Przeprowadzone w 1999 roku w Wielkiej Brytanii badania związane z popularnością ISMS opartych o BS 7799 oraz gotowością do akredytowanej certyfikacji c:cure wskazują na nieuświadomioną do końca potrzebę, systemowego bezpieczeństwa informacji.*

Jacek **ŁUCZAK**

Zarządzanie bezpieczeństwem informacji

Użyteczność rozwiązań opartych na standardzie BS 7799 i podobnych oraz zasadność ich stosowania ma swoje dwa podstawowe źródła, pierwsze to zdrowy rozsądek nakazujący ochronę zasobów informacyjnych, drugi to zapewnienie zgodności z prawem. (W polskich warunkach ustawa o ochronie danych osobowych z 29 sierpnia 1997 roku, czy też najpopularniejsza w Europie – Data Protection Act ustanowiona w Wielkiej Brytanii).

Dokumentacja systemu zarządzania bezpieczeństwem informacji – ISMS

Podobnie jak w systemach zarządzania jakością, środowiskiem czy bezpieczeństwem pracy (zgodnymi z normami ISO 9001, QS-9000, TL9000, ISO 14001, PN-N 18001) ISMS musi być w pierwszej kolejności udokumentowany. I podobnie, najważniejszą rolę w tym względzie odgrywają procedury ISMS. Udokumentowanie zasad postępowania pozwala na ich powtarzalną realizację i weryfikację np. w trybie auditów, w tym przypadku auditów bezpieczeństwa.

W trakcie realizacji założonej polityki bezpieczeństwa firmy, m. in. wszystkie operacje wykonywane przez użytkowników w czasie pracy z systemem powinny zostać precyzyjnie udokumentowane. Szczegółowość dokumentacji nie jest w normie BS 7799 jednoznacznie określona. Przy tym przyjmuje się jednak założenie, że powinna zostać zaprojektowana i przygotowana w taki sposób, aby po poprawnym wdrożeniu formalnych procedur gwarantowały one pełne bezpieczeństwo systemu jako całości. Formalne procedury ISMS tworzone w ramach systemu bezpieczeństwa powinny obejmować takie aktywności jak, m.in.: rozwój systemu informatycznego, jego utrzymanie w ruchu (uruchamianie oraz zatrzymywanie systemu, archiwizacja danych, zasady obsługi sprzętu itd.), ochrona i kontrola dostępu do wyznaczonych obiektów, działanie w sytuacjach awaryjnych i inne.

Procedury związane z podstawowymi działaniami obejmującymi planowanie i realizacją procesów mogą przywoływać precyzyjne instrukcje wykonywania określonych czynności, krok po kroku, ze szczególnym uwzględnieniem:

- zasad posługiwania się i wykorzystywania wszelkich danych zawartych w systemie;
- wymagań dokładności i regularności wykonywania powierzonych zadań wszędzie tam gdzie istnieją zależności pomiędzy różnymi systemami, procesami, aplikacjami czy procedurami;
- reakcji na sytuacje krytyczne powstałe w wyniku błędów pojawiających się w trakcie pracy systemu;
- zasad korzystania z wszelkich dostępnych w systemie aplikacji narzędziowych i wspomagających (system utilities);
- reguł tworzenia, przechowywania i usuwania wszelkich drukowanych z systemu informacji uznanych za istotne z punktu widzenia tworzonej polityki bezpieczeństwa systemu – również w przypadkach wydruków błędnych, niepełnych czy kontrolnych;
- procedur uruchamiania systemu po awarii z dokładnym opisem czynności administratorskich.

