BIBLIOTECZKA IZBY RZECZOZNAWCÓW PTI

Bezpieczeństwo danych w sektorze publicznym

CC BY

35 lat PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Bezpieczeństwo danych w sektorze publicznym

WARSZAWA 2016

ISBN 978–83–60810–84-2 (druk)
ISBN 978–83–60810–85-9 (e-book)

Praca ta objęta jest licencją Creative Commons Uznanie Autorstwa 3.0 Polska.
Aby zapoznać się z kopią licencji, należy odwiedzić stronę internetową
http://creativecommons.org/licenses/by/3.0/pl/legalcode lub wysłać list do
Creative Commons, 543 Howard St.,5th Floor, San Francisco, California, 94105, USA.

CC by POLSKIE TOWARZYSTWO INFORMATYCZNE 2016

Redakcja: Tomasz Szatkowski
Recenzenci:
dr inż. Marek Bolanowski – Politechnika Rzeszowska
dr inż. Andrzej Paszkiewicz – Politechnika Rzeszowska
prof. Politechniki Warszawskiej dr hab. Kazimierz Waćkowski

Korekta: Ewa Ignaczak
Skład: Marek W. Gawron

Wydawca:
POLSKIE TOWARZYSTWO INFORMATYCZNE
00-394 Warszawa, ul. Solec 38 lok. 103
tel. +48 22 838 47 05
e-mail: pti@pti.org.pl
www.pti.org.pl

Druk i oprawa:
ELPIL
08-110 Siedlce, ul. Artyleryjska 11
tel. +48 25 643 65 51
e-mail: info@elpil.com.pl

Wszystkie tabele, rysunki i wykresy, o ile nie zaznaczono inaczej, zostały wykonane przez Autorów

Spis treści

Szanowni Państwo,
mamy przyjemność przekazać w Państwa ręce czwartą książkę z cyklu wydawniczego Polskiego Towarzystwa Informatycznego ***Biblioteczka Izby Rzeczoznawców PTI***.

Celem cyklu jest przedstawienie treści mogących zainteresować zarówno osoby zajmujące się zawodowo informatyką, jak i tych z Państwa, którzy w swojej pracy stykają się z zagadnieniami i problemami związanymi z informatyką.

Zadania wykonywane przez instytucje publiczne, niezależnie od ich formy organizacyjnej czy prawnej, wymagają zazwyczaj przetwarzania zbiorów danych. Systemy informacyjne są coraz bardziej narażone na niepożądane ingerencje, w miarę wzrostu świadomości dotyczącej wartości rynkowej informacji i jej oddziaływania na przewagę konkurencyjną. Straty wynikające z naruszenia bezpieczeństwa informacji są trudne do oszacowania. Mając na uwadze rosnące znaczenie systemów informacyjnych instytucji publicznych celowym wydaje się przeprowadzenie analizy stanu bezpieczeństwa informacji i danych w tych organizacjach oraz sformułowanie na ich podstawie wniosków i potencjalnych zaleceń.

Monografia składa się z sześciu rozdziałów przedstawiających tematykę dotyczącą szeroko rozumianego bezpieczeństwa danych, z uwzględnieniem specyfiki działania instytucji publicznych. Autorami czwartego tomu z cyklu ***Biblioteczka Izby Rzeczoznawców PTI*** są eksperci, rzeczoznawcy Polskiego Towarzystwa Informatycznego, specjalizujący się w tematyce polityki bezpieczeństwa i ochrony danych.

Zapraszamy do lektury niniejszego oraz poprzednich i kolejnych tomów z serii ***Biblioteczka Izby Rzeczoznawców PTI***.

Marian Noga

Prezes
Polskiego Towarzystwa Informatycznego

Tomasz Szatkowski

Dyrektor Izby Rzeczoznawców
Polskiego Towarzystwa Informatycznego

Warszawa 15 maja 2016 roku

Tadeusz Kifner

Elementy kultury organizacji IT wspomagające wdrażanie systemu bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji

Dbałość o bezpieczeństwo informacji

W obecnej dobie powszechności urządzeń komputerowych takich jak komputery osobiste, laptopy, tablety czy smartfony, nikogo nie dziwi potrzeba odpowiedniego zarządzania zasobami informacji, zgromadzonymi w pamięci tych urządzeń i instalowanie zabezpieczeń – programów antywirusowych czy zapór ogniowych (ang. *firewall*). Zasady bezpieczeństwa stały się praktykami rutynowymi dla osób wykorzystujących sieć Internet czy przekazujących dane między komputerami. Sami dostawcy sprzętu czy oprogramowania w ostatnim czasie mocno inwestują w zagadnienia bezpieczeństwa i starają się chronić swoje produkty, usługi i systemy, a w ten sposób pośrednio chronią swoich klientów i użytkowników.

Podobną tendencję widać również w sektorze administracji publicznej, która coraz bardziej otwiera swoje systemy informatyczne na społeczeństwo informacyjne. Systemy rządowe, samorządowe czy organizacji sektora publicznego oferują obsługę mieszkańców, podatników, przedsiębiorców w formie elektronicznej, a tym samym są bardziej narażone na podatności związane z używaniem zaawansowanej technologii i muszą zawierać odpowiednie zabezpieczenia. Wyraz dbałości o obywateli w zakresie zapewnienia bezpieczeństwa informacji o nich samych znajdziemy w wielu wprowadzanych aktach prawnych i rozporządzeniach, m.in. w:

- ustawie z 29 sierpnia 1997 roku o ochronie danych osobowych z póź. zm. [1];
- ustawie z 6 września 2001 roku o dostępie do informacji publicznej [2];

- ustawie z 18 września 2001 roku o podpisie elektronicznym [3];
- ustawie z 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną [4];
- ustawie z 17 lutego 2005 roku. o informatyzacji działalności podmiotów realizujących zadania publiczne (zwaną dalej Ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne) [5];
- ustawie z 5 sierpnia 2010 r. o ochronie informacji niejawnych [6];
- rozporządzeniu Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych [7].

Dużo wartościowych wskazań znaleźć można również w rekomendacjach branżowych, takich jak Rekomendacja D [8] czy Wytycznych IT [9] Komisji Nadzoru Finansowego, dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych, zakładach ubezpieczeń i reasekuracji, towarzystwach funduszy inwestycyjnych czy firmach inwestycyjnych.

Jednocześnie warto wskazać, że na szczeblu międzypaństwowym Unii Europejskiej czy w ramach NATO wskazywane są konkretne kierunki rozwoju obszarów bezpieczeństwa, publikowane w przykładowo w:

- Europejskiej Agendzie Cyfrowej Rady Europejskiej [10];
- Strategii Rozwoju Społeczeństwa Informacyjnego [11];
- Strategii Bezpieczeństwa Narodowego [12].

Rządzący RP również widzą konieczność prowadzenia działań mających na celu zapewnienie bezpieczeństwa infrastruktury teleinformatycznej Państwa i z tego względu stworzono m. in. Politykę Ochrony Cyberprzestrzeni RP [13], Doktrynę cyberbezpieczeństwa RP [14] i powołano Ministerstwo Cyfryzacji, a w nim specjalną jednostkę zajmującą się cyberbezpieczeństwem.

