

Czy warto wdrażać normę BS 7799-2?

Coraz więcej firm, których istotnym aktywem jest bardzo różnie pojmowana informacja, decyduje się na wdrożenie normy BS 7799-2. Wdrożenie systemu i jego certyfikacja potwierdzają, że firma chroni informacje w sposób przewidziany światowym standardem, co ma istotny wpływ na jej pozycję na rynku.

Zyjemy w dobie informacji, co oznacza, że jest ona towarem. Utrata czy manipulowanie informacjami, ich niewłaściwe przetwarzanie w systemach informatycznych oznaczają dla firm ogromne straty i to bez względu na branżę. – W rezultacie każdego roku wydaje się coraz więcej na różne zabezpieczenia techniczne organizacyjne – począwszy od systemów fizycznego nadzoru, na różnych procedurach kontroli pracowników kończąc. W większości przypadków wydatki związane z bezpieczeństwem nie traktuje się jako inwestycji, ale niezbędny koszt działania. Wiedza o istniejących zagrożeniach i stosowanych zabezpieczeniach ogranicza się do pracowników kilku komórek organizacyjnych – zazwyczaj działu IT oraz pionu ochrony informacji niejawnych. Efekt jest taki, że firma nie zarządza swoim bezpieczeństwem, a tylko wdraża kolejne zabezpieczenia, które lepiej lub



gorzej chronią ją przed zagrożeniami – ocenia Marcin Zastawa.

wa, dyrektor Departamentu Zarządzania DGA.

Dlatego rośnie zainteresowanie systemowym podejściem do bezpieczeństwa informacji, bazującym na analizie ryzyka – takie podejście reprezentuje właśnie międzynarodowy standard BS 7799-2. – Jego siła polega na indywidualnej analizie ryzyka, zbiorach polityki, procedur i instrukcji, dzięki którym bezpieczeństwo informacji staje się integralną częścią mechanizmów zarządzania i ochrony firm. Podobnie jak w przypadku innych systemów zarzą-

PLAN MINIMALIZACJI RYZYKA

To dokument określający:

- zagrożenia, dla jakich podejmowane są działania;
- bieżący poziom ryzyka;
- wdrożone środki kontroli;
- metodę dalszego ograniczania ryzyka (redukcja, transfer itd.);
- dodatkowe środki kontroli (zabezpieczenia), które zostały wybrane w celu redukcji ryzyka;
- osobę odpowiedzialną za wdrożenie zabezpieczeń;
- termin realizacji.

dzania, głównym celem systemu bezpieczeństwa informacji jest wprowadzenie określonego sposobu postępowania – a więc standaryzacja postępowania, także w sytuacjach kryzysowych – dodaje Marcin Zastawa.

→ JAK ZABRAĆ SIĘ DO WDRAŻANIA BS 7799-2?

Norma ta reguluje tak duży obszar, że firmy przymierzające się do jej wdrożenia mają przede wszystkim kłopot z jej nadmiarom. Ta nadmiarowość standardu, wynikająca z jego uniwersalności, ma też swoje dobre strony, bo łatwiej wyselekcjonować te obszary działań i rodzaje zabezpieczeń, które będą najwłaściwsze dla danej firmy, zwłaszcza że norma przewiduje możliwość dokonywania tzw. wyłączeń. Przy tej selekcji należy posługiwać się analizą zagrożeń, dokonaną pod kątem prawdopodobieństwa ich wystąpienia w firmie. Generalnie norma omawia wytyczne i wymagania do budowy zintegrowanego systemu bezpieczeństwa informacji (tzw. najlepsze praktyki) oraz definiuje poszczególne elementy kontroli i sterowania bezpieczeństwem informacji, porządkując całość w 10 grup wymagań.

Budowę systemu zarządzania bezpieczeństwem informacji powinna poprzedzić analiza stanu obecnego bezpieczeństwa informacji, w tym analiza systemów teleinformatycznych związanych z jej przetwarzaniem.

