje prawne i wymogi formalne.

Każda z części zawiera od kilku do kilkunastu rozdziałów odnoszących się do zakresu określonego w tytule. Dla przykładu, w części poświęconej środkom i zasobom norma zwraca uwagę na konieczność posiadania dokładnej informacji na temat posiadanych przez firmę komputerów czy nawet biurek. Informacja powinna zawierać szczegóły odnośnie tego, kto jest odpowiedzialny za serwis, a kto jest stałym użytkownikiem; kto może korzystać z określonych zasobów incydentalnie i w jakich sytuacjach. W normie przedstawiony został przykład, jakie środki i zasoby powinny zostać zakwalifikowane do systemu informacyjnego organizacji i jak należy je zaklasyfikować np.:

- bazy danych, kartoteki, dokumentacja systemu, podręczniki użytkownika, materiały szkoleniowe oraz procedury powinny zostać sklasyfikowane jako informacje;
- oprogramowanie użytkowe, systemowe oraz narzędziowe powinno zostać sklasyfikowane jako oprogramowanie;
- komputery, urządzenia telekomunikacyjne, drukarki, zasilacze, UPS'y, meble itp. jako wyposażenie;
- usługi centrum obliczeniowego, łączności czy np. służby utrzymania klimatyzacji jako usługi.

Bazując na informacjach zebranych w trakcie inwentaryzacji środków i zasobów firmy, norma sugeruje, w jaki sposób połączyć konkretny środek lub zasób z odpowiednim poziomem jego ochrony – generalna zasada brzmi, że ochronie podlega wszystko, ale w

różnym stopniu. W odniesieniu do środków i zasobów określonych jako informacje, określony powinien zostać adekwatny poziom ochrony przy uwzględnieniu trzech potrzeb dotyczących specyfiki organizacji i rynku na jakim działa:

- tajności – czyli potrzeby posiadania mechanizmu utajniania wybranych, czy wszystkich informacji;
- spójności – czyli potrzeby posiadania mechanizmu utrzymywania starych i nowych informacji w stanie pozwalającym na zagwarantowanie ich spójności;
- dostępności – czyli potrzeby kontrolowanego i jednocześnie pełnego dostępu do posiadanych informacji.

Istotne jest także zwrócenie uwagi na wskazanie w normie, że nie istnieje ogólnie akceptowany standard nazywania i oznaczania informacji uznanych za tajne czy poufne, i jest to sprawa indywidualna dla każdej organizacji.

W innym fragmencie normy zwraca się szczególną uwagę na konieczność budowania świadomości wdrażanego systemu ochrony informacji wśród samych pracowników. Przedstawione tam sugestie odnośnie naboru pracowników na określone stanowiska dokładnie określają cel – minimalizację ryzyka wystąpienia zagrożenia wynikającego z błędów popełnianych przez ludzi.

Wszystkie aspekty zarządzania bezpieczeństwem informacji w firmie poruszone w standardzie i wynikające z nich problemy wymuszają na kadrze kierowniczej bardzo dobre przygotowanie do realizacji zamierzonego celu. Z praktycznego punktu widzenia, każda z osób odpowiedzialnych za wdrożenie systemu zarządzania bezpieczeństwem informacji w danej firmie stanie przed problemem identyfikacji, definicji i analizy zagrożeń. Pełen obraz mapy zagrożeń jest etapem wstępnym przed rozpoczęciem wdrażania sugestii przedstawionych w normie BS 7799.

BS 7799 a ISO

Norma brytyjska 7799-1 została zgłoszona przez BSI do Międzynarodowej Organizacji Normalizacyjnej – ISO jako podstawa ustanowienia międzynarodowego standardu zarządzania bezpieczeństwem informacji. Nadany został jej numer ISO/ IEC 17799-1 i uruchomiona została uproszczona procedura legislacyjna, tzw. fast – track. W tym przypadku przewidziany czas na tajne głosowanie to sześć miesięcy, który rozpoczął się 3 lutego i zakończył 3 sierpnia bieżącego roku.