Regulacje prawne a sposoby zarządzania bezpieczeństwem informacji

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 ro w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych

wymagań dla systemów teleinformatycznych (dalej jako Krajowe Ramy Interoperacyjności, KRI) [15] wskazuje na wprost minimalne wymagania dla systemów teleinformatycznych, dotyczące zapewnienia bezpieczeństwa przy wymianie informacji. W paragrafie 20 znajdujemy szeroko opisane zasady przetwarzania danych nakazujące konieczność stosowania szeregu praktyk zarządczych w formie utrzymywanego i doskonalonego systemu zarządzania bezpieczeństwem informacji, który ma zapewnić poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Definicja systemu zarządzania bezpieczeństwem wraz z atrybutami wydaje się przeniesiona wprost z Polskiej Normy PN-ISO/IEC 27001:2007 [16], gdzie zdefiniowano pojęcie systemu zarządzania bezpieczeństwem informacji jako część całościowego systemu zarządzania, składającego się z procesu ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. W treści KRI wskazano, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie szeregu działań, zmierzających do zagwarantowania bezpieczeństwa informacji, rozumianego jako utrzymanie odpowiedniego poziomu atrybutów informacji. Klasycznymi atrybutami bezpieczeństwa informacji wyszczególnionymi w normie PN-ISO/IEC 27001:2007 są:

- poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności informacji,
- dostępność – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.

Dodatkowo wskazuje się również inne własności informacji takie jak: autentyczność, rozliczalność, niezaprzeczalność, niezawodność [16].

Norma ISO 27001, a raczej grupa norm dotyczących systemu bezpieczeństwa informacji[1], oparta jest na podejściu procesowym i wykorzystuje model Planuj – Wykonuj – Sprawdzaj – Działaj (PDCA, tj. *Plan – Do – Check – Act*), który stosowany jest dla całej struktury procesów Systemów Zarządzania Bezpieczeństwem Informacji. W załączniku A normy ISO/IEC 27001:2007 wyróżniono jedenaście obszarów, mających wpływ na bezpieczeństwo informacji w organizacji, które należy uregulować:

- Polityka bezpieczeństwa;
- Organizacja bezpieczeństwa informacji;
- Zarządzanie aktywami;
- Bezpieczeństwo zasobów ludzkich;
- Bezpieczeństwo fizyczne i środowiskowe;
- Zarządzanie systemami i sieciami;
- Kontrola dostępu;
- Zarządzanie ciągłością działania;
- Pozyskiwanie, rozwój i utrzymanie systemów informatycznych;
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- Zgodność z wymaganiami prawnymi i własnymi standardami [16].

Sposób zabezpieczenia tych obszarów zależy od wymagań biznesowych i powinien być oparty na przeprowadzonej analizie ryzyka.

Warto wspomnieć również o innym *de facto* branżowym standardzie, COBIT 4.1 [17], gdzie kryteria dotyczące zarządzania i przetwarzania informacją są inaczej sformułowane niż w normie ISO 27001. Opisuje on 34 wysokopoziomowe procesy, obejmujące 210 celów kontrolnych pogrupowanych w czterech domenach: planowanie i organizacja, nabywanie i wdrażanie, dostarczanie i wsparcie oraz monitorowanie i ocena. Metodyka ta bardziej skupia

[1] Grupa norm 2700x opisuje następujące obszary: System Zarządzania Bezpieczeństwem Informacji (SZBI) – podstawy i terminologia; SZBI wymogi – charakter normatywny; Praktyczne zasady zarządzania bezpieczeństwem informacji – zalecenia; SZBI wytyczne wdrożenia; SZBI pomiar; Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji; Wymagania dla jednostek prowadzących audyt i certyfikację SZBI; Wytyczne dla audytorów SZBI; Wytyczne bazujące na 27001 do zarządzania BI dla sektora telekomunikacji; Bezpieczeństwo sieci – Podstawy i pojęcia; Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002.

się na wykorzystaniu biznesowym informacji i jej zastosowaniu w procesach biznesowych. Z tego względu lista atrybutów jest inna, z zastrzeżeniem, że istnieje możliwość znalezienia referencji między wymaganiami szczegółowymi COBIT, a ISO 27001.

Lista atrybutów przedstawia się następująco:

- Skuteczność (ang. *effectiveness*) – cecha informacji używanej w procesie biznesowym. Skuteczna informacja to taka, która jest odpowiednia, istotna, dostarczona na czas w poprawny, spójny i nadający się do użycia sposób.
- Wydajność (ang. *efficiency*) – własność informacji dostarczonej optymalnie, czyli w sposób najbardziej produktywny, ekonomicznie uzasadniony i z użyciem odpowiednich środków.
- Poufność (ang. *confidentiality*) – właściwość w pełni zbieżna z atrybutami informacji określonymi w grupie norm ISO 2700x, dotycząca ochrony wrażliwej informacji przed nieautoryzowanym dostępem.
- Integralność (ang. *integrity*) – cecha informacji, która jest kompletna i dokładna, a także jest ważna, czyli stanowi wartość dla strony biznesowej.
- Dostępność (ang. *availability*) – odnosi się do stanu, w którym informacja jest dostępna wtedy, gdy proces biznesowy jej potrzebuje, a jednocześnie dotyczy stanu zachowania potrzebnych środków i zdolności do działania procesu biznesowego.
- Zgodność (ang. *compliance*) – mówi o zgodności z prawem i regulacjami wewnętrznymi czy branżowymi, a także ze zobowiązaniami kontraktowymi.
- Wiarygodność (ang. *reliability*) – własność stanowiąca o dostarczaniu odpowiedniej informacji dla kierownictwa organizacji, aby mogło podejmować właściwe decyzje, zarządzać procesami i pełnić swoją rolę zarządczą.

COBIT definiuje więc szerszą perspektywę i opisuje całościowo wykorzystanie informacji w organizacji i w jej procesach. Mimo szerszego patrzenia na sprawy bezpieczeństwa, metodyka ta nie jest bezpośrednio promowana do wdrożenia w administracji publicznej. Obecnie raczej stosuje się ją do oceny

stanu organizacji IT i w systemie kontroli zarządczej, opierając na wymaganiach COBIT odnośnie czynności audytorów i kontrolerów.

W ustawach, dokumentach formalnych czy politykach administracji publicznej wskazuje się pośrednio potrzebę kontroli w oparciu o wymogi wynikające z COBIT, ale samego wdrożenia do zarządzania organizacją IT (ang. *framework*) już się nie wymaga. Między innymi rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych [18] wskazuje, że osobą uprawnioną do przeprowadzania czynności kontrolnych jest osoba posiadająca między innymi certyfikaty CISA (ang. *Certified Information System Auditor*) oraz CGEIT (ang. *Certified in the Governance of Enterprise IT*). Osoby tytułujące się tymi certyfikatami, zgodnie z obowiązującym ich kodeksem etycznym, powinny wykorzystywać odpowiednie narzędzia kontrolne i zarządcze, co naturalnie wskazuje na promowany przez Stowarzyszenie ISACA standard COBIT [19].

Wdrożenie wymagań wynikających z COBIT w jednostkach publicznych jest dużo trudniejsze z uwagi na większy zakres uregulowania i wdrożenia procesów IT. Oprócz samych kwestii bezpieczeństwa technicznego i procesów bezpośrednio z tym związanych, w COBIT są regulowane również kwestie wynikające z innych procesów, np. projektowania i wytwarzania, utrzymania infrastruktury, dostarczanie usług czy obsługi użytkowników. Należy podkreślić, że pośrednio oczywiście te „dodatkowe" procesy IT wpływają na odporność rozwiązań informatycznych i krzepkość działania całej organizacji IT.

Wszystkie spośród 34 procesów COBIT zazębiają się w pełni z wytycznymi normy ISO 27001 [20]. Wydaje się więc kwestią czasu, kiedy to jednostki administracji publicznej zaczną wdrażać cele zarządcze według COBIT. Prawdopodobnie pomóc w tym może opublikowanie zapisów COBIT w formie normy, podobnie jak to miało miejsce z normą ISO 20000 i biblioteką wytycznych ITIL. Część 1 (Specyfikacja) i 2 (Reguły postepowania) normy Norma Technika informatyczna – Zarządzanie usługami [21] za-

wierają wymagania i rekomendacje bazujące na modelu Information Technology Infrastructure Library (ITIL), elementach Microsoft Operations Framework i COBIT.

