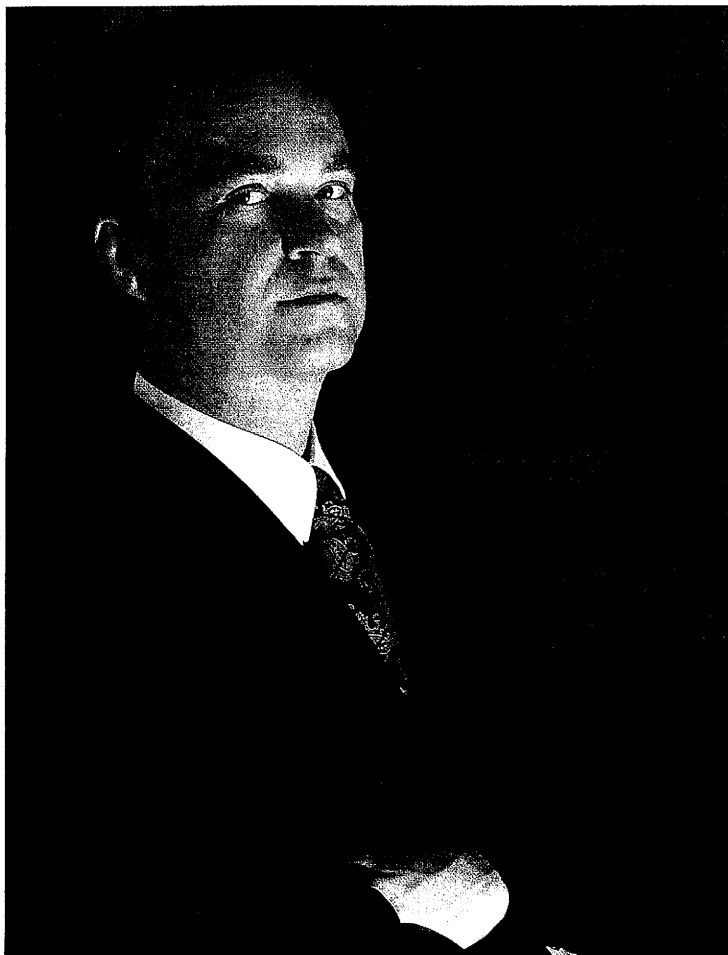


Prawodawstwo kamieniem u nogi IT



Krok w nieznanne. Pojawiają się pytania o wpływ państwa na wybór standardów informatycznych używanych w kontaktach z administracją. W szczególności chodzi o to, czy preferowane powinny być standardy otwarte, czy zamknięte — informuje Bogdan Fischer, partner w kancelarii prawnej Chatas i Wspólnicy.

Teoretycznie państwo nie powinno preferować żadnych rozwiązań i standardów informatycznych, ale w praktyce jest różnie.



Marcin Zloch

Bogdan Fischer, partner w kancelarii Chatas i Wspólnicy, podkreśla, że prawo nie powinno narzucać konkretnych rozwiązań informatycznych ani wskazywać konkretnych produktów czy producentów dla realizacji zadań wynikających z przepisów prawa.

— Założenie to wynika m.in. zarówno z konstytucyjnej zasady równości wobec prawa, jak i ze swobody prowadzenia działalności gospodarczej — twierdzi Bogdan Fischer.

Operacja się udała...

Plan informatyzacji państwa na lata 2007-10 oraz rozporządzenie Rady Ministrów z 28 marca 2007 r. w sprawie planu informatyzacji państwa na lata 2007-10 stanowią, że neutralność technologiczna rozwiązań informatycznych wykorzystywanych przez administrację publiczną jest jednym z istotnych priorytetów rozwoju systemów teleinformatycznych. Aby osiągnąć ten cel, obowiązujące w Polsce prawo zaleca stosowanie jawnych, powszechnie dostępnych standardów komunikacji i wymiany danych.

— W wielu dziedzinach konieczna jest standaryzacja. W związku z tym pojawiają się pytania o wpływ państwa na wybór standardów. W szczególności dyskutowane są kwestie, czy preferowane powinny być standardy otwarte, czy zamknięte — informuje Bogdan Fischer.

Komentarz: Jak to robią za wielką wodą?

Arnold Nowak, prezes zarządu itelligence

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). Jego celem ma być przywrócenie zaufania do graczy na rynkach finansowych przez 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, co weryfikuje niezależny audytor. Niezgodne z prawdą poświadczanie rzetelności sprawozdań finansowych przez dyrektora naczelnego i dyrektora finansowego zagrożone jest bardzo wysoką karą — do 20 lat więzienia i 5 mld USD grzywny. Jednak często ważniejszy od kar ustawowych jest odstręczający inwestorów wizerunek firmy „nie-transparentnej” finansowo.