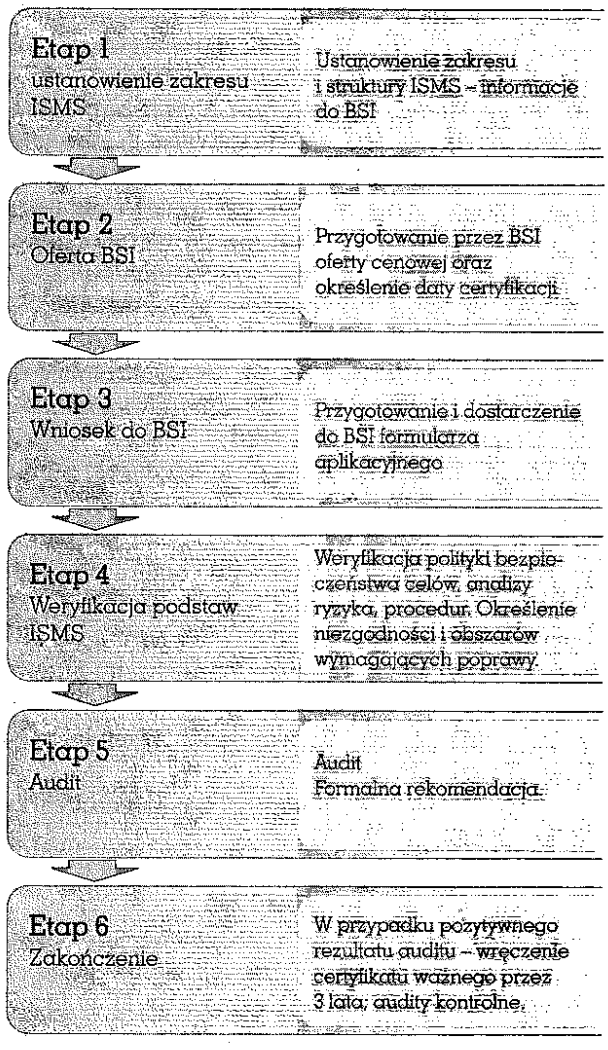
Z założenia procedura fast – track może zakończyć się przyjęciem projektu bez zastrzeżeń, dezaprobatą ze wskazaniem na możliwości dokonania zmian lub odrzuceniem.

Dla ważności rozstrzygnięć i przyjęcia normy, zgodnie z założeniami procedury fast – track, konieczne jest spełnienie czterech kryteriów:

- przynajmniej $^1/_3$ członków wyrazi aprobatę,
- nie więcej jak $^1/_4$ głosów nie wyrazi dezaprobaty,
- nie będzie głosów wstrzymujących,
- 50% członków musi głosować na proces w uznaniu jego ważności.

c:cure

Enigmatycznie brzmiąca nazwa c:cure jest brytyjską procedurą akredytowanej certyfikacji systemów zarządzania bezpieczeństwem informacji (ISMS) zgodnych z BS 7799. Procedura została pierwotnie ustanowiona w 1998 przez Ministerstwo Handlu i Przemysłu Wielkiej Brytanii, jest natomiast rozwijana przez BSI-DISC[2]. Procedura zobowiązuje jednostki certyfikujące do poddania się procesowi krajowej akredytacji w zakresie realizowanej działalności. Zgodnie z założeniami c:cure auditorzy powoływani przez jednostki certyfikujące są wcześniej akredytowani zgodnie z określonymi kryteriami przyjętymi przez International Register of Certified Auditors (IRCA).



Rys. 1. Certyfikacja systemu zarządzania bezpieczeństwem informacji (ISMS). Źródło: materiały źródłowe BSI – DISC, 2000.

[2] DISC jest strukturą wewnętrzną British Standards Institution odpowiedzialną za rozwój i publikację BS 7799 oraz sprawującą za zgodą Ministerstwa Przemysłu i Handlu Wielkiej Brytanii nadzór nad procedurą c:cure.

Do końca czerwca bieżącego roku akredytację United Kindom Accreditation Service zgodną z przewodnikiem ISO 62 (EN 45012) na prowadzenie certyfikacji BS 7799 uzyskało sześć organizacji, przy czym, cztery z nich uzyskały akredytację na c:cure:

- BSI Quality Assurance – BS 7799;
- Bureau Veritas Quality International Ltd – BS 7799 oraz c:cure;
- Lloyd`s Register Quality Assurance Ltd– BS 7799 oraz c:cure;
- Det Norske Veritas Quality Assurance Ltd – BS 7799 oraz c:cure;
- National Quality Assurance Ltd – BS 7799 oraz c:cure;
- SGS Yarsley International Certification Service Ltd – BS 7799.

Przeznaczenie BS 7799

Zdecydowanie potrzeba systemowego ograniczania ryzyk związanych z niezamierzonym dostępem do zasobów informacyjnych osób trzecich dotyczy znacznie szerszego grona organizacji, niż tylko związanych z IT.

