Bolesław Szafrański[1]

Niezależność systemów bezpieczeństwa teleinformatycznego podmiotu publicznego od dostawców rozwiązań bezpieczeństwa teleinformatycznego

1. Uwagi wstępne

W artykule został omówione zagadnienia wpływające na bezpieczeństwo teleinformatyczne podmiotu publicznego, ze szczególnym podkreśleniem problemu niezależności podmiotów publicznych od dostawców rozwiązań w dziedzinie bezpieczeństwa informacyjnego. Z tego względu podstawowym celem i myślą przewodnią artykułu jest zwrócenie uwagi na to, jakie znaczenie dla bezpieczeństwa informacyjnego podmiotu publicznego ma nieuwzględnienie na etapie opracowywania materiałów przetargowych kwestii zagwarantowania niezbędnego poziomu niezależności tego podmiotu od ww. dostawców. Zagadnienie to, jak podkreślono we wnioskach końcowych, powinno stanowić integralną część wymagań dotyczących szeroko pojętego bezpieczeństwa informacyjnego. Warto przy tym pamiętać, że Zamawiający (udzielający zamówienia publicznego), przygotowując specyfikację istotnych warunków zamówienia, może swoje wymagania zawierać w opisie przedmiotu zamówienia, opisie warunków udziału w postępowaniu, opisie kryteriów, którymi zamawiający będzie się kierował przy wyborze najkorzystniejszej oferty, oraz w istotnych dla stron postanowieniach wprowadzonych do treści umowy. Biorąc to pod uwagę, trzeba na wstępie stwierdzić, że wspomniany wyżej aspekt bezpieczeństwa informacyjnego nadal jest w niewystarczającym stopniu doceniany i uwzględniany wśród istotnych warunków zamówienia. Do tej pory poza ogólnymi wytycznymi w niektórych dokumentach normatywnych nie ma regulacji prawnych oraz powszechnie uznawanych wytycznych metodycznych dotyczących tych kwestii. Dlatego sformułowane dalej

[1] Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Systemów Informatycznych.

zalecenia i wnioski są próbą wypełnienia tej luki z zastrzeżeniem, że powinny być traktowane jako autorskie propozycje i oceny Autora artykułu. Ponadto warto już w tym miejscu odnieść się do poprawności używania pojęcia bezpieczeństwo informacji. Zdaniem Autora trafniejsze merytorycznie i formalnie jest stosowanie szerszego pojęcia bezpieczeństwo informacyjne zamiast węższego – bezpieczeństwo informacji. Na takie szersze znaczenie wskazuje np. definicja jednej z trzech najważniejszych cech bezpieczeństwa, czyli dostępności, która według normy obejmuje nie tylko same informacje, lecz także związane z nimi aktywa („mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne".). Świadomie trywializując zasygnalizowany tu problem terminologiczny, można by stwierdzić, że informacje gromadzone w systemie informatycznym są najbezpieczniejsze, gdy nie działa funkcja ich udostępniania. Wtedy informacje są bezpieczne, ale organizacja jest pozbawiona zasilania informacyjnego. Stąd w dalszej części opracowania będziemy używać pojęcia bezpieczeństwa w szerszym sensie, tzn. pojęcia bezpieczeństwa informacyjnego danej organizacji (podmiotu). Bazą dla niniejszej publikacji są przede wszystkim ustawy Prawo Zamówień Publicznych, Ustawa o ochronie danych Osobowych, Ustawa o ochronie informacji niejawnych oraz wskazane w odpowiednich miejscach normy. Ogólne informacje na temat bezpieczeństwa informacyjnego wystarczające do lektury tekstu można znaleźć w dowolnej książce dotyczącej tego zagadnienia. Biorąc to pod uwagę, zrezygnowałem z zamieszczenia odwołań do poszczególnych pozycji literaturowych.