Na etapie dokumentowania ISMS konieczne jest opracowanie procedur działania przygotowujących pracowników organizacji do postępowania w sytuacjach awaryjnych. Konieczne w tym przypadku jest zwrócenie uwagi na następujące aspekty:

- awarie i uszkodzenia systemu;
- błędy wynikające z próby przetwarzania niekompletnych, niepoprawnych lub uszkodzonych danych;
- próby włamania do systemu z zewnątrz firmy;
- próby włamania do systemu z wewnątrz firmy;
- utratę wewnętrznych mechanizmów zabezpieczeń spowodowaną awarią sprzętu lub systemu; przy opracowywaniu planów odbudowy systemu po awarii należy między innymi uwzględnić:
- analizę i identyfikację przyczyn awarii systemu;

* Zob. nr 11/2000 „PJ"

- **dokładną definicję przyczyny** oraz określenie konkretnych planów i kroków mających w przyszłości wyeliminować skutki wystąpienia zdefiniowanej przyczyny.

Procedury opracowane na potrzeby sytuacji odbudowy bezpieczeństwa systemu po próbie włamania się do systemu powinny w przypadku ich zastosowania gwarantować, że wyłącznie uprawnieni i dokładnie zidentyfikowani użytkownicy mają dostęp do danych i zasobów systemu. A więc

- wszystkie kroki przedsięwzięte po zaistnieniu sytuacji krytycznej zostały dokładnie udokumentowane i przedstawione do wglądu kierownictwu,
- bezpieczeństwo systemu zostanie na powrót przywrócone w możliwie najkrótszym czasie.

Wymagania BS 7799 dotyczące dokumentacji są znacznie szersze, niż przedstawione powyżej.

Wszystkie procedury ISMS muszą być nadzorowane, aktualne, dostępne w miejscach stosowania, autoryzowane, podobnie jak zmiany, którym podlegają.

Wiodące wymagania legislacyjne w zakresie ochrony danych

Ochrona danych i informacji, w tym osobowych, stała się podstawą dla opracowania wielu aktów prawnych w skali poszczególnych państw, jak również obszarów ekonomicznych czy konkretnych kontraktów handlowych. Do najbardziej znaczących w Europie na pewno zaliczyć należy Data Protection Act (1998) opracowany w Wielkiej Brytanii. Jest uznawany za najlepszy dokument tego typu na świecie, jego ustanowienie na pewno także leży u podstaw intensyfikacji prac związanych z budową i doskonaleniem normatywnych podstaw systemowego zarządzania bezpieczeństwem informacji (BS 7799). DPA nakłada obowiązki na pracodawców – pracowników odpowiedzialnych za nadzorowanie danych personalnych, wskazuje konieczne zasady i regulacje w zakresie powyższych aktywności.

DPA określa wymagania, jakim musi sprostać pracodawca w odniesieniu do danych personalnych; restrykcyjność postępowań jakie muszą być przyjęte w praktyce są związane z rodzajem i przeznaczeniem danych, źródłem ich pochodzenia oraz procesów jakim celowo są poddawane.

Data Protection Act definiuje podstawowe zasady dotyczące bezpieczeństwa danych nakazujące postępowanie z danymi personalnymi w zgodzie z prawem. W podstawowym względzie zasady niniejsze stawiają ograniczenia, m. in.

- dane personalne nie mogą być wykorzystywane w żadnym innym celu poza tym dla jakich zostały zebrane,
- dane personalne powinny być wierne i utrzymywane dłużej niż jest to konieczne w związku z celem dla osiągnięcia jakiego zostały pozyskane.

Istotną cechą opracowanego w 1998 roku dokumentu jest uwzględnienie transferu danych personalnych na zewnątrz EEA (European Economic Area). Konieczne jest w powyższym zakresie zapewnienie, że dane personalne nie będą transferowane do państwa na zewnątrz Europejskiej Strefy Ekonomicznej przed zapewnieniem przez to państwo adekwatnego poziomu bezpieczeństwa oraz swobody w przetwarzaniu tego typu informacji.

DPA definiuje także wymagania w zakresie pozyskiwania, rejestracji, archiwowania oraz przetwarzania danych.