COBIT został też wskazany w Rekomendacji D [8] Komisji Nadzoru Finansowego, dotyczącej zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, jako jeden z uznanych standardów międzynarodowych, dotyczących badania i oceny bezpieczeństwa informacji w systemach informatycznych.

COBIT definiuje pojęcie celów kontrolnych, czyli minimalnych dobrych praktyk, które powinien stosować personel IT i pracownicy jednostki, promowanych przez kierownictwo w celu zapewnienia kontroli nad każdym z procesów IT. Wskazanie tego wymaga zdefiniowania sposobu mierzenia poprawności zachowań. Kierownictwo powinno zatem zdefiniować praktyki kontrolne, czyli kluczowe mechanizmy zarządcze i kontrolne, które wspierają osiąganie celów oraz dają możliwość zapobiegania, wykrywania i naprawiania niepożądanych zdarzeń. Świat nie jest idealny – dlatego pracownikom IT trudno jest zawsze utrzymywać odpowiedni „kurs na cel". Kierownictwo, monitorując sytuację, wspomaga personel, podając deklaracje oczekiwanych wartości (kryteria sukcesu) i poziomy akceptowalnego ryzyka (jak dużo odstępstwa od zakładanego kursu jest jeszcze do zaakceptowania). Cały system kierowniczy oparty o wytyczne COBIT wspomaga definiować dobre praktyki zarządcze w każdym z 34 procesów, co przekłada się na oszczędność czasu, korzyści dla organizacji i brak błędów w definiowaniu „kursu". „Aby działalność IT skutecznie spełniała wymagania biznesowe, kierownictwo firmy powinno wdrożyć wewnętrzny system lub metodykę kontroli. Metodyka kontroli COBIT umożliwia zaspokojenie tych potrzeb poprzez:

- zapewnienie powiązania z wymaganiami biznesowymi;
- zorganizowanie działalności IT w ramach ogólnie akceptowanego modelu procesów;
- określenie głównych zasobów IT, które mają być wykorzystywane;
- zdefiniowanie celów kontroli zarządczej, które należy uwzględnić" [17: 5].

Najnowsza wersja COBIT, czyli 5, jeszcze bardziej skupia się na aspektach biznesowych i dostarczaniu wartości biznesowej przez technologię informatyczną, wymagając od organizacji dużej dojrzałości w obszarze zarządzania informatyką. Stąd wdrożenie wymogów COBIT 5 w polskich realiach wydaje się bardzo utrudnione.

Wdrożenie praktyk organizacyjnych i technicznych dotyczących bezpieczeństwa informacji

Wyzwania dla jednostek publicznych są coraz większe. Samo zapewnienie bezpieczeństwa informacji wymaga bardzo szerokiej specjalistycznej wiedzy i wsparcia ekspertów. Często wdrożenie regulacji wewnętrznych w zakresie bezpieczeństwa i ich okresowa aktualizacja nie jest wystarczająca z uwagi na zmieniające się warunki zewnętrzne. Konieczna jest zmiana kultury działania pracowników instytucji publicznych oraz dostawców usług informatycznych dla administracji. Podejście całościowe określone w wymaganiach COBIT i grupie norm ISO 27001 w dużej mierze daje gwarancję zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Ważnym elementem kultury pracy jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko (stosownie do wyników przeprowadzonej analizy) [15]. Pomóc w tym mogą uznane metodyki oceny ryzyka, a także ścisła współpraca z audytem wewnętrznym, w tym specjalizowanym w obszarze IT audytem technicznym.

Niestety, zazwyczaj administracja publiczna nie posiada wymaganych zasobów ludzkich oraz ekspertów z dziedziny bezpieczeństwa. Dlatego biorąc pod uwagę konieczność utrzymania działania skomplikowanego systemu powiązanych ze sobą aplikacji w sektorze administracji publicznej, wydaje się, że przeprowadzanie czynności sprawdzających (takich jak testy penetracyjne oraz niezależny audyt techniczny stosowanych rozwiązań), należy zlecać specjalistom z konkretnych dziedzin informatyki oraz certyfikowanym audytorom i rzeczoznawcom.

Testy penetracyjne

Przyjmuje się jako dobrą praktykę, że każde wdrożenie systemów otwartych na Internet (czyli dostępnych w sieci Internet) poprzedzają testy penetracyjne bezpieczeństwa, zapewniające bezpieczeństwo techniczne utrzymywanych systemów. Ich celem jest walidacja prawidłowości zastosowanych zabezpieczeń danych i oprogramowania oraz sprawności działania systemu przy zaplanowanej liczbie potencjalnych użytkowników.

Przykładowa lista zabezpieczeń będących przedmiotem testów może zawierać testy dotyczące m.in.:

- antysniffingu,
- skanowania portów sieciowych,
- podszywania się,
- filtrowania ruchu na zaporze sieciowej,
- ochrony przed atakiem Ping of Death,
- wykrywania i unieszkodliwiania usług nadmiernie wykorzystujących zasoby komputerowe,
- walidacji sesji szyfrowanych,
- sprawdzania integralności systemu plików,
- kontroli dostępu do usług zdalnych,
- odporności na włamanie techniczne,
- odporności na włamanie za pomocą środków socjotechnicznych.

Metody i techniki testów penetracyjnych zależą od samego systemu (środowisko, narzędzia wytwórcze, metody wytwarzania) i interfejsów z innymi systemami (liczba powiązań, sposób wymiany danych, uczestnictwo stron trzecich). Przykładowo można użyć ogólnodostępnych metodyk testów penetracyjnych, takich jak OWASP (Open Web Application Security Project) czy OSSTM (Open Source Security Testing Methodology).

Audyt technologiczny

Audyt technologiczny jest metodą identyfikacji słabych i mocnych stron organizacji poprzez dokonanie oceny środowiska IT. Badanie środowiska technologicznego IT oparte jest zazwyczaj na:

- wytycznych stowarzyszenia ISACA (wytyczne dla audytorów, COBIT, standardy audytowe),
- wytycznych dla audytorów wewnętrznych IIA (ang. *Institute of Internal Auditors*),
- wybranych standardach branżowych, np. ISO 27001 lub dobrych praktykach, np. ITIL, COBIT, TOGAF.

W ramach audytu technologicznego audytorzy stosują między innymi następujące techniki poznawcze:

- oględziny miejsc przetwarzania danych;
- przegląd stosowanego oprogramowania;
- analiza dokumentacji techniczno-technologicznej;
- analiza dokumentacji organizacyjnej i procesów biznesowych;
- testy samodzielne i obserwacje;
- przegląd dokumentacji przygotowanej przez organizację na wniosek audytorów czy zgromadzonej dzięki odpowiedziom z ankiet wysłanych do pracowników.

Odpowiednie podejście do prowadzenia audytu wymaga pełnej współpracy osób audytowanych i odpowiedniego upoważnienia wydanego audytorom przez kierownictwo. Tylko wtedy audyt może być wartościowy dla organizacji. Warto w tym miejscu zaznaczyć, że audyt technologiczny jest skupiony wokół domen związanych z infrastrukturą IT i ma dostarczyć informacje na temat obecnego stanu poziomu technologicznego infrastruktury wykorzystywanej do świadczenia usług informatycznych. Ma być pomocny dla zarządzających i jego wyniki nie powinny być stosowane jako metoda rozliczania pracowników z wykonywanej pracy.