RÓŻNICE W PODEJŚCIU DO BEZPIECZEŃSTWA INFORMACJI

Firma niedbająca o bezpieczeństwo w sposób systemowy	Firma z wdrożonym systemem zarządzania bezpieczeństwem informacji
→ Brak koordynacji polityki bezpieczeństwa pomiędzy różnymi jednostkami organizacyjnymi (departament IT, ochrona fizyczna, Pion Ochrony Informacji Niejawnych).	→ Standaryzacja bezpieczeństwa informacji w całej organizacji – stworzenie odpowiednich struktur nadzorczych.
→ Koncentracja na zabezpieczeniach.	→ Koncentracja na analizie ryzyka.
→ Wydatki na bezpieczeństwo traktowane jako koszt działania.	→ Wydatki na bezpieczeństwo traktowane jako inwestycja (możliwość wyznaczania wskaźników zwrotu z inwestycji).

Zdjęcia: DGA

JACEK MARKOWSKI
Menedżer w Dziale Zarządzania
Ryzykiem Informatycznym firmy
Ernst & Young

W ciągu ostatnich dwóch lat zauważamy w Polsce znaczny wzrost zainteresowania ze strony firm uzyskaniem certyfikatu zgodności z normą BS 7799-2:2002. Niestety, w wielu przypadkach początkowe zainteresowanie nie przekłada się na działania związane z ustanowieniem efektywnego Systemu Zarządzania Bezpieczeństwem Informacji.

Z naszych doświadczeń wynika, iż bardzo często przedsiębiorstwa za szybko przystępują do procesu certyfikacji, nie będąc w pełni przygotowanymi do audytu. W rezultacie przytłoczone dużą liczbą zidentyfikowanych słabości, rezygnują.

Należy pamiętać, że skuteczny System Zarządzania Bezpieczeństwem Informacji to nie tylko odpowiednia konfiguracja techniczna serwerów i urządzeń aktywnych sieci komputerowych, ale również kompleksowe rozwiązania organizacyjno-proceduralne. Właśnie wdrożenie odpowiednich procedur oraz wprowadzenie zmian w organizacji okazuje się często procesem najtrudniejszym i najbardziej czasochłonnym. Dlatego też do certyfikacji powinny przystępować firmy, które osiągnęły już pewien poziom dojrzałości, zarówno pod względem organizacji IT, jak i bezpieczeństwa informacji.

Jedną z głównych korzyści z uzyskania certyfikatu zgodności z normą BS 7799-2:2002 jest ujednolicenie modelu zarządzania bezpieczeństwem informacji w firmie oraz wdrożenie rozwiązań adekwatnych do istniejących potrzeb, a w perspektywie długoterminowej zwiększenie poziomu zaufania klientów. Coraz częściej posiadanie certyfikatu jest warunkiem koniecznym, aby firma mogła brać udział m.in. w ogłaszanych postępowaniach przetargowych. Jego brak to świadome zmniejszanie przewagi konkurencyjnej.

W ciągu ostatniego półrocza coraz więcej przedsiębiorstw zwraca się do nas z prośbą o pomoc w procesie przygotowania do certyfikacji. Według naszych klientów współpraca z wykwalifikowanym doradcą pozwala na dokonanie niezależnej oceny istniejącego stanu bezpieczeństwa informacji oraz umożliwić efektywną realizację kolejnych kroków w procesie wdrażania Systemu Zarządzania Bezpieczeństwem Informacji. W konsekwencji skraca to czas potrzebny na przygotowanie i zwiększa szansę na pomyślną certyfikację.

niem – od topologii sieci poprzez procedury eksploatacyjne wszystkich krytycznych systemów informatycznych, procedury zarządzania kopiami zapasowymi czy uprawnieniami użytkowników po wyniki częściowych i pełnych audytów teleinformatycznych. Tak uzyskaną informację trzeba odpowiednio sklasyfikować pod kątem minimalizacji ryzyka utraty kluczowych dla firmy danych – w efekcie powinny wyłonić się obraz zagrożenia. – Po etapie klasyfikacji informacji i analizie podat-

ności można przystąpić do analizy ryzyka – kluczowego elementu systemu zarządzania bezpieczeństwem informacji. Jest to także element, który często sprawia największe problemy – osoby odpowiedzialne za przeprowadzenie analizy mają trudności z wiarygodnym identyfikowaniem zagrożeń czy z oceną prawdopodobieństwa ich spełnienia. Efektem tego etapu powinna być macierz ryzyka, określająca ryzyko utraty (poufność, integralność, dostępność) informacji w wyniku zrealizowania się konkretnego

zagrożenia – wyjaśnia Marcin Zastawa.