Dla zobrazowania powyższej tezy można powołać się na źródłowe informacje BSI, związane z odpowiedzią na pytanie: Dlaczego konieczne jest zainteresowanie BS 7799:

- norma jest zbiorem praktycznych wskazówek, powstała jako odpowiedź na żądania wysuwane przez firmy różnych branż i sektorów przemysłu, co do określenia metod walki z narastającą falą zagrożeń płynących z postępującej informatyzacji życia (np. szpiegostwo przemysłowe, defraudacja, zwykłe przypadki kradzieży czy awarii systemów informatycznych);
- w środowiskach otwartych systemów ICT i w dobie elektronizacji handlu standard daje możliwość wprowadzenia bardzo dobrych podstaw dla tworzenia sprawnych systemów zarządzania bezpieczeństwem informacji;
- standard jest niezbędnym i najistotniejszym elementem, w oparciu o który buduje się bezpieczeństwo w rozproszonych i współdzielonych systemach teleinformatycznych. Standard gwarantuje partnerom, dostawcom i odbiorcom końcowym bezpieczeństwo wymienianych między sobą informacji.

Istotne jest jednak skomentowanie powyższej argumentacji, która przykłada szczególną wagę do zagrożeń zewnętrznych, powszechnie uznawanych za najbardziej niebezpieczne. W praktyce jednak, gdy system ICT łączy wiele firm w jeden organizm (systemy EDI – Electronic Data Interchange), mamy do czynienia z modelem, dla którego przede wszystkim należy mówić o analizie zagrożeń wewnętrznych. A zatem nie tylko partnerzy rynkowi, dostawcy i odbiorcy mogą stanowić potencjalne zagrożenie dla informacji gospodarczych, bowiem równie istotne są zagrożenia wewnętrzne, związane z pracownikami.

Mapy zagrożeń każdej organizacji można zbudować z czterech podstawowych elementów:

- pracowników, czyli nas samych;
- procesów, którymi zarządzamy;
- technologii, które wykorzystujemy
- oraz struktury organizacyjnej, której się podporządkowujemy będąc jej elementami.

Każdy z przedstawionych elementów może stanowić dla nas potencjalne źródło zagrożeń wewnętrznych.

Systemy informacyjne w tym, np. teleinformatyczne przez swoją specyfikę oraz możliwość łączenia się bez względu na odległość i porę dnia muszą być traktowane w kategorii zagrożeń wewnętrznych oraz zewnętrznych – każda organizacja musi indywidualnie zdecydować ostatecznie, jaka rola zostanie im przypisana.

Dlatego właśnie analizując istotę standardu BS 7799 można powiedzieć, że zawarte w nim regulacje powinno się traktować jako uniwersalne dla każdego typu organizacji i każdego systemu informacyjnego.

Przy tworzeniu normy założono, że będzie ona przeznaczona dla osób odpowiedzialnych za określanie, wprowadzanie i zarządzanie mechanizmami ochrony informacji w przedsiębiorstwach, a zawarte w niej informacje powinny być traktowane jako wytyczne dla określania własnych standardów ochrony. W wielu opracowaniach podkreśla się, że cechą zawartych w dokumencie wskazówek jest ich zwięzłość i uniwersalność oraz, że zakres poruszonych problemów pokrywa najczęstsze przypadki spotykane w codziennej pracy organizacji wszelkich branż.

Podsumowanie

Coraz częściej, jednak nadal zbyt rzadko, zwraca się uwagę na najistotniejsze zasoby każdej organizacji. Bez wątpienia w każdym przypadku są to dane – na różnych nośnikach i w różnej formie. Nie można przecenić znaczenia faktu utraty informacji związanych z kontraktem handlowym, bazy danych klientów, planu produkcyjnego, czy założeń biznesplanu. Zagrożenia w tym przypadku mogą pochodzić tak z zewnątrz firmy, jak również od samych pracowników.

W tym kontekście niepokojące są ogłoszenia w internecie wskazujące na możliwości dokonania zakupu kompletnej bazy danych dużego klienta, czy też coraz częstsze ataki hakerów na zasoby bardzo różnych instytucji. Wbrew powszechnej opinii, hakerzy to nie tylko zdolna młodzież, a jeżeli nawet, to do czego są zdolni szkoleni w tym zakresie specjaliści.

W raportach PricewaterhouseCoopers można przeczytać opinię, że w Polsce powszechne staje się zjawisko kradzieży firmowej własności intelektualnej, a menedżerowie albo nic o niej nie wiedzą albo bagatelizują rozmiary szkody, albo celowo tają takie przypadki z uwagi na opinię rynkową.