2. Istota i definicja niezależności

Kierownictwo podmiotu publicznego, a także działające w jego imieniu komórki odpowiedzialne za bezpieczeństwo informacyjne w ramach obowiązujących regulacji prawnych muszą na każdym etapie zachować możliwości swobodnego, w określonym przez siebie przedziale czasu, kształtowania systemu bezpieczeństwa informacyjnego. W sytuacji dominującego lub wyłącznego dostawcy kluczowych elementów tego systemu ww. swoboda może być znacząco ograniczona. Wystarczy rozpatrzyć sytuację, gdy kierownictwo podmiotu publicznego straci zaufanie (z jakichkolwiek przyczyn: gospodarczych, merytoryczno-technicznych, prawnych, a nawet niemożliwych do wykluczenia przyczyn politycznych) do dominującego dostawcy. Czy wtedy będzie w stanie zareagować zgodnie z powyższą zasadą? Jeśli więc aktualnie występujące

uzależnienie nie daje możliwości takiego zareagowania, to każda nowa inwestycja w obszar bezpieczeństwa informacyjnego musi przybliżać podmioty publiczne do odzyskania wspomnianej swobody. Jest to jeden z najważniejszych warunków utrzymania bezpieczeństwa informacyjnego. W przeciwnym razie bezpieczeństwo informacyjne podmiotu publicznego będzie pozorne, a koszty eksploatacji i utrzymania systemu bezpieczeństwa mogą być ekonomicznie nieuzasadnione. Dlatego planowanie rozwoju rozwiązań bezpieczeństwa jest istotne dla prawidłowego i ekonomicznego działania podmiotu publicznego. W odniesieniu do rozwiązań teleinformatycznych jest to zagadnienie złożone ze względu na dynamikę zmian technologii teleinformatycznych wykorzystywanych przez podmioty publiczne oraz dynamikę zmian w obszarze możliwości wykrywania podatności rozważań informatycznych na ciągle doskonalone metody ataków teleinformatycznych. Dodatkowo wzrasta złożoność zależności między elementami systemów informatycznych, w tym zwłaszcza z chwilą podjęcia decyzji o odejściu od koncepcji niemalże galwanicznej izolacji systemów informatycznych administracji publicznej od systemów informatycznych otoczenia gospodarczego i społecznego.

Dlatego ocena wdrażanych rozwiązań teleinformatycznych w administracji publicznej z punktu widzenia zachowania bezpieczeństwa będzie wymagać rosnącej wiedzy eksperckiej: technicznej, prawnej i organizacyjno-zarządczej. Z oczywistych powodów dostawcy rozwiązań starają się dostarczać wiele produktów o uzupełniającej się funkcjonalności tak, aby można było za ich pomocą wdrożyć kompletne rozwiązanie teleinformatyczne, łącznie z systemem bezpieczeństwa. Celem biznesowym dostawców może być dążenie do tego, aby całe rozwiązanie było oparte wyłącznie na dostarczanych przez nich produktach. Takie podejście może mieć istotne zalety, np. jeden system monitorowania, zarządzania oraz raportowania, łatwiejsza integracja, jednolity system pomocy technicznej i serwisu, mniejsze nakłady na szkolenia itd. Z punktu widzenia bezpieczeństwa informacyjnego nawet przy tak oczywistych zaletach bezwarunkowa akceptacja takiego podejścia może być nieuzasadniona, a nawet niebezpieczna!

Dlatego należy zwrócić uwagę na ryzyka polegające na tendencji lub pojedynczych próbach celowego, długoterminowego uzależniania podmiotu publicznego od dostarczonych rozwiązań prowadzących do tego, by:

- nie było możliwości rozwoju posiadanego rozwiązania za pomocą produktów innych dostawców,
- rozwój posiadanego rozwiązania był nadmiernie kosztowny,
- rozwój posiadanego rozwiązania nie mógł być przeprowadzony w akceptowalnym czasie.

Gdyby taka sytuacja miała miejsce, to w efekcie podmiot publiczny mógłby podlegać dyktatowi producenta (dostawcy) i być zmuszanym do zakupu lub eksploatacji rozwiązań o gorszych parametrach niż rozwiązania innych producentów i o bardziej ograniczonych możliwościach rozwojowych. Tego rodzaju zagrożeń, bez przeprowadzenia dogłębnej analizy ryzyka uwzględniającej nie tylko stan obecny, ale także przyszłość funkcjonowania systemów informatycznych, nie da się właściwie uwzględnić w procedurach udzielania zamówień publicznych. Może to prowadzić do sytuacji, w której proponowane rozwiązanie w momencie zakupu spełnia postawione wymagania, ale w przyszłości może generować problemy wynikające m.in. z ograniczeń rozwoju albo z faktu, że rozwój rozwiązania może okazać się możliwy, ale znacznie przekraczający dopuszczalne dla podmiotu koszty.

