

Informatyka a bezpieczeństwo informacji



Coraz więcej polskich organizacji oczekuje od wprowadzanych rozwiązań informatycznych nie tylko wzrostu efektywności firmy i obniżenia kosztów utrzymania infrastruktury IT, ale także gwarancji odpowiedniej jakości informacji finansowej.

Przepisy nie definiują wprawdzie precyzyjnie wymagań w stosunku do systemów informatycznych przetwarzających informację finansową, ale odpowiednia jej jakość oznacza, że powinna być aktualna, prawidłowa, dostępna w odpowiednim czasie i dla uprawnionych użytkowników. Obecnie wszystkie informacje finansowe przetwarzane są nie tylko z udziałem ludzi, ale także sprzętu, aplikacji, baz danych, sieci i systemów operacyjnych. Do wszystkich tych elementów „łańcucha” informacyjnego zarząd firmy musi podejść odrębnie, kontrolując poszczególne etapy generowania, modyfikowania i przesyłania informacji. Od efektywności tej kontroli zależy wprost wiarygodność raportów finansowych, którą zarząd poświadcza pod groźbą odpowiedzialności karnej.

Ustawa SOX

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” (w skrócie SOX lub SOA). Jego celem ma być przywrócenie zaufania do graczy na rynkach finansowych poprzez poprawę jakości i wiarygodności sprawozdawczości finansowej. Gwarantem tej poprawy mają być w znacznym stopniu zarządy spółek, na których spoczywa obowiązek zapewnienia mechanizmów kontroli wewnętrznej i efektywnego sprawowania tej kontroli, weryfikowanej przez niezależnego audytora. Niezgodne z prawdą poświadczenie rzetelności sprawozdań finansowych przez dyrektora naczelnego i dyrektora finansowego zagrożone jest wysoką karą – do 20 lat więzienia i 5 mld USD grzywny. W Polsce ustawie tej podlegają przedsiębiorstwa należące do firm notowanych na giełdach amerykańskich.

W praktyce spełnienie wymogów SOX wymaga rewizji orga-

nizacji całego działu IT. Kontrolując od strony informatycznej cały okres życia informacji finansowej, zarządy firm muszą ocenić zarówno dostęp do danych i programów, jak i proces wprowadzania zmian oraz bieżącą pracę wszystkich systemów informatycznych w firmie. Muszą także uwzględnić nieustanny rozwój systemów informatycznych. Do takiej złożoności środowiska IT trzeba dostosować odpowiednie procedury jego kontroli. Nie jest to łatwe, zważywszy, że ustawodawstwo nie tylko nie precyzuje ich szczegółowo, ale i interpretacja ustaw nieustannie się zmienia. Kontrola bieżącej pracy systemów IT może dotyczyć problemów zarządzania całym działem IT, jak i weryfikacji każdego ogniwa systemów, poczynając od „peceta”. Na każdym poziomie kontroli trzeba stworzyć odpowiednie procedury i wyznaczyć osoby odpowiedzialne za nie, co sprawia, że zapewnienie zgodności z SOX jest przede wszystkim ogromnym wyzwaniem natury organizacyjnej. O randze tego wyzwania niech świadczy opinia jednej ze światowych firm audytorskich, że średni koszt zapewnienia wymaganej zgodności wynosi 3 mln USD i pochłania 25 tys. godzin pracy.

Doświadczenie w cenie

Ustawa SOX tak naprawdę nakłada na firmy obowiązek dokonania samooceny, czy stosowane rozwiązania – w tym systemy informatyczne – zapewniają poprawność informacji finansowej i działają skutecznie. W procesie samooceny firm niezbędna jest pomoc podmiotów zewnętrznych – audytorów lub dostawców innych usług, na przykład informatycznych. Ich doświadczenie w obszarze zapewniania zgodności z ustawą SOX jest niezwykle cenne. Najszerzą wiedzą mogą pochwalić się międzynarodowi dostawcy. Firma itelligence, wdrażając rozwiązania informatyczne realizowała

u swoich klientów projekty zapewnienia zgodności systemu informatycznego z wymaganiami ustawy SOX – Mamy także inny ważny atut: jesteśmy firmą świadczącą usługi outsourcingowe, a więc bezpieczeństwo, poufność oraz integralność danych klienta jest dla nas sprawą priorytetową – mówi Arnold Nowak, prezes itelligence. – Oznacza to, że jest nam znacznie łatwiej, jako firmie oferującej usługi o najwyższym standardzie bezpieczeństwa, zapewnić zgodność rozwiązań informatycznych z ustawą SOX. Możemy czerpać z doświadczeń związanych z zabezpieczeniami i procedurami obowiązującymi w naszym Centrum Danych – dodaje.