Należy się także spodziewać, że w większości przypadków informacje wyciekają z firmowych zasobów kropla po kropli, a sprawcy w znaczący sposób ograni-

czają ryzyko związane z ujawnieniem przestępstwa[3]. Bardzo wiele wirusów to, tzw. wirusy śledzące (konie trojańskie)[4], które umożliwiają monitorowanie zawartości dysków lokalnych czy poczty elektronicznej. W internecie znajdują się programy służące łamaniu haseł.

Nonszalanckie podejście większości firm do ochrony własnych zasobów informacyjnych, będzie się zmieniało w miarę ujawniania kolejnych przypadków kradzieży własności intelektulnej, a przede wszystkim uświadamiania rozmiarów szkód. Jak podaje Forrester Research, w Stanach Zjednoczonych przeciętne włamanie do poufnych danych firmy kosztuje ją 365 tysięcy USD. W przypadku instytucji finansowych, straty wahają się od 2 – 40 mln USD![5]

Błędy w zakresie ochrony danych popełniane są na każdym kroku: nie uporządkowanie biurka po dniu pracy, nie wykorzystywanie niszczarek dokumentów, lekceważenie rotacji haseł i zachowania ich tajności, niekontrolowany dostęp pracowników do internetu, niesprawdzeni pracownicy służb czyszczących i inne. Upowszechniającą się plagą są wirusy komputerowe. Szczególnie niepokojąca jest globalizacja problemu; np. wirus I love you.

W obliczu groźby ataku z wielu kierunków: ze strony hakera, konkurenta rynkowego, czy nawet wywiadu gospodarczego czy państwowego, skuteczna obrona nie jest rzeczą prostą. Zabezpieczenie danych wymaga nakładów, jednak w pierwszej kolejności wyobraźni. Można na przykład wydać setki tysięcy złotych na sprzęt i oprogramowanie w celu ochrony sieci przed niepożądaną ingerencją z zewnątrz, a jednocześnie tolerować korzystanie z modemów przez pracowników.

Z założenia system zarządzania jakością powinien osiągać cele zewnętrzne – zadowolenie klientów, jak również wewnętrzne – zróżnicowane w zależności od charakteru organizacji oraz rynku, na jakim działa. ISMS jest mechanizmem pozwalającym zarządzać oraz chronić wszystkie aktywa informacyjne poprzez zapewnienie ich poufności, integralności oraz dostępności danych i informacji. Wdrażanie systemu zarządzania bezpieczeństwem informacji związane jest w pierwszej kolejności z dbałością o zapewnienie podstaw bezpiecznego funkcjonowania firmy. I tak np. czy jest możliwe wprowadzenie nowej technologii bez dokonania analizy ryzyka, jakie z tym przedsięwzięciem się wiążą. Na takich samych zasadach niezbędne wydaje się dokonanie analizy ryzyka związanego z utratą różnego typu danych i informacji. Powyższe założenia w istotny sposób wpływają również na satysfakcję klienta, bowiem tylko systemowe rozwiązania w zakresie bezpieczeństwa informacji mogą spowodować, że firma zrealizuje postanowienia umowne. Co więcej w wielu przypadkach dane powierzone przez klientów, stanowią znacznie większą wartość niż samo zlecenie. Tak jest np. w przypadku firm pracujących na bazach danych klientów.

[3] Dopiero we wrześniu 1998 r. wprowadzono do polskiego kodeksu karnego przestępstwo przeciwko informacji (art. 266 – 269 kk.)

[4] z ich wykorzystaniem, w czerwcu tego roku, nieznani sprawcy ukradli z serwerów America Online numery kart kredytowych klientów.

[5] na podstawie Forrester Research Raport 1999

Literatura:

1. BS 7799 – 1 Code of practice for Information Security, 1999.
2. BS 7799 – 2 Specyfication for Information Security Managemet Systems, 1999.
3. EC DGX III/ 07 ETSII Project SEDUCER (23186).
4. materiały źródłowe BSI.
5. Materiały szkoleniowe BS 7799 Risk Assesment Workshop, ODI 2000.
6. M. Oldegard, Applying the management system approach to information security and working conditions in Sweden, ISO News, vol. 9, no. 3 may/ June 2000.
7. Forrester Research Raport 1999.
8. PD 3001 Preparing for BS 7799 certification.
9. PD 3003 Are you ready for a BS 7799 audit?
10. PD 3004 Guide to BS 7799 auditing.
11. c:cureworld newsletter, BSI – DISC, summer 99.
12. The c:cure survey 1999, BSI – DISC, 2000.
13. E. Stankunowicz, Nie śpij bo cię okradną, Businessman Magazine, sierpień 2000.

W następnych numerach:

- Zarządzanie przez jakość w polskich firmach
- Kontroling jakości
- Jakość produktu
- Ergonomia w systemie zarządzania jakością