Rozpatrując problem niezależności podmiotu publicznego od dostawców rozwiązań z dziedziny bezpieczeństwa teleinformatycznego, proponujemy na użytek niniejszego artykułu przyjąć następującą definicję: system bezpieczeństwa teleinformatycznego podmiotu publicznego jest niezależny od dostawców rozwiązań bezpieczeństwa teleinformatycznego, jeśli w akceptowalnym przez podmiot publiczny czasie oraz po akceptowalnych kosztach można zastąpić posiadane rozwiązanie jednego producenta rozwiązaniami innych producentów o nie gorszych właściwościach funkcjonalno-technicznych.

W ogólnym przypadku można mówić o zależności uzasadnionej i zależności szkodliwej. Uzasadniona zależność występuje wtedy, gdy system bezpieczeństwa podmiotu publicznego mimo istnienia pewnego poziomu zależności spełnia wymagania definicji niezależności. Każda inna zależność jest szkodliwa i stanowi zagrożenie, bo narusza bezpieczeństwo informacyjne.

Szczegółowa dyskusja wszystkich problemów niezależności bądź zależności wykracza poza ramy umowy. Warto jednak zwrócić uwagę choćby na niektóre zagrożenia wynikające z być może celowego działania dostawców rozwiązań informatycznych. Część rozwiązań z dziedziny zabezpieczeń systemów sieciowych wymusza z przyczyn biznesowych, a nie koncepcyjnych stosowanie określonego sprzętu, który w żadnej mierze nie jest związany z bezpieczeństwem informacyjnym, np. stacji roboczych określonego producenta i typu lub określonego, ściśle dedykowanego typu czytników kart procesorowych. Wymuszenia te nie podnoszą poziomu bezpieczeństwa, nie zapewniają dodatkowej, korzystnej funkcjonalności, ale przez celowo wprowadzone wyłączne cechy identyfikacyjne w niedopuszczalny sposób uzależniają podmioty publiczne od określonych rozwiązań lub określonego dostawcy. Kolejnym rodzajem szkodliwego uzależnienia jest zakup urządzeń wielofunkcyjnych od producenta, który nie jest w stanie

zapewnić rozwoju każdej z funkcji do poziomu rosnących wymagań podmiotów publicznych lub poziomu wiodących rozwiązań rynkowych. Innym zagrożeniem jest dopuszczenie do tworzenia systemu według tzw. łańcucha zależności, polegającego na tym, że wymiana jednego z urządzeń wymusza automatycznie, zgodnie z celową polityką dostawcy, wymianę innych w „łańcuchu".

Podstawowym warunkiem uniknięcia szkodliwej zależności jest uświadomienie sobie faktu jej istnienia oraz zrozumienie i docenienie zagrożeń wynikających z niej dla bezpieczeństwa informacyjnego. Konieczność zapewnienia niezależności powinna znaleźć swoje odzwierciedlenie w dokumentacji systemu bezpieczeństwa informacyjnego, zwłaszcza w polityce bezpieczeństwa. Mierzalne wymagania odnoszące się do tak rozumianej niezależności powinny wynikać z przeprowadzonej pod tym kątem analizy ryzyka.

Specyfikacja czynników służących zapewnieniu niezależności systemów bezpieczeństwa teleinformatycznego od dostawców rozwiązań bezpieczeństwa teleinformatycznego obejmuje następujące najważniejsze zagadnienia:

- zgodność z normami i standardami,
- certyfikacja, audyt, weryfikacja pilotowa,
- otwartość, powszechność, referencje rynkowe.

3. Zgodność z normami i standardami

Istotnym celem tworzenia i upowszechniania norm oraz standardów jest wypracowanie warunków do poprawnego współdziałania produktów różnych dostawców. Bardzo rzadko się zdarza, żeby normy lub standardy opracowywane i upowszechniane przez międzynarodowe instytucje normalizacyjne powstawały „pod dyktando" jednego, dominującego producenta (w przeszłości takie praktyki występowały często). Z samej istoty norm i standardów pośrednio wynika, że dotyczą rozwiniętego już rynku i tym samym najczęściej należą do zbioru obligatoryjnych wymagań projektowych adresowanych do otwartego rynku produktów i producentów, a więc są przeznaczone dla różnych producentów rozwiązań o tożsamych lub zbliżonych funkcjonalności i przeznaczeniu. Z tego powodu w znacznym zakresie zapewniają niezależność od dostawców. Dlatego w razie potrzeby rozwiązanie z dziedziny bezpieczeństwa, działające skutecznie i zgodnie z oczekiwaniami, może być złożone z wielu elementów pochodzących od różnych producentów, a dzięki temu będzie poprawnie funkcjonować i może być przy tym centralnie monitorowane (np. zestaw ruter

firmy-1, przełącznik firmy-2, firewall firmy-3, zabezpieczenia przed intruzami firmy-4 itp.).