Podstawą dla opracowania DPA były doświadczenia związane z zarządzaniem bezpieczeństwem informacji i wnioskowanie w tym zakresie leży u podstaw wszystkich punktów tego dokumentu. Warto zwrócić uwagę o uzupełnienie DPA w stosunku do poprzednich koncepcji o wymagania definiujące konieczność ustanowienia systemu monitorowania i pomiarów związanych z nieautoryzowanym i nie w pełni zgodnym z prawem działaniem na danych personalnych związanych z utratą, zniszczeniem czy ich uszkodzeniem.

DPA w swojej treści odwołuje się do systemowego podejścia związanego z bezpieczeństwem informacji i danych. Wskazuje na konieczność wdrożenia i utrzymywania ISMS – Systemu zarządzania bezpieczeństwem informacji, odwołuje się w tym przypadku do normy BS 7799.

A zatem spełnienie wymagań normy BS 7799 może okazać się bardzo pomocnym mechanizmem demonstrowania i dowodzenia gotowości do spełnienia wymagań prawa w zakresie ochrony danych.

Prawna konieczność ochrony danych, stwarza korzystny klimat dla zainteresowania systemowym zarządzaniem bezpieczeństwem informacji (ISMS – Information Security Management System) zgodnego z normą BS 7799.

Przemawia za tym kilka argumentów:

- wymagania niniejszego standardu są związane z koniecznością systemowych działań dotyczących oceny ryzyk oraz ustanawiania adekwatnych zabezpieczeń przed realizacją działań mogących spowodować utratę czy też uszkodzenie danych organizacji,
- zobowiązanie do periodycznej weryfikacji ryzyk dotyczących bezpieczeństwa informacji, związanych ze zmianami w otoczeniu rynkowym, doświadczeń itd.,
- jest uznanym narzędziem, które z założenia zobowiązuje do respektowania wymagań prawa, prywatności danych i innych zasobów informacyjnych.

W kontekście powyższych analiz szczególnego znaczenia nabiera procedura akredytowanej certyfikacji c:cure, dzięki której organizacja może na drodze niezależnego auditu trzeciej strony uzyskać certyfikat zgodności i demonstrować na rynku posiadanie udokumentowanego, wdrożonego i efektywnego systemu zarządzania bezpieczeństwem informacji.

Analiza zainteresowania organizacji ISMS oraz BS 7799

W 1999 roku przeprowadzone zostały w Wielkiej Brytanii badania związane przypadkami utraty informacji przez firmy oraz działań i planów związanych z ustanowieniem systemu zarządzania bezpieczeństwem informacji zgodnym z normą BS 7799 (c:cure survey 1999).

Rezultaty badań oddają obraz obaw przedsiębiorstw związanych z niekontrolowaną utratą danych oraz mogą stanowić podstawę dyskusji w tym względzie.

Ocenie poddanych zostało ponad 1000 organizacji brytyjskich, z szerokiego spektrum instytucji produkcyjnych i usługowych – począwszy od liczących mniej niż 10 pracowników (18%) do zatrudniających tysiące pracowników w różnych lokalizacjach. Badane organizacje reprezentują 10 szerokich kategorii, zawierają w sobie firmy z sektora prywatnego i publicznego, producentów i usługodawców, przedstawicieli usług profesjonalnych i innych.

Lp.	Sektory	Udział
1.	Sektor publiczny	22%
2.	Przemysł	20%
3.	Usługi finansowe i prawne	18%
4.	IT (Information Technology)	16%
5.	Usługi serwisowe	11%
6.	Usługi przemysłowe	4%
7.	Usługi transportowe	4%
8.	Sprzedaż i dystrybucja	3%
9.	Obronność	2%

Tab 1. Respondenci c:cure survey 1999. Źródło: c:cure survey 1999, BSI – DISC, Admiral plc.

W przypadku pytań dotyczących przypadków naruszenia zasad bezpieczeństwa większość firm odpowiadała, że nie zanotowali takich sytuacji w ogóle – szczególnie taka odpowiedź dotyczyła dużych organizacji, natomiast druga grupa organizacji wskazywała na bardzo liczne przypadki tego typu.