Audyt jest systematyczny, niezależny i ma udokumentowany proces uzyskiwania dowodu z audytu (udowodnienia istnienia obserwacji). Podaje

obiektywną ocenę określającą stopnień pełnienia jego kryteriów [22]. Jest metodą oceny organizacji IT pod kątem:

- potencjału technologicznego;
- stosowanych procedur i metod zarządczych;
- nowoczesności stosowanej technologii;
- skalowalności stosowanej technologii;
- wydajności stosowanej technologii;
- adekwatności zastosowanej technologii do wymagań organizacji.

Audyt skupia się nie tylko na weryfikacji spełnienia wymagań stawianych przez przepisy i normy systemowi zarządzania, ale także ocenia stopień dojrzałości oraz poziom spełnienia potrzeb i oczekiwań klientów (użytkowników technologii informatycznej).

Należy pamiętać, że badanie środowiska technologicznego jest ściśle związane z bezpieczeństwem informacji, w tym danych przetwarzanych elektronicznie oraz w formie tradycyjnej (papierowej). Pomocnym jest więc rzetelne wykorzystanie wyników analizy ryzyk, w których audytor wskazuje obszary mogące prowadzić do ujawnienia informacji lub utraty reputacji, skupiając się nie tylko na aspektach fizycznej ochrony, ale również na ochronie organizacyjnej, w tym na kwestiach zapewnienia poufności, integralności, dostępności danych oraz zapewnienia ciągłości działania (procedury BCP/DRP). Wpływ na bezpieczeństwo może też mieć projekt architektury szczegółowej rozwiązania technicznego oraz produkty (rezultaty prac), dostarczane przez dostawców i twórców oprogramowania (kod źródłowy, dokumentacja, konfiguracja sprzętu i oprogramowania). Audytor zawsze będzie w stanie pomóc zweryfikować, czy prace zostały odpowiednio przeprowadzone z zachowaniem standardów i wytycznych stosowanych dla tego typu przedsięwzięć.

Obserwując problemy bezpieczeństwa w organizacjach administracji publicznej można zauważyć, że często wskazuje się konieczność zgodności działania dostawców z normą ISO 2700. Ochrona danych osobowych oraz ochrona informacji związanych z realizacją umów na świadczenie usług informatycznych winny być priorytetem dla każdej instytucji, w której zaufa-

nie to podstawa budowy odpowiednich relacji z klientem/obywatelem. Niestety, obserwacje rzeczywistych przypadków wskazują, że o ile dostawcy potrafią wdrożyć normę ISO 27001 u siebie, to organy administracji bazują na obecności certyfikatu i nie przeprowadzają analizy ryzyk dostawców czy przeglądów ich sposobów działania. Tym samym organy administracji nie mogą właściwie zweryfikować istnienia dobrych praktyk związanych z bezpieczeństwem informacji w aspekcie konkretnej usługi czy relacji.

Dobrą praktyką w tym zakresie jest wykorzystanie audytora technicznego, który w ramach badania bezpieczeństwa informacji u dostawcy zweryfikuje:

- regulacje wewnętrzne i procesy dostawcy w zakresie relacji z organem administracji,
- realne działania pracowników dostawcy związane z zapewnieniem bezpieczeństwa informacji,
- znajomość wymogów Ustawy o Ochronie Danych Osobowych,
- dostosowanie użytkowanych systemów oraz aplikacji do wymogów ustaw, rozporządzeń czy dobrych praktyk zarządczych,
- bezpieczeństwo kanałów łączności między klientem, a firmami outsourcingującymi usługi IT,
- zgodność z wybranymi elementami normy ISO 270001,

a także dokona przeglądu serwerów i platform, na których świadczone są usługi (parametry sprzętowe, parametry programowe, konfiguracja, administracja zasobami, bezpieczeństwo danych i stosowanych zasad archiwizacji).

Międzynarodowa norma ISO 27001 [23] określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji w danej organizacji. Wdrożenie ISO 27001 u dostawcy nie zwalnia z odpowiedzialności jednostek administracji publicznej z analizowania ryzyk, weryfikacji, zapobiegania i monitorowania zdarzeń w ramach systemu bezpieczeństwa informacji działającego w danej jednostce. Zarządzania ryzykami jednostka administracji publicznej nie może oddelegować do dostawcy.

Kultura pracy

Kultura pracy z systemami informatycznymi bezpośrednio przekłada się na poziom bezpieczeństwa. Badanie „Security Trends. Bezpieczeństwo w cyfrowej erze" [24] przeprowadzone przez Microsoft oraz EY w roku 2015 pokazuje jasno, że najsłabsze ogniwa organizacji to:

- użytkownicy końcowi, którzy nie przestrzegają zasad bezpieczeństwa,
- niewystarczające zaangażowanie zarządów w kwestie bezpieczeństwa,
- brak świadomości zagrożeń ze strony działów biznesowych,
- brak spójnej strategii działań w obszarze bezpieczeństwa.

Generalnie praktyka audytorska w jednostkach administracji publicznej i w firmach potwierdza te spostrzeżenia. W trakcie przeprowadzanych przeglądów i audytów stwierdza się między innymi brak działania pracowników zgodnie z politykami i regulacjami wewnętrznymi. Dzieje się tak często z powodu braku nadzoru, ale również w wyniku nieznajomości przez pracownika obowiązującej regulacji. Istnieje wtedy znaczne ryzyko niedopełnienia obowiązku ochrony informacji, a w konsekwencji utrata informacji. Ucierpi na tym reputacja organizacji. Sytuacja też może rodzić problemy prawne i konieczność dodatkowego wydatkowania środków publicznych na naprawę i usunięcie skutków ujawnienia informacji. Możliwe jest również ukaranie przez Inspektora GIODO.

Do powyższej listy można dodać również inne, często występujące nieprawidłowości związane z bezpieczeństwem informacji. Wskazywaną nieprawidłowością jest możliwość nieuprawnionego dostępu do pomieszczeń i systemów, w których znajdują się informacje wrażliwe, objęte tajemnicą przedsiębiorstwa lub tajemnicą służbową. Dzieje się tak zazwyczaj z powodu niefrasobliwości w nadawaniu samych uprawnień, ale także – co jest częstsze – z uwagi na fakt, że jeśli nawet organizacje dokładają należytych starań przy nadawaniu uprawnień, to zapominają zabierać uprawnienia wtedy, gdy są one już niepotrzebne pracownikowi. Jest to element kultury organizacji, którego nie można poprawić przez proste wdrożenie następnej

procedury. W praktyce audytorskiej zdarzają się przypadki, że pozostawione uprawnienia dawały możliwość wykonania działań w systemach i danych zdalnie już po ustaniu stosunku pracy, np. przez byłego administratora.

Inną częstą obserwacją powiązaną z podejściem kulturowym do bezpieczeństwa, jest nieodpowiednie wyznaczanie miejsc na serwerownie i miejsca przetwarzania danych wrażliwych. Umiejscowienie serwerowni przy głównym wejściu do budynku, korytarzu ogólnodostępnym dla petentów czy w piwnicy nie jest czymś zaskakującym. Zabezpieczenia fizyczne są wtedy minimalne i istnieje możliwość wtargnięcia do serwerowni osoby postronnej i dokonania sabotażu. Często też stwierdzano braki w monitoringu pomieszczeń serwerowych z zewnątrz. Jednocześnie zdarzały się przypadki, że wszelkie kable zasilające i sieciowe były dostępne na korytarzu, co dawało możliwość uszkodzenia infrastruktury lub nieautoryzowanego wpięcia się w sieć.