Wdrażając uznane normy

Ustawa SOX pośrednio dotyczy również firm outsourcingowych, które świadczą usługi na rzecz podmiotów zobowiązanych do zapewnienia zgodności z SOX. Kontroli podlegają bowiem istotne procesy oddane w outsourcing firmom zewnętrznym. Część firm w USA poddaje się z tego powodu ocenie niezależnego rewidenta. W itelligence uznano, że firmie outsourcingowej i wdrożeniowej potrzebne są najbardziej uznane standardy. Sięgnęliśmy po trzy najważniejsze: normę jakości ISO 9001:2000, normę w zakresie bezpieczeństwa informacji BS 7799-2 (w przyszłości będzie zastąpiona przez ISO 27001) oraz audyt według standardu SAS nr 70 (Statement of Auditing Standard nr 70).

Certyfikat zgodności z normą BS 7799 potwierdza, że system zarządzania bezpieczeństwem informacji gwarantuje jej poufność, integralność i dostępność. Norma wskazuje na takie elementy, jak: polityka bezpieczeństwa, organizacja bezpieczeństwa, bezpieczeństwo a pracownicy, techniczne środki kontroli dostępu, zasady korzystania z sieci i komputerów,

– Od początku swojej działalności przykładaliśmy dużą wagę do bezpieczeństwa informacji, ponieważ w sektorze IT wiedza jest jednym z podstawowych czynników sukcesu, dlatego podjęliśmy odpowiednie działania w celu zabezpieczenia systemów informatycznych spółki przed utratą danych. Kierownictwo firmy zauważyło jednak, że ochrona informacji nie może ograniczać się do jednej z jej form występowania – konieczne stało się wdrożenie rozwiązań technicznych i proceduralnych, które objęły swym zasięgiem całą spółkę. W szczególności oczekiwano, że wszystkie aspekty bezpieczeństwa zorganizowane zostaną wokół informacji, a nie zasobów IT. Szczególną uwagę zwróciliśmy na możliwość wdrożenia systemu zarządzania bezpieczeństwem informacji BS 7799-2. Opracowanie systemu w oparciu o tę normę, pozwalało Lumenie na skorzystanie z najlepszych światowych wzorców związanych z bezpieczeństwem informacji, przy jednoczesnej możliwości potwierdzenia odpowiedniego poziomu ochrony danych przez niezależną certyfikację – Tadeusz Browarek, prezes Lumena Sp. z o.o.

zasady kontroli dostępu do systemów, rozwój i rozbudowa systemu i jego utrzymanie, planowanie strategii firmy dla zagrożeń krytycznych oraz ochrona danych a regulacje prawne. Wdrożenie ISO 9001:2000 łącznie z BS 7799-2 zakończone certyfikatem będzie formalnie potwierdzało przygotowanie itelligence do oferowania usług dla klientów, którzy podlegają ustawie SOX. Pozwoli na usystematyzowane podnoszenie jakości usług itelligence, zależne głównie od kompleksowego zapewnienia bezpieczeństwa informacji. Potwierdzi także zdolności itelligence nie tylko do świadomej ochrony informacji, ale i do zarządzania ryzykiem z nią związanym.

Z kolei kontrola według standardów SAS 70 oznacza badanie procesów i transakcji realizowanych w firmie usługowej w celach udostępniania jego wyników zarządom i audytorom firm-klientów. W raporcie kończącym audyt znajduje się szczegółowy opis kontroli usługodawcy i niezależna ocena dotycząca tego, czy wytyczne audytora zostały przez firmę odpowiednio zaprojektowane, wcielone w życie i efektywnie działają. Arnold Nowak twierdzi, że firmy zewnętrzne posiadające dostęp do danych swoich klientów muszą prezentować najwyższą troskę o kontrolę, jakość i bezpieczeństwo informacji, z którymi mają styczność. Trzeba decydować się na potwierdzanie wysokiej wiarygodności swych. To ułatwia pracę dostawcom, klientom i ich audytorom.

Karolina Romanowska
pełnomocnik zarządu ds. jakości i bezpieczeństwa informacji
itelligence sp. z o.o.