Opracowaniem standardów zajmują się międzynarodowe instytucje. Jak wcześniej napisano, najbardziej uznaną z nich, również w dziedzinie bezpieczeństwa, jest International Organization for Standarization (ISO) („ISO zajmuje się organizacją i ustanawianiem międzynarodowych standardów technologicznych i handlowych. Powstała w 1949 r. na skutek porozumienia najważniejszych na świecie organizacji standaryzacyjnych: amerykańskiej ANSI, niemieckiej DIN, francuskiej AFNOR i brytyjskiej BSI. Członkami ISO mogą być wyłącznie agencje rządowe zajmujące się standaryzacją lub podobne do samego ISO pozarządowe organizacje standaryzacyjne").

W Polsce opracowywaniem i wprowadzaniem norm zajmuje się **Polski Komitet Normalizacyjny (PKN)**. Polska Norma (PN) jest dokumentem dobrowolnym, ale jej przestrzeganie zapewnia duże korzyści, także w zakresie niezależności od dostawców i swobodnego rozwoju systemów teleinformatycznych (wg normy PN-EN 45020:2000 „Norma, to dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną ustalający – do powszechnego i wielokrotnego stosowania – zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie. Zaleca się, aby normy były oparte na osiągnięciach zarówno nauki, techniki, jak i praktyki oraz miały na celu uzyskanie optymalnych korzyści społecznych".).

Podstawowym sposobem badania zgodności z wybraną normą lub standardem jest przeprowadzenie procesu autoryzacji w czasie, w którym zwykle zabiega się, by:

- nowe urządzenia miały odpowiednie dopuszczenia, sankcjonujące ich przeznaczenie i sposób użycia.
- osoba odpowiedzialna za utrzymanie środowiska bezpieczeństwa systemu informatycznego powinna dysponować właściwym dopuszczeniem do pełnienia tej roli, co ma zapewnić spełnienie stosownych wskazań polityki i wymagań bezpieczeństwa,
- tam gdzie jest konieczne, sprzęt i oprogramowanie było zgodne z innymi komponentami systemu.

Osoba wydająca dopuszczenie może się oprzeć na zapewnieniach producenta, wynikach procesu autoryzacji ogłaszanych publicznie przez wiarogodne instytucje autoryzacyjne lub na wynikach własnych procedur autoryzacyjnych (wykonywanych samodzielnie lub zlecanych). Planując zakupy rozwiązań teleinformatycznych, warto jest zweryfikować ich zgodność z obowiązującymi normami

i standardami. Wsparcie wielu standardów świadczy o „otwartości" rozwiązania. Problematyka standardów i norm jest bardzo złożona i trudna, zarówno ze względu na ich liczbę, stopień uwikłania, jak i bardzo specjalistyczną wiedzę niezbędną do zrozumienia ich znaczenia i właściwego zinterpretowania.

Komórki odpowiedzialne za bezpieczeństwo teleinformatyczne powinny zwrócić uwagę na to, że niektórzy producenci celowo i w sposób niejawny mogą stosować odstępstwa od standardów w celu osiągnięcia zamierzonych korzyści, np. określonego efektu marketingowego, handlowego. Przykładowo: komponenty serwera WWW oraz klienta usługi WWW (przeglądarki) jednego z dostawców mogłyby być celowo poddane modyfikacji sposobu działania, tak aby klient, korzystający zarówno z usługi serwera WWW, jak i z przeglądarki WWW pochodzących od tego właśnie dostawcy, miał zapewnioną wyższą szybkość działania. Teoretycznie więc klient może stosować w komunikacji sieciowej tylko jeden z komponentów pochodzący od tego dostawcy i używać innego, dowolnego produktu stanowiącego drugą stronę komunikacji, ale choć taki scenariusz działania jest możliwy, to efekty wydajnościowe będą dużo niższe.