Niedocenianym przez zarządzających jest fakt nadużywania uprawnień na komputerach przenośnych. Jeśli kultura organizacji wymaga pełnej dyspozycyjności, a co za tym idzie elastyczności, pracownicy otrzymują uprawnienia administracyjne, aby sobie „jakoś" poradzić w sytuacji kryzysowej lub odciążyć administratorów od rutynowych czynności, np. instalacji oprogramowania czy sterownika drukarki. Dane na laptopach są jednak chronione tylko wtedy, gdy komputer posiada odpowiednią konfigurację i są zabezpieczone oprogramowaniem antywirusowym czy szyfrującym.

Niestety, posiadanie przez użytkowników „nadmiarowych" uprawnień prowadzi często do używania zbyt wielu nośników danych (często prywatnych), instalowania szkodliwego oprogramowania czy zdejmowanie kontroli dostępu do komputera. „Nadmiarowe" rozumiane są tutaj nie jako uprawnienia nadane i zatwierdzone przez przełożonego pracownika (administrator nadał uprawnienia, jakie powinien nadać), ale nadmiarowe w stosunku do roli pracownika w organizacji i wymaganych dla niego dostępów (pracownik ma zbyt szerokie uprawnienia z punktu widzenia bezpieczeństwa, ale oczywiście „legalne"). Konsekwencją takiej sytuacji może być nie tylko zawirusowanie albo stworzenie dodatkowych połączeń mostowych

umożliwiających przejęcie kontroli nad komputerem, ale również realny transfer danych poza organizację (dodatkowe zmiany konfiguracyjne i nieautoryzowane oprogramowanie mogą powodować niezabezpieczoną transmisję danych chronionych).

Parę lat temu zdarzył się przypadek używania komputera służbowego urzędnika do wymiany plików w sieci. Traf chciał, że doinstalowane oprogramowanie wymagało (przed ściągnięciem jakiegoś pliku filmowego czy muzycznego) podania własnych zasobów nie mniejszych niż ściągany plik. W przypadku pliku z filmem należało więc najpierw wystawić do sieci co najmniej 1 GB plików. Urzędnik zastosował najprostszą metodę i udostępnił całość dysku, w tym ważne pliki urzędowe. Wyciek danych był nieunikniony.

Łatwość wymiany informacji wpływa również na poziom bezpieczeństwa. W wielu organizacjach stosowane zabezpieczenia portów USB blokują możliwość zapisywania na nośnikach przenośnych (ang. *pendrive*). W ten sposób organizacja unika sytuacji, kiedy pracownik skopiuje ważne dane na nośnik nieszyfrowany USB i zgubi ten nośnik w środkach komunikacji publicznej.

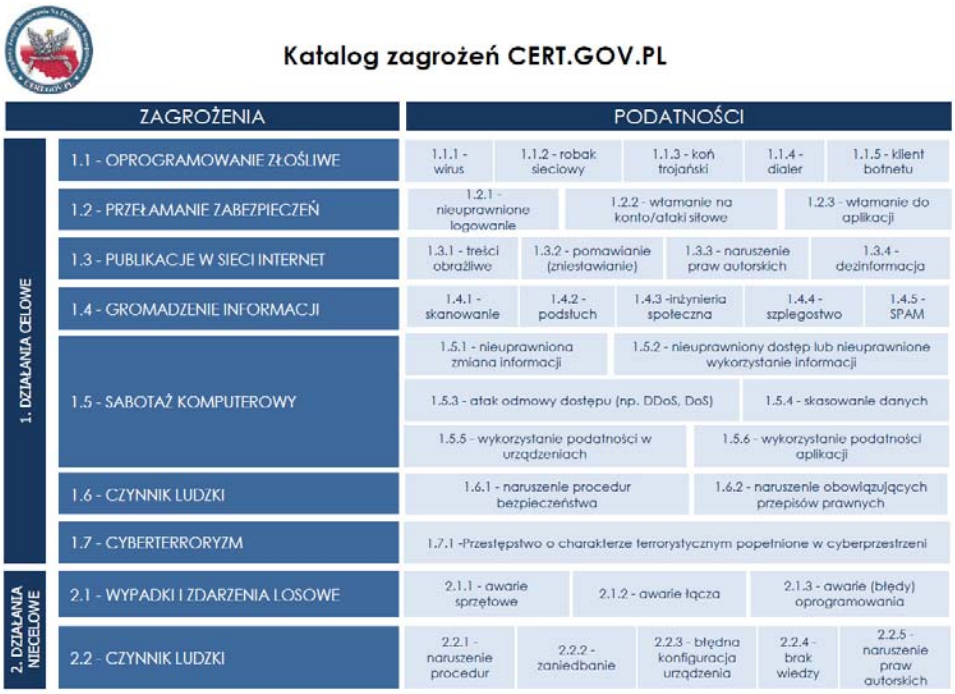
Oczywiście stosowanie zabezpieczeń stwarza pracownikom dodatkowe problemy i wymagania. Potwierdza to wynik badania wspomnianego raportu *Security Trends. Bezpieczeństwo w cyfrowej erze* [24], zgodnie z którym 28% osób odpowiedzialnych za bezpieczeństwo uważa, iż są postrzegani jako spowalniający rozwój i działanie organizacji.

Rola CERT w wymianie informacji o trendach w bezpieczeństwie informacji

Należy pamiętać, że istnieją też zespoły zajmujące się śledzeniem podatności i monitorujące sieć i środowisko pracy aplikacji informatycznych, takie jak na przykład CERT (ang. *Computer Emergency Response Team*). Są to struktury tworzone w ramach firm (komercyjne) czy instytucji publicznych, których celem jest całodobowe nadzorowanie ruchu internetowego (sieciowego) i podejmowanie natychmiastowych akcji w razie pojawienia się zagrożenia.

Zespoły CERT często publikują swoje materiały edukacyjno-szkoleniowe albo prowadzą stronę internetową lub blogi.

Przykładowo, w administracji publicznej Rzeczypospolitej Polskiej istnieje Rządowy Zespół Reagowania na Incydenty Komputerowe w obszarze administracji rządowej i obszarze cywilnym, CERT.GOV.PL, który zapewnia i rozwija zdolności jednostek organizacyjnych administracji publicznej do ochrony przed cyberzagrożeniami. Używa on w swojej pracy szczegółowej klasyfikacji podatności i zagrożeń, która może być pomocna do skutecznej analizy incydentów. Katalog zagrożeń przedstawiono na rysunku 1. 1.



Rys. 1.1. Katalog zagrożeń wg CERT.GOV.PL [25]

Warto dodać, że ponad połowa osób odpowiedzialnych za bezpieczeństwo informacji opowiada się za zintensyfikowaniem regularnej wymiany informacji o zagrożeniach i sposobach prewencji pomiędzy firmami działającymi w tej samej branży lub zbliżonej [24]. Współpraca z organizacjami

zajmującymi się cyberbezpieczeństwem i monitorującymi sieć jest ważna i cenna, ponieważ daje po wykryciu ataku możliwość podjęcia skutecznych kroków prawnych i wyjaśniających.

Trendy i minimalizacja ryzyk

Praktyka audytorska wskazuje, że istnieje szeroki wachlarz działań, które mają utrudnić zadanie przestępcom komputerowym, włamywaczom, a także ustrzec organizacje przed wyciekiem danych. Ochrona przed wyciekami danych jest priorytetem dla organizacji publicznych w obliczu globalizacji, wszechobecności Internetu i zagrożeń związanych z terroryzmem i wojną w cyberprzestrzeni. Zwiększanie zaangażowania i wydatków na bezpieczeństwo jest nieuniknione i wydaje się, że powinno się skupić przede wszystkim na następujących obszarach:

- monitorowanie,
- zapewnienie środków technicznych,
- zarządzanie organizacją w oparciu o ryzyka.