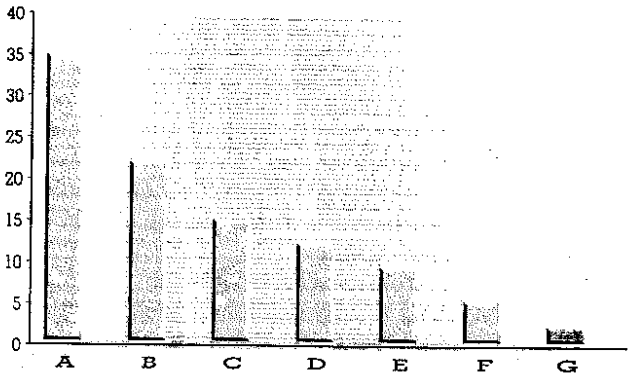
Zdecydowana większość badanych organizacji nie jest świadoma zagrożeń związanych z nieskutecznym systemem bezpieczeństwa informacji. Można dopatrywać się dwóch podstawowych przyczyn, dla jakich organizacje nie wykazują problemów dotyczących bezpieczeństwa informacji i danych.

Po pierwsze nie są świadome ich występowania. Jest całkiem logiczne, że jeżeli firma nie zapewniła dostępności efektywnych rozwiązań w zakresie uniemożliwienia nieautoryzowanych działań, to nie jest w stanie definiować większości z takich przypadków, jeśli w ogóle jakiekolwiek.

Po drugie w sytuacji, kiedy klient czy też partner rynkowy dostrzeże problemy dotyczące bezpieczeństwa, ich reputacja oraz wiarygodność zostają wystawione na wielką próbę. Na pewno także w wielu przypadkach organizacje poświęcają uwagę dyskrecji w działaniach służących eliminowaniu skutków zdarzeń dotyczących nieskuteczności zabezpieczeń.

Powszechność normy BS 7799 oraz certyfikacji c:cure

Obecna struktura i treść BS 7799, w której wielokrotnie można odnaleźć szczególny nacisk na warunki i relacje rynkowe jest jednoznacznym dowodem na odpowiedniość wobec współczesnych wymagań rynkowych. Jednak badania wykazały, że większość organizacji w Wielkiej Brytanii – ponad 50%, jest na bardzo zróżnicowanym poziomie zainteresowania wdrażaniem ISMS w oparciu o BS 7799 oraz certyfikacji systemu zarządzania bezpieczeństwem informacji.



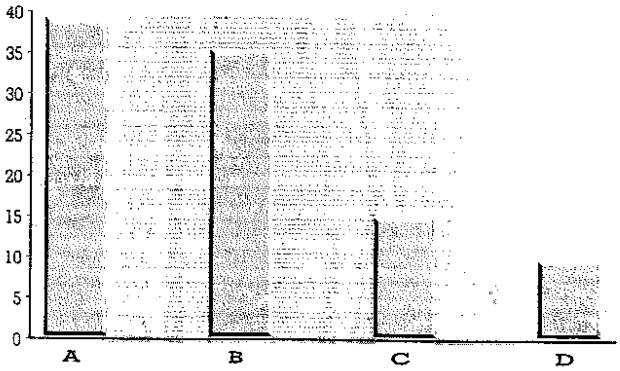
Rys. 1. Powszechność normy BS 7799 oraz certyfikacji c:cure. Źródło: c:cure survey 1999, BSI – DISC, Admiral plc.