4. Certyfikacja, audyt, weryfikacja pilotowa

Profesjonalne i jednoznaczne sprawdzenie zgodności produktów teleinformatycznych, w tym z dziedziny bezpieczeństwa teleinformatycznego, ze standardami i normami jakości z punktu widzenia technicznej realizowalności wymaga wysokiej klasy specjalistów, wiarogodnych procedur i odpowiednio wyposażonych laboratoriów certyfikacyjnych. Jednakże spełnienie tych warunków nie wystarczy, jeśli instytucja wykonująca to sprawdzenie nie potwierdzi w praktyce swej wiarogodności i niezależności.

Proces certyfikacji tym różni się od procesu autoryzacji, że może być wykonany jedynie przez autoryzowane do tego celu organizacje. Najczęściej uznaje się, że dla systemów zabezpieczeń najważniejsza jest certyfikacja Common Criteria for IT Security Evaluation. Aktualny wykaz produktów poddanych certyfikacji, w tym przede wszystkim tych, dla których skończyła się ona pozytywnym rezultatem, można znaleźć na stronie: http://niap.nist.gov/cc-scheme/vpl/vpl_type.html. Historycznie rzecz biorąc, innymi ważnymi międzynarodowymi standardami w zakresie oceniania bezpieczeństwa teleinformatycznego, znanymi w Polsce, są m.in.: Trusted Computer System Evaluation Criteria (TCSEC, czyli tzw. pomarańczowa księga – Orange Book), Information Technology Security

Evaluation Criteria (ITSEC), Control Objectives for Information and Related Technology (COBIT – standard ISACA).

Proces certyfikacji jest prowadzony zwykle w wąskim zakresie, bo dotyczy wybranych parametrów lub funkcji (np. bezpieczeństwa elektrycznego, bezpieczeństwa sieciowego, ściśle określonych standardów). Same wyniki certyfikacji nie wystarczą do oceny praktycznej przydatności produktów, również w kwestii wyżej zdefiniowanej niezależności. Kompletną ocenę rozwiązania można uzyskać na podstawie audytu, który weryfikuje jakość i poprawność całego rozwiązania zarówno pod względem technicznym, jak i z punktu widzenia wymagań zawartych w polityce bezpieczeństwa obowiązującej dany podmiot. Proces audytorski wymaga bardzo zaawansowanej wiedzy specjalistycznej w odniesieniu do produktów wykorzystywanych w danym rozwiązaniu, środowiska informatycznego, w którym dane rozwiązanie ma być eksploatowane, i wiedzy metodycznej pozwalającej na weryfikację „audytowanego" rozwiązania z punktu widzenia polityki i praktycznych zasad zarządzania bezpieczeństwem. Z tego powodu prace audytorskie są zwykle prowadzone przez wieloosobowe zespoły, grupujące audytorów posiadających zaawansowane stopnie specjalizacji zawodowej (np. Juniper Networks Certified Internet Specialist, Cisco Certified Internetwork Professional, Check Point Certified Security Expert) oraz audytorów metodyków. Ostatecznym weryfikatorem danego rozwiązania, zwłaszcza ze względu na współdziałanie wielu elementów, może być dopiero wdrożenie pilotowe.

5. Otwartość, powszechność, referencje rynkowe

Niezależność podmiotu publicznego od dostawców rozwiązań systemów bezpieczeństwa może w dużym zakresie zostać zapewniona dzięki świadomemu stosowaniu rozwiązań powszechnie używanych (istotnymi wskazówkami w tym względzie są raporty niezależnych organizacji na temat preferencji rynkowych). Takie rozwiązania, nazywane często „otwartymi", najczęściej spełniają obowiązujące aktualnie standardy i dzięki temu mogą współdziałać z produktami i systemami innych dostawców.

Odmienne postępowanie, czyli stosowanie rozwiązań niszowych, może narazić ich nabywców na duże ryzyko związane z ograniczoną niezależnością, ograniczeniem możliwości ich rozwoju, trudnościami z zapewnieniem zgodności ze standardami oraz zapewnieniem ciągłości, rzetelności i jakości wsparcia. Autor

artykułu nie nawołuje do bezwarunkowej rezygnacji z rozwiązań mniej znanych lub niszowych, ale zachęca do wnikliwego rozpatrzenia ryzyk z tym związanych.