Szczególnie ważny jest ostatni punkt. Prowadzenie rzetelnego rejestru ryzyk technicznych, stosowanego do podejmowania decyzji zarządczych, jest kluczowe dla zachowania dobrych praktyk zarządczych i nauczenia organizacji odpowiedniej kultury pracy. Warto podkreślić, że wymagania formalne i prawne dla organizacji administracji publicznej zobowiązują kierownictwo podmiotów publicznych do realizacji zadań w zakresie zarządzania bezpieczeństwem informacji, zatem nie można analizy ryzyk scedować na dostawcę czy konsultanta.

Świat się zmienia i zmienia się oblicze przestępczości komputerowej. Obecnie cyberprzestępcy działają głównie z terenów Chin. Z tego kraju pochodzi 37% ataków DDOS i aż 51% ataków na aplikacje internetowe [26]. Częściowo pokrzepiający może być fakt, że w związku z sytuacją polityczną na świecie większość ataków celuje w Stany Zjednoczone i na razie Polska nie jest popularnym celem. Nie zmienia to faktu, że skuteczne włamania zdarzały się również w naszym kraju. Atakujący stale zwiększają swoją agresywność i wyrafinowanie, a za atakami stoją coraz większe pieniądze

i zasoby techniczne, co powoduje, że kwestia bezpieczeństwa staje się priorytetem dla administracji publicznej i całego państwa.

Sposób zarządzania bezpieczeństwem informacji jest elementem kultury pracy. Ważne są praktyczne umiejętności rozpoznawania zagrożeń oraz podejmowanie właściwych decyzji i działań przez każdego pracownika. Środki techniczne są nieodzowne, ale przestępcy i atakujący rozwijają również metody wykorzystujące podatności pracowników (użytkowników technologii), np. złe przyzwyczajenia, brak ostrożności czy lekceważenie obowiązków i procedur. Warto zatem monitorować nie tylko to, co się dzieje w sieci i na komputerach, ale również to, jak zachowują się pracownicy i urzędnicy. Skupienie wysiłków wokół wskazanych trzech filarów (tj. monitorowania, zapewnienia środków technicznych i zarządzania organizacją w oparciu o ryzyka) będzie wyrazem dbałości o obywateli (użytkowników systemów administracji publicznej) w zakresie zapewnienia bezpieczeństwa informacji i danych przetwarzanych przez urzędy i instytucje państwowe.

Literatura

[1] Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych z póź. zm., Dz.U. 2015. poz. 2135 z późn. zm.

[2] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2001 nr 112 poz. 1198

[3] Ustawa z 18 września 2001 r. o podpisie elektronicznym, Dz.U. 2001 nr 130 poz. 1450

[4] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002 nr 144 poz. 1204

[5] Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

[6] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. z 2010 r. nr 182, poz. 1228

[7] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz

minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 16 maja 2012 r., poz. 526

[8] Rekomendacja D Komisji Nadzoru Finansowego, Komisja Nadzoru Finasowego, Warszawa 2013, https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf

[9] Wytyczne IT Komisji Nadzoru Finansowego, Komisja Nadzoru Finasowego, Warszawa 2014, https://www.knf.gov.pl/Images/ZU_Wytyczne_IT_16_12_2014_tcm75-40004.pdf

[10] Europejska Agenda Cyfrowa, http://oide.sejm.gov.pl/oide/images/files/pigulki/cyfrowa.pdf

[11] Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2008

[12] Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej, Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf

[13] Polityka Ochrony Cyberprzestrzeni RP, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf

[14] Doktryna cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf

[15] Krajowe Ramy Interoperacyjności, Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526

[16] Norma Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PN ISO/IEC 27001:2007

[17] COBIT 4.1 Frame-work, Control Objectives, Management Guidelines, Maturity Models, IT Governance Institute, USA 2007

[18] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych, Dz.U. 2010 nr 177 poz. 1195

[19] Kodeks etyki zawodowej ISACA, https://www.isaca.org/About-ISACA/History/Documents/ISACA-Code-of-Ethics-Polish.pdf

[20] ISACA "Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit", http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf

[21] Norma Technika informatyczna – Zarządzanie usługami, PN-ISO/IEC 20000-1: 2007

[22] Norma Wytyczne dotyczące auditowania systemów zarządzania jakością i/lub zarządzania środowiskowego, PN-EN ISO 19011:2002 IDT

[23] Międzynarodowa norma ISO 27001, Norma System zarządzania bezpieczeństwem informacji, ISO/IEC 27001:2005

[24] Badanie „Security Trends. Bezpieczeństwo w cyfrowej erze" przeprowadzone przez Microsoft oraz EY w roku 2015, za: Marek Zalewski, *Bezpieczeństwo w sieci*, 9 lutego 2016 r., https://news.microsoft.com/pl-pl/2016/02/09/bezpieczenstwo-w-sieci/#sm.000013grgtsa34f4iqmmo6ojahj7c

[25] Katalog zagrożen wg. CERT.GOV.PL, http://www.cert.gov.pl/download/3/168/KatalogzagrozenCERTGOVPL.pdf

[26] Akamai Releases Q2 2015 State of the Internet – Security Report, Cambridge 2015, http://www.stateoftheinternet.com/security-report

Streszczenie

Celem opracowania jest przedstawienie aspektów związanych z wdrożeniem praktyk organizacyjnych i technicznych dotyczących bezpieczeństwa informacji i metod oceny ryzyk i ich mitygacji, w szczególności w działach IT jednostek administracji publicznej oraz organizacjach współpracujących z administracją publiczną.

Słowa kluczowe: *ryzyko IT, audyt bezpieczeństwa informacji, system bezpieczeństwa informacji, cyberprzestępczość, testy penetracyjne,*

Nota o autorze

Tadeusz Kifner – rzeczoznawca Polskiego Towarzystwa Informatycznego. Autor książek i artykułów o tematyce informatycznej. Posiada 20-letnie doświadczenie zawodowe w branży IT, z czego ponad 12 lat na stanowisku menadżerskim. Uczestniczył w wielu projektach międzynarodowych. Jako konsultant IT świadczył usługi związane z zarządzaniem IT, bezpieczeństwem i implementacją strategii IT oraz BCM. Przeprowadzał audyty technologiczne w oparciu o znane standardy i dobre praktyki zarządcze. Przez wiele lat nadzorował i kontrolował proces SOX w dużej korporacji międzynarodowej. Ma doświadczenie w sektorze bankowym, sektorze przemysłu ciężkiego, administracji publicznej, sektorze farmaceutycznym. Prowadził również projekty dla firm działających na rynku B2B oraz B2C. Asystował i wdrażał ład korporacyjny i nadzór w obszarze IT.

Adam Mizerski

Wyzwania audytu w dobie nowych zagrożeń bezpieczeństwa

Analiza

Ocena stanu istniejącego – raporty NIK i PTI

Podstawowym dokumentem (poza Ustawą o Ochronie Danych Osobowych wraz z rozporządzeniami wykonawczymi) opisującym wymagania dotyczące bezpieczeństwa systemów informatycznych w jednostkach administracji publicznej, jest Rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych [1].

Najwyższa Izba Kontroli (NIK) postanowiła sprawdzić, jak jednostki administracji publicznej realizują wymagania zawarte w KRI, czego efektem była kontrola w przeprowadzona w 25 jednostkach, tj. w: Ministerstwie Administracji i Cyfryzacji oraz w 24 wybranych urzędach gmin miejskich i miast na prawach powiatu w województwach: dolnośląskim, małopolskim, mazowieckim, śląskim, wielkopolskim i zachodniopomorskim. Owocem kontroli jest raport NIK *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu* z 23 marca 2015 roku.