A – posiadają informacje i rozważają podjęcie projektu ISMS (64,9%)
B – świadomi istnienia BS 7799, ale nie podejmujący żadnych działań (22,9%)
C – nie posiadający żadnej wiedzy dotyczącej BS 7799 (14,9%)
D – zgodni z wymaganiami standardu BS 7799 (11,9%)
E – przeprowadzający audity wewnętrzne (8,6%)
F – rozważający z zarządem zasadność podjęcia projektu ISMS zgodnie z BS 7799 (4,9%)
G – gotowi do certyfikacji BS 7799 (1,9%)

Korzyści związane z ustanowieniem systemu zarządzania bezpieczeństwem informacji zgodnym z BS 7799

Ponad 40% organizacji wskazuje na korzyści, jakie mogłyby być związane z ustanowieniem ISMS. W pierwszej kolejności jest wymieniana pomoc w ochronie informacji i danych w drugiej natomiast, możliwość ustanowienia podstawy systemowych rozwiązań wewnątrz firmy.

Inna grupa organizacji postrzega BS 7799 oraz procedurę c:cure jako korzystne z uwagi na podniesienie wiarygodności w oczach klientów, pomoc w osiąganiu koniecznego poziomu bezpieczeństwa danych personalnych oraz przewagę konkurencyjną.

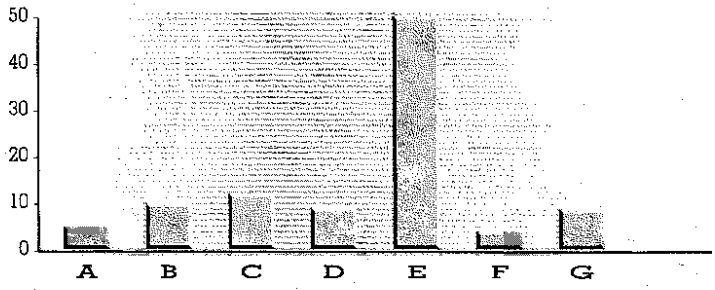


Rys. 2. Korzyści związane z systemem zarządzania bezpieczeństwem informacji zgodnym z BS 7799. Źródło: c:cure survey 1999, BSI – DISC, Admiral plc.

A – ochrona informacji i danych (40%)
B – podstawa wewnętrznego bezpieczeństwa informacji (35%)
C – konieczny element działalności organizacji (15%)
D – ochrona wymiany informacji rynkowej (10%)

Przygotowanie do certyfikacji

Zważywszy na fakt, że c:cure jest stosunkowo nową koncepcją weryfikacji skuteczności ISMS, 15% badanych organizacji zadeklarowało wstępnie swoją gotowość do certyfikacji w najbliższym czasie, a najdalej w ciągu 12 miesięcy. Ponad 1/3 firm – 36% powzięło decyzję o spełnieniu wymagań BS 7799 i przystąpienie do procedury certyfikacyjnej. W kilku przypadkach firmy posiadają ustanowione systemy zarządzania bezpieczeństwem informacji lub elementy systemu oparte o inne zasady niż BS 7799. Tylko 4% firm wyraziło pogląd o nieadekwatności BS 7799 wobec prowadzonej działalności.



Rys. 3. Przygotowanie ISMS do certyfikacji. Źródło: c:cure survey 1999, BSI – DISC, Admiral plc.

A – gotowość do certyfikacji w okresie krótszym niż 6 miesięcy (4,5%)
B – gotowość do certyfikacji w okresie 6 – 12 miesięcy (9,9%)
C – gotowość do certyfikacji w okresie 12 – 18 miesięcy (13,5%)
D – gotowość do certyfikacji w czasie dłuższym niż 18 miesięcy (8,9%)
E – zainteresowanie BS 7799 ale zbyt mało informacji (48,7%)
F – brak zainteresowania z uwagi na nieadekwatność (4,0%)
G – mało prawdopodobne wdrażanie BS 7799 i certyfikacja (9,9%)