W Polsce jurysdykcji ustawy — obok podmiotów zależnych publicznych spółek amerykańskich — od 15 lipca 2005 r. podlegają także przedsiębiorstwa należące do firm zarejestrowanych i działających poza Stanami Zjednoczonymi, ale

notowanych na giełdach amerykańskich. Sama ustawa nie definiuje wprawdzie precyzyjnie wymagań w stosunku do systemów informatycznych przetwarzających informacje finansową, ale zapisany w niej obowiązek „odpowiedniej jakości informacji finansowej” oznacza, że powinna ona być aktualna, prawidłowa, dostępna w odpowiednim czasie i dla uprawnionych użytkowników. W praktyce spełnienie SOX wymaga rewizji organizacji całego działu IT. W przetwarzanie informacji finansowej zaangażowany jest bowiem nie tylko sprzęt i aplikacje, ale także bazy danych, sieci i systemy operacyjne. Do każdej z tych części składowych środowiska IT zarząd firmy musi podejść wieloaspektowo, kontrolując wszystkie etapy tworzenia, modyfikowania i przesyłania informacji. Od efektywności tej kontroli zależy wprost wiarygodność raportów finansowych, którą zarząd poświadcza pod groźbą odpowiedzialności karnej.

Ustawa SOX tak naprawdę nakłada na firmy obowiązek dokonania samooceny, czy stosowane rozwiązania zapewniające poprawność informacji finansowej (w tym systemy informatyczne) działają skutecznie. W tym procesie samooceny potrzebna jest pomoc firm zewnętrznych — audytorów lub dostawców.

Zgodnie z definicją Komisji Europejskiej z 2004 r. standard otwarty musi być przyjęty i zarządzany przez niedochodową organizację, a jego rozwój musi odbywać się w drodze otwartego procesu, w którym mogą uczestniczyć wszyscy zainteresowani. Co więcej, jest on opublikowany, a jego specyfikacja jest dostępna dla wszystkich zainteresowanych bezpłatnie lub po kosztach sporządzenia kopii oraz udostępniona wszystkim do kopiowania, dystrybuowania i używania również bezpłatnie lub po kosztach operacyjnych. Wreszcie wszelkie związki z nim prawa autorskie, patenty i inna własność przemysłowa są nieodwołalnie udostępnione bez opłat. Nie ma też żadnych ograniczeń w jego wykorzystaniu.

...ale pacjent nie przeżył

Ustawa z 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne ustanawia m.in. obowiązki, które mają doprowadzić do osiągnięcia stanu współdziałania systemów teleinformatycznych i rejestrów publicznych oraz równego traktowania rozwiązań informatycznych.

— Nakaz stosowania konkretnego oprogramowania nie wynika więc bezpośrednio z przepisów. Zamierzenia są zgoła odwrotne. Zdarzały się jednak i prawdopodobnie będą się zdarzać sytuacje, w których może dochodzić do pośredniego narzucenia określonych rozwiązań — zauważa Bogdan Fischer.

Dobrze znany przykład to program „Płatnik” stosowany przez ZUS. W tym przypadku obowiązek przesyłania części dokumentów drogą elektroniczną ustawa nałożyła na podmioty rozliczające się z ZUS. Płatnik działa na podstawie systemu operacyjnego Microsoft Windows, gdyż zastosowanie któregośkolwiek innego programu uniemożliwiłoby spełnienie ustawowych wymagań. Nie został jednocześnie stworzony analogiczny program dla innych platform systemowych.

Także inne działania — jak np. nieudostępnienie specyfikacji protokołu przesyłu danych — uniemożliwiają stworzenie innych programów współpracujących. Problematyczne w praktyce mogą być również rozwiązania oparte na wykorzystaniu bezpiecznego podpisu elektronicznego.

— Ten temat wrócił przy okazji ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, która od 21 lipca tego roku wprowadza obowiązek korzystania z bezpiecznego podpisu w kontaktach z ZUS (m.in. podpisywanie zgłoszeń do ubezpieczeń społecznych, deklaracje rozliczeniowe) przez płatników zatrudniających więcej niż 5 osób. Kolejny przykład to rozporządzenie Ministra Finansów z 14 lipca 2005 r. o wykorzystaniu bezpiecznego podpisu w wystawianiu e-faktur VAT — wylicza Bogdan Fischer.