Pomimo pozytywnej oceny całości wyników przeprowadzonej kontroli, niepokój wywołują wyniki raportu:

> „**NIK, ze względu na liczne nieprawidłowości, ogólnie negatywnie ocenia działania burmistrzów i prezydentów miast w zakresie zarządzania**

> **bezpieczeństwem informacji w urzędach**, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie (UM w : Głogowie, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Pruszkowie i Świnoujściu). (…)
>
> **Zdaniem NIK, stwierdzone nieprawidłowości mogą skutkować utratą dostępności, integralności i poufności informacji przetwarzanych w systemach informatycznych urzędów wykorzystywanych do elektronicznej komunikacji i świadczenia usług.** (…)
>
> Nieprawidłowości dotyczyły przede wszystkim:
>
> - ✓ braku w kontrolowanych urzędach całościowej Polityki Bezpieczeństwa Informacji (poza bezpieczeństwem danych osobowych), która jest wymagana przepisami § 20 ust. 1 i 3 rozporządzenia KRI;
> - ✓ **nieprzeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI;**
> - ✓ niewłaściwego zarządzania uprawnieniami użytkowników w zakresie dostępu do systemów informatycznych, co było niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI" [2, wytłuszczenia autora].

Czytając raport NIK można stwierdzić, że kontrolowane urzędy skoncentrowały się głównie na ochronie danych osobowych, jednak „nie wprzęgły" ochrony danych osobowych w kompleksowy System Zarządzania Bezpieczeństwem Informacji:

> **„Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach, którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji"** [2, wytłuszczenie autora]

Negatywną ocenę obrazu przedstawionego w raportach NIK pogłębia analiza danych, pozyskanych w ramach grantu badawczego sfinansowanego przez Polskie Towarzystwo Informatyczne (PTI), zrealizowanego pod kierownictwem dr inż. Przemysława Jatkiewicza *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności*

w jednostkach samorządu terytorialnego. Raport z badań [3]. Warto podkreślić, że NIK objął kontrolą 24 urzędy, a badanie PTI (realizowane za pomocą ankiety w formie wniosku o udostępnienie informacji publicznej) objęło 339 urzędy.

Dodatkowo w raporcie NIK z 22 lutego 2016 roku *Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego* można znaleźć informację, iż w zakresie audytów bezpieczeństwa nadal sytuacja w jednostkach administracji publicznej budzi poważne zastrzeżenia:

> **„W 1/3 skontrolowanych urzędów nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z obowiązującymi przepisami. Nieprawidłowość tę tłumaczono najczęściej brakiem wykwalifikowanych pracowników"** [4, wytłuszczenie autora].

Wytyczne Ministerstwa Cyfryzacji

Próbą działań naprawczych związanych z bezpieczeństwem systemów informatycznych jednostek administracji publicznej, ocenionych w raportach NIK i PTI, jest dokument *Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*, opublikowany przez Ministerstwo Cyfryzacji (MC) z 15 grudnia 2015 roku.

Zgodnie z deklaracją zawartą w wytycznych, ich celem:

> „jest zapewnienie wsparcia dla kontroli, w tym wskazanie jednolitych kryteriów merytorycznych realizacji obowiązku określonego w art. 25 ust. 1 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – Dz.U. z 2014 r., poz. 1114 (dalej: ustawa o informatyzacji), dotyczącego przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji" [5].

Z zagadnień zawartych w KRI, Ministerstwo Cyfryzacji skoncentrowało się w swojej propozycji oceny na trzech tematach podlegających badaniu:

1. **Interoperacyjność**

   Ocena negatywna w obszarze nr 1 (interoperacyjność) może zostać przyznana w szczególności, gdy:

- „nie udostępniono elektronicznej skrzynki podawczej i nie zapewniono jej obsługi (art. 16 ust. 1a ustawy o informatyzacji; pkt 1.1 tematyki kontroli);
- nie zarządza się usługami realizowanymi przez systemy teleinformatyczne na deklarowanym poziomie dostępności usług i **w oparciu o udokumentowane procedury** (§ 15 ust. 2 rozporządzenia; pkt 1.3 tematyki kontroli)" [5, wytłuszczenie autora].

W tym punkcie warto przytoczyć wyniki badania PTI, z którego wynika, że „ponad połowa (56%) ankietowanych instytucji nie posiada żadnej procedury z zakresu wdrażania, eksploatacji, testowania i wycofywania aktywów" [3].

- „nie zapewniono, aby interoperacyjność na poziomie semantycznym osiągnięta została przez stosowanie w rejestrach prowadzonych przez podmioty odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań (§ 5 ust. 3 rozporządzenia; pkt 1.4 tematyki" [5].

2. Bezpieczeństwo informacji

Ocena negatywna w obszarze nr 2 (bezpieczeństwo informacji) może zostać przyznana w szczególności, gdy:

- „nie opracowano, nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) (§ 20 ust. 1 rozporządzenia; pkt 2.1.1 tematyki kontroli);
- nie została opracowana i wdrożona Polityka Bezpieczeństwa Informacji (Polityka BI) (§ 20 ust. 1 , ust. 2 pkt 12h rozporządzenia; pkt 2.1.1 tematyki kontroli);
- **nie jest przeprowadzana okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz nie są podejmowane działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy** (§ 20 ust. 2 pkt 3 rozporządzenia; pkt 2.2 tematyki kontroli);
- **nie jest przeprowadzany audyt wewnętrzny w zakresie BI co najmniej raz w roku** (§ 20 ust. 2 pkt 14 rozporządzenia; pkt 2.9 tematyki kontroli);

- nie zarządza się dostępem do systemów teleinformatycznych w sposób zapewniający, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (§ 20 ust. 2 pkt 4 rozporządzenia; pkt 2.4 tematyki kontroli);
- **nie zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem określonych w zarządzeniu zagadnień** (§ 20 ust. 2 pkt 6 rozporządzenia; pkt 2.5 tematyki kontroli);
- **nie zapewniono, aby incydenty naruszenia bezpieczeństwa informacji były bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących** (§ 20 ust. 2 pkt 13 rozporządzenia; pkt 2.8 tematyki kontroli)" [5, wytłuszczenia autora].

W tym miejscu warto przytoczyć wyniki badania PTI, z którego wynika, że „Ponad połowa (53,69%) respondentów zadeklarowała prowadzenie rejestru incydentów, jednakże 134 pozostają puste, gdyż nie zarejestrowano w nim żadnego incydentu [3].

- „nie zabezpieczono informacji w sposób uniemożliwiający nieuprawnionemu ich ujawnienie, modyfikacje, usunięcie lub zniszczenie (§ 20 ust. 2 pkt 9 rozporządzenia; pkt 2.12 tematyki kontroli);
- nie zapewniono, aby w dziennikach systemów zostały odnotowane obligatoryjnie działania użytkowników lub obiektów systemowych (§ 21 rozporządzenia; pkt 2.12 tematyki kontroli)" [5].

3. Dostosowanie dla osób niepełnosprawnych

Ocena negatywna w temacie nr 3 (dostosowanie dla osób niepełnosprawnych) może zostać przyznana w szczególności, gdy:

- „nie zapewniono spełnienia przez system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia (§ 19 rozporządzenia; pkt 3 tematyki kontroli)" [5].

W tym punkcie warto zapoznać się z Bazą Wiedzy dotyczącą WCAG, udostępnioną przez PTI [6].