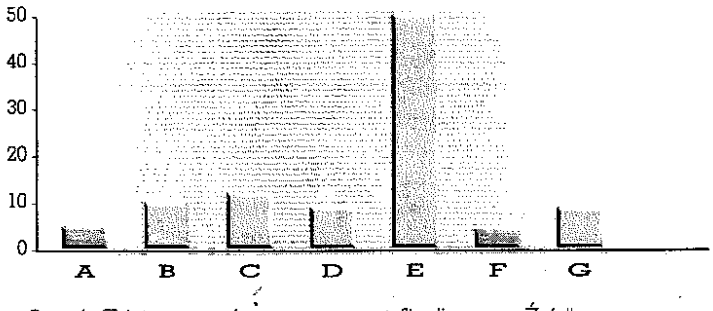
Można przytoczyć powtarzające się opinie przedstawicieli firm, którzy uznali, że jest mało prawdopodobne zainteresowanie BS 7799 oraz przystąpienie do procesu certyfikacji:

- zbyt mała firma – brak efektywności finansowej przedsięwzięcia (typowa opinia firm jednoosobowych),
- tylko w przypadku kiedy będzie to wymaganiem klientów,
- mamy inne procedury w zakresie bezpieczeństwa informacji (np. instytucje rządowe).

Zainteresowanie procesem certyfikacji

Podstawową przyczyną, dla jakich organizacje podejmują decyzje o certyfikacji ISMS w oparciu o normę BS 7799, jest bezpieczeństwo prowadzonej działalności oraz podążanie za najlepszymi i sprawdzonymi koncepcjami w tym zakresie. W dalszej kolejności przedsiębiorcy zwracają uwagę na przewagę konkurencyjną, z jaką wiążą posiadanie certyfikatu. Na ostatnim miejscu zainteresowania pozostaje zainteresowanie partnerów handlowych oraz wymagania klientów.

Spośród innych przyczyn, na jakie zwracali uwagę przedstawiciele badanych firm, można przytoczyć także: dowodzenie zgodności z wymaganiami legislacyjnymi (Data Protection Act), osiągnięcie poziomu bezpieczeństwa w standardzie, jakim to realizują najlepsze firmy.



Rys. 4. Zainteresowanie procesem certyfikacji c:cure. Źródło: c:cure survey 1999, BSI – DISC, Admiral plc.

A – najlepsza praktyka w zakresie zarządzania bezpieczeństwem informacji (42,3%)
B – bezpieczeństwo prowadzonej działalności (40,1%)
C – przewaga konkurencyjna (10,4%)
D – wymagania klientów (7,2%)

Podsumowanie

Do argumentów przemawiających za budową systemu zarządzania bezpieczeństwem informacji, które wskazane zostały we wcześniejszym artykule, można przytoczyć postanowienia ustawy o ochronie danych osobowych. Zobowiązuje ona m.in. administratora danych do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności wskazuje na powinność zabezpieczenia danych przed ich udostępnieniem osobom nie upoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Dla zapewnienia zgodności organizacji z powyższymi wymaganiami konieczne jest ustanowienie systemowych rozwiązań.

PJ

Literatura:

1. J. Łuczak, Systemy zarządzania bezpieczeństwem informacji (ISMS), Problemy Jakości, 11/2000.
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. z 1997 r. Nr 133, poz. 883)
3. BS 7799 – 1 Code of practice for Information Security, 1999.
4. BS 7799 – 2 Specyfication for Information Security Managemet Systems, 1999.
5. EC DGX III/ 07 ETSII Project SEDUCER (23186).
6. Materiały źródłowe BSI.
7. Materiały szkoleniowe BS 7799 Risk Assesment Workshop, ODI 2000.
8. M. Oldegard, Applying the management system approach to information security and working conditions in Sweden, ISO News, vol. 9, no. 3 may/ June 2000.
9. Forrester Research Raport 1999.
10. PD 3001 Preparing for BS 7799 certification.
11. PD 3003 Are you ready for a BS 7799 audit?
12. PD 3004 Guide to BS 7799 auditing.
13. c:cureworld newsletter, BSI – DISC, summer 99.
14. The c:cure survey 1999, BSI – DISC – Admiral plc, 2000.