

Dla wiarygodności sprawozdań finansowych

SOX: kontrola wewnętrzna

Celem SOX ma być przywrócenie zaufania do podmiotów przez uwiarygodnienie ich sprawozdań.

Arnold Nowak

W odpowiedzi na serię skandali finansowych, z których najgłośniejszy był przypadek Enronu, kongres Stanów Zjednoczonych uchwalił w 2002 r. akt prawny, nazwany od nazwisk jego twórców „Sarbanes-Oxley Act” (SOX). Jego celem ma być przywrócenie zaufania do graczy na rynkach finansowych przez poprawę jakości i wiarygodności sprawozdawczości finansowej. Ustawa nakłada więc na zarządy spółek obowiązek zapewnienia mechanizmów kontroli wewnętrznej. Sposoby tej kontroli i ich efektywność są weryfikowane przez niezależnego audytora. Niezgodne z prawdą poświadczenie rzetelności sprawozdań finansowych przez dyrektora naczelnego i dyrektora finansowego grozi wysoką karą – do 20 lat więzienia i 5 mld USD grzywny.

Jakość informacji

Wprawdzie sama ustawa nie definiuje precyzyjnie wymagań w stosunku do systemów informatycznych przetwarzających informację finansową. Nakazuje jednak odpowiednią jakość informacji finansowej, co oznacza, że powinna ona być aktualna, prawidłowa, dostępna w odpowiednim czasie i dla uprawnionych użytkowników.

W praktyce spełnienie wymagań SOX wymaga rewizji organizacji całego działu IT. W przetwarzaniu informacji finansowej zaangażowany jest bowiem nie tylko sprzęt i aplikacje, ale także bazy danych, sieci i systemy operacyjne.

Trzeba więc dostosować odpowiednie procedury kontroli środowiska IT. Nie jest to zadanie proste, zważywszy na fakt, że ustawa nie tylko nie precyzuje ich szczegółowo, ale i jej interpretacja nieustannie się zmienia. Kontrola bieżącej pracy systemów IT może dotyczyć problemów zarządzania całym działem IT, jak też weryfikacji każdego ogniwa systemów. Na każdym poziomie kontroli trzeba stworzyć odpowiednie procedury i wyznaczyć osoby odpowiedzialne, co sprawia, że zapewnienie zgodności z SOX jest przede wszystkim ogromnym wyzwaniem natury organizacyjnej. O randze tego wyzwania świadczy fakt, że – wg danych jednej ze światowych firm audytorskich – średni koszt zapewnienia zgodności wynosi 3 mln USD i pochłania 25 tys. godzin pracy.

Ustawa i norma

Mimo że SOX nie wymaga wprost od organizacji wprowadzenia norm bezpie-

czeństwa informacji, jest oczywiste, że wdrożenie odpowiednich systemów zarządzania jakością i bezpieczeństwem IT z jednej strony pomoże w zapewnieniu wymagań SOX, a z drugiej – powinno znacznie ułatwić sam proces audytu. Dlatego firmy, które wdrożyły normę BS 7799, kontrolują również obszar ryzyka związany ze zgodnością z ustawą SOX. Norma BS 7799 ma dwie części. Pierwsza to rodzaj kodeksu praktyki, druga to specyfikacja wymagań zarządzania bezpieczeństwem informacji, na którą składa się wiele elementów – obok polityki i organizacji bezpieczeństwa, zasady korzystania z sieci i komputerów oraz zasady kontroli dostępu do systemów, również ochrona danych zgodnie z regulacjami prawnymi.

W kontekście ustawy SOX duże znaczenie ma także amerykański standard SAS 70 (type II), który wymusza okresową kontrolę wprowadzonych procedur. ■



W POLSCE Jurysdykcji SOX w naszym kraju, obok podmiotów zależnych publicznych spółek amerykańskich, od 15 lipca 2005 r. podlegają także przedsiębiorstwa należące do firm zarejestrowanych i działających poza USA, ale notowanych na giełdach amerykańskich – informuje Arnold Nowak, prezes polskiego oddziału itelligence