Analizując treść dokumentu *Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych* Ministerstwa Cyfryzacji dotyczącą bezpieczeństwa, należy zauważyć kluczową rolę w zakresie właściwie przeprowadzonej analizy ryzyka systemów teleinformatycznych podmiotów administracji publicznej, gdyż **współczesne bezpieczeństwo opiera się na zarządzaniu ryzykiem, czyli na adekwatnym doborze zabezpieczeń do zidentyfikowanych i ocenionych ryzyk uwzględniających ich prawdopodobieństwo i skutek:**

> **„(…) pozytywną ocenę BI może uzyskać system posiadający mało zabezpieczeń, jeśli taka ich ilość (i jakość) wynika z rzetelnie przeprowadzonej analizy ryzyka (np.: system jednostanowiskowy przetwarzający dane powszechnie dostępne). Jednocześnie ocenę negatywną może uzyskać system posiadający znaczną liczbę zabezpieczeń, w przypadku, gdy rodzaj zabezpieczeń (w tym ich ilość i jakość) został zastosowany przypadkowo, bez potwierdzenia poprzez rzetelnie wykonaną analizę ryzyka i powstały w jej wyniku plan postępowania z ryzykiem. W takiej sytuacji jednostka nie zarządza właściwie ryzykiem bezpieczeństwa BI, gdyż system jednostki dla pewnych ryzyk może posiadać nadmierne, niczym nieuzasadnione zabezpieczenia, natomiast dla innych całkowity ich brak”** [5, wytłuszczenie autora].

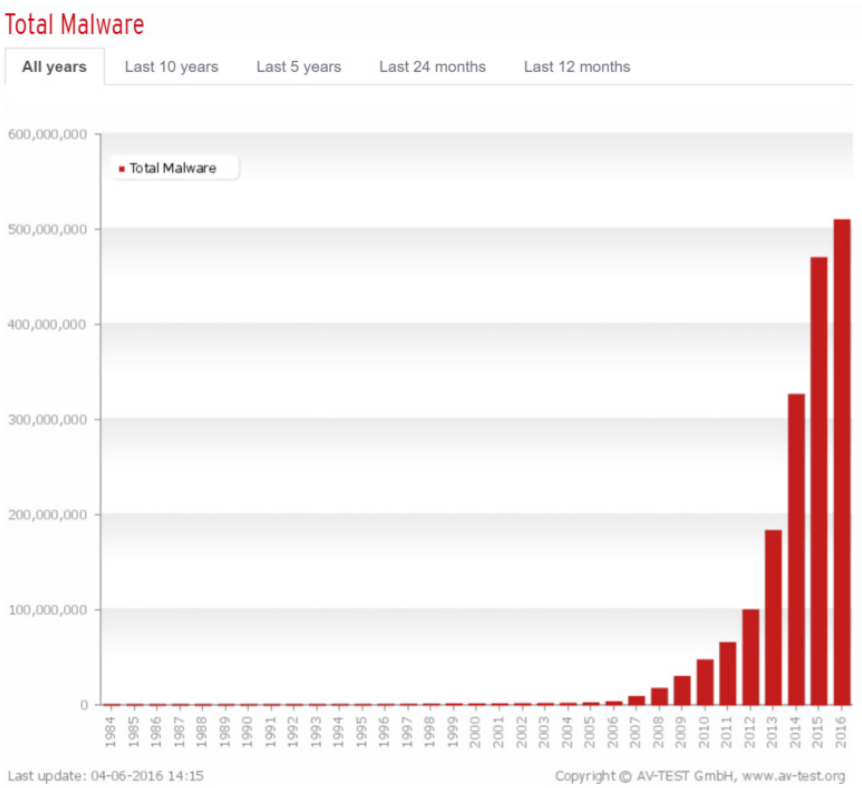
Wyzwania

„Nie najlepsza” ocena bezpieczeństwa przedstawiona w raportach NIK i PTI zderza się z dynamicznie zmieniającym się otoczeniem współczesnych zagrożeń w zakresie bezpieczeństwa systemów informatycznych.

Ewolucja zagrożeń

Jednym z kluczowych zagrożeń, z jakim zmagają się od lat informatycy, jest szkodliwe oprogramowanie (tzw. malware, czyli wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do

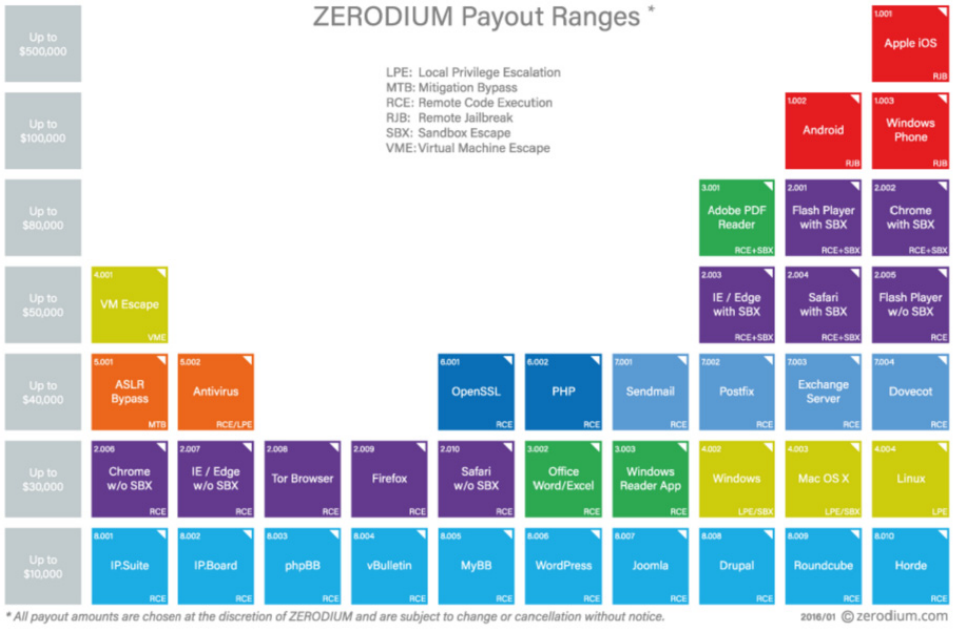
użytkownika komputera – wirusy, trojany, rootkity, C&C: *command and control* czy zyskujące ostatnio na popularności szyfrujące dane i żądające od użytkowników okupu ransomware). Zgodnie z raportem opracowanym przez AV-Test od 8 lat mamy do czynienia z corocznym 100% wzrostem ilości szkodliwego oprogramowania, co obrazuje poniższy wykres.



Rys. 2. 1. Coroczny przyrost złośliwego oprogramowania [7]

Analiza opracowanego przez AV-Test Institute wykresu wskazuje, że zgodnie z negatywnym trendem już w pierwszym kwartale 2016 roku zidentyfikowano więcej szkodliwego oprogramowania niż w całym roku 2015. Ilość powstającego szkodliwego oprogramowania, jak również metody maskowania szkodliwego charakteru malware powodują, że wśród specjalistów zajmujących się bezpieczeństwem od kilku już lat można słyszeć opinię o nieskuteczności mechanizmów zabezpieczających, jakim są klasyczne

instalowane na komputerach systemy antywirusowe. Powstają wprawdzie próby rozwiązania tego problemu, takie jak np. multiplatformowy system VirusTotal [8], bazujący na 40 silnikach antywirusowych, czy wielofunkcyjne zapory sieciowe UTM (Unified Threat Management) nowej generacji, które stosując środowiska wirtualizacyjne typu „sandbox" dokonują analizy przesyłanych do organizacji plików, jednakże powyższe rozwiązania nie gwarantują pełnej ochrony organizacji przed skutkami działania nieznanego ich producentom szkodliwego oprogramowania.



Rys. 2. 2. ZERODIUM Payout Ranges [10]