Wydaje się, że dobrą praktyką jest stosowanie produktów ogólnie dostępnych na rynku i unikanie rozwiązań „autorskich", ponieważ dostawca, tworząc rozwiązanie „dedykowane", ma duże możliwości wprowadzenia własności, które będą funkcjonowały poprawnie tylko z produktami tego producenta.

Aktualnie istnieje duża niepewność co do zasad bezpieczeństwa informacyjnego. Dotyczy ona rozwiązań opartych na oprogramowaniu „open source". Tego typu rozwiązania nie mają jeszcze długiej historii i dlatego powinny być stosowane szczególnie ostrożnie, a w przypadku zamiaru zastosowania ich w procesach krytycznych (a takimi z pewnością są wszystkie procesy bezpieczeństwa informacyjnego) dla danej organizacji, powinny być poddane audytowi i zweryfikowane w trakcie pilotowego wdrożenia.

Ponadto w przypadku nabywania rozwiązań z dziedziny bezpieczeństwa informacyjnego zgodnie z zasadami określonymi w ustawie Prawo Zamówień Publicznych, należy wprowadzić odpowiednie zapisy dotyczące niezależności do Specyfikacji Istotnych Warunków Zamówienia. Przykładowe zapisy mogłyby przyjąć następujące brzmienie:

- nabywane rozwiązanie powinno zapewnić:
  - bezpieczeństwo eksploatacji, także gdyby którykolwiek z producentów wykorzystywanych produktów zaniechał obsługi jego elementów,
  - możliwość migracji na platformę sprzętową innego producenta,
  - możliwość zmiany systemu operacyjnego serwerów na właściwy dla innej platformy sprzętowej lub na system typu „open source", pochodzący od producenta niezależnego wobec systemu zastępowanego,
  - możliwość migracji na platformę bazodanową pochodzącą od innego producenta lub na co najmniej jedną platformę bazodanową typu „open source", pochodzącą od producenta niezależnego wobec platformy zastępowanej,
  - zachowanie dostępność kodu źródłowego, aktualizowanego w środowisku rozwojowym Zamawiającego wraz z każdą wprowadzaną w systemie korektą oraz kompletnym, licencjonowanym środowiskiem rozwojowym,
  - prawo do wprowadzania przez Zamawiającego lub osoby działające w jego imieniu potrzebnych zmian i uzupełnień (o ile to w ogóle będzie możliwe), aż do możliwości pełnego przejęcia konserwacji rozwiązania włącznie.

Z uwagi na rozwój rynku rozwiązań w dziedzinie bezpieczeństwa informacyjnego oraz rozwój i upowszechnienie prac standaryzacyjnych można określić ścieżkę dojścia do sytuacji, w której osiągnie się wymagany poziom niezależności od jakiegokolwiek dostawcy. Z tego względu formułowanie w SIWZ wymagań

dotyczących niezależności jest uzasadnione, a same wymagania często możliwe do spełnienia.

Aktualnie w podmiotach publicznych eksploatowane są systemy, które mogą cechować się szkodliwą zależnością od dominujących dostawców. Stwierdzenie takiej sytuacji nie musi oznaczać, że celem podmiotu publicznego powinno być automatyczne eliminowanie tego dominującego dostawcy z partnerstwa w budowie niezależnego systemu bezpieczeństwa. Wręcz przeciwnie taki partner może spełnić bardzo istotną rolę w procesie pozbawiania cech zależności dostarczonego przez siebie, najczęściej bardzo kosztownego rozwiązania od jednego, wyłącznego dostawcy (np. dostawcy sprzętu). Musi się jednak zgodzić z tym, że również jego rozwiązanie, zgodnie z obowiązującymi lub zalecanymi normami bezpieczeństwa, powinno spełniać publiczne znane, jawne standardy bezpieczeństwa w taki sposób, by do ich implementacji można było użyć rozwiązań różnych dostawców lub w razie potrzeby zastąpić je produktami innych dostawców.