→ PORA NA MINIMALIZACJĘ RYZYKA

Wiedząc już, co mamy minimalizować, możemy przygotować plan minimalizacji ryzyka, bazując zarówno na samych wskazaniach normy, jak i na wymaganiach branżowych. Na tym etapie trzeba też dokonać selekcji ryzyka akceptowalnego, w stosunku do którego nie będziemy na razie podejmować żadnych działań. Później rodzi się dokumentacja planu minimalizacji ryzyka, obejmująca zarówno politykę bezpieczeństwa informacji, jak i procedury związane z systemami teleinformatycznymi. Dokumentacja z kolei jest podstawą audytu wewnętrznego, obejmującego zarówno elementy organizacyjne, jak i informatyczne. Jeśli audyt wykaże, że wszystkie działy firmy stosują się do zasad polityki bezpieczeństwa, dopiero wówczas można mówić o certyfikacji systemu zarządzania bezpieczeństwem przez niezależną jednostkę certyfikującą. Nic więc dziwnego, że wdrożenie normy BS 7799-2 trwa zwykle więcej niż rok.

→ KTO WDRAŻA NORMĘ BS 7799-2

Zainteresowanie tym rozwiązaniem systemowym w Pol-

sce rośnie ze strony firm, które z racji swojej specyfiki muszą zwracać szczególną uwagę na bezpieczeństwo informacji. Wśród firm, które już wdrożyły ten standard, znajdziemy zarówno operatorów telekomunikacyjnych (np. PTK – Centertel), banki, branżę energetyczną, administrację państwową, jak i spółki o profilu informatycznym. Wśród tych ostatnich wdrożeniem normy zainteresowane są zwłaszcza spółki outsourcingowe, bo jakoś świadczone przez nie usługi w decydującej mierze zależą od kompleksowego zapewnienia bezpieczeństwa informacji.

– Certyfikacja z normy BS 7799-2 będzie nie tylko potwierdzeniem zdolności itelligence do świadomej ochrony informacji, ale i do zarządzania ryzykiem z nią związanym. Tym samym staniemy się jeszcze bardziej wiarygodni dla naszych klientów wprowadzających zgodność z ustawą Sarbanes Oxley Act – oni muszą bowiem zidentyfikować te procesy, które wpływają na wiarygodność sprawozdania finansowego i ocenić, w jakim stopniu zaordynowana przez nich kontrola zminimalizuje zidentyfikowane czynniki ryzyka – mówi Arnold Nowak, prezes itelligence, dostawcy usług outsourcingowych.

MMK

Marcin Zastawa
Dyrektor Departamentu
Zarządzania
DGA

Autorzy normy BS 7799 świadomie posługują się analizą ryzyka w celu opracowania mechanizmów zabezpieczających informacje, aby uniknąć sytuacji, w której okaże się, że tylko najbogatsze firmy będzie stać na myślenie o bezpieczeństwie. Podstawowy efekt, jaki osiąga się poprzez wdrożenie systemu bezpieczeństwa informacji opierając się na BS 7799-2, to zbudowanie świadomości co do zagrożeń oraz opracowanie i realizacja planów minimalizacji ryzyka. Podejście takie oznacza, że tak naprawdę każdego stać na wdrożenie systemu bezpieczeństwa, a likwidowanie luk technologicznych, ale przede wszystkim organizacyjnych, jakie

pojawiają się w systemie, należy rozłożyć w czasie zgodnie z możliwościami finansowymi organizacji. System bezpieczeństwa informacji z góry zakłada, że nie uzyska się stanu maksymalnego, a jedynie optymalny na daną chwilę. System ma dać nam odpowiedź, czy jesteśmy świadomi zagrożeń, a jeżeli tak, to jakie dostępne (w granicach możliwości finansowych poszczególnej firmy) mechanizmy nadzoru wybraliśmy i wdrożyliśmy, aby ich wpływ minimalizować. Oznacza to, że dopuszcza się istnienie luk w systemie bezpieczeństwa, ale w sposób świadomy, z podjętymi działaniami minimalizującymi negatywny ich wpływ.