6. Wnioski

- Wszystkie wymagania bezpieczeństwa, w tym zasygnalizowane w artykule kwestie niezależności systemu bezpieczeństwa, powinny być zidentyfikowane i uzasadnione już w fazie opracowywania wymagań dla inwestycji informatycznej. Muszą one stanowić integralną część ogólnego biznesowego modelu systemu informacyjnego podmiotu publicznego. Należy upowszechnić wiedzę na temat znaczenia, pomijanego lub lekceważonego problemu niezależności systemu bezpieczeństwa informacyjnego.
- Niezbędne jest zapewnienie, że bezpieczeństwo informacyjne zostanie wbudowane w procesy informacyjne, zwłaszcza decyzyjne, i będzie dotyczyć wszystkich elementów infrastruktury informacyjnej podmiotu publicznego. Wymagania bezpieczeństwa powinny być uzgodnione i zidentyfikowane przed lub w trakcie tworzenia Specyfikacji Istotnych Warunków Zamówienia.
- Wymagania bezpieczeństwa i środki zabezpieczeń powinny odzwierciedlać wartość biznesową odnośnych aktywów informacyjnych oraz potencjalne szkody dla działalności biznesowej, które mogłyby być wynikiem uszkodzeń lub braku zabezpieczeń w poszczególnych systemach informatycznych. Im większa wartość biznesowa procesów informacyjnych, tym większe znaczenie ma uwzględnienie czynnika niezależności rozwiązań bezpieczeństwa od

dostawców rozwiązań informatycznych obejmujących również mechanizmy bezpieczeństwa.

- Podstawą prowadzenia analizy wymagań bezpieczeństwa i określania rodzajów zabezpieczeń, które je spełniają, jest szacowanie ryzyka i zarządzanie ryzykiem. Zabezpieczenia wprowadzane na etapie projektowania są znacząco tańsze we wprowadzeniu i w utrzymaniu niż te, które są dodane w trakcie lub po wdrożeniu systemu. **Odnosząc się do treści artykułu, należy zadbać, by stosowane metody identyfikacji i oceny ryzyka uwzględniały opisaną w artykule niezależność systemu bezpieczeństwa informacyjnego (teleinformatycznego).** Ważne jest, by utrwalić zasadę ustawicznych, okresowych i doraźnych przeglądów ryzyka tak, aby:
  - uwzględnić zmiany wymagań dotyczących działalności biznesowej i priorytetów, zwłaszcza wtedy, gdy w podmiocie publicznym potencjalnie mogą zaistnieć przesłanki rozszerzenia zbioru procesów krytycznych,
  - uwzględnić nowe zagrożenia i podatności,
  - potwierdzić bezpieczny stan systemu informacyjnego.
- Zapewnienie bezpieczeństwa teleinformatycznego w procesach rozwojowych wymaga ścisłej kontroli środowiska projektowego i przede wszystkim eksploatacyjnego. Przed rozpoczęciem prac nad zmianami konieczne jest dokonanie „profilaktycznej" oceny ryzyk, których zmaterializowanie się w toku prowadzenia prac rozwojowych lub naprawczych może niekorzystnie wpłynąć na ograniczenie niezależności systemu bezpieczeństwa informacyjnego. Ryzyka mogą dotyczyć zarówno istoty wprowadzanych zmian, jak i sposobu ich wprowadzania. Właściwa ocena ryzyka może np. doprowadzić do ustanowienia rygorystycznie przestrzeganych procedur formalnych, w tym np. ograniczenia możliwości dostępu programistów wyłącznie do tych części systemu, które są im niezbędne do wprowadzenia uzgodnionych zmian.
- Właściwe zabezpieczenia i środki monitorowania, dzienniki audytu lub dzienniki zawierające zapisy czynności dotyczących prac rozwojowych lub naprawczych powinny być zaprojektowane jako część systemu bezpieczeństwa. Dobrą praktyką, szczególnie użyteczną z punktu widzenia niezależności, jest utworzenie i utrzymywanie osobnych środowisk, rozwojowego i testowego, oddzielonych od środowiska produkcyjnego.

* * *

Independence of IT Security Systems of Public Units from IT Security Solutions Providers

Abstract

The article discusses the issue of the independence of public units from IT security solutions providers. After presenting the essence and the definition of such independence, there were discussed some actions to be taken to minimise the risk of excessive dependence, among others, the issue of applying recognised norms and practices, following the outcomes of certification processes, as well as taking into account the independence discussed in the article in risk analyses. The summary points out that all the security requirements, including the issue of the security systems independence touched on in the article, should be verified and justified already in the phase of elaborating on given IT investment requirements. They need to constitute an integral part of the general business IT system model of a given public unit. Therefore, the knowledge on the security system independence, often omitted or disregarded, should be disseminated.

Keywords: IT security, public unit, independence of public units from IT security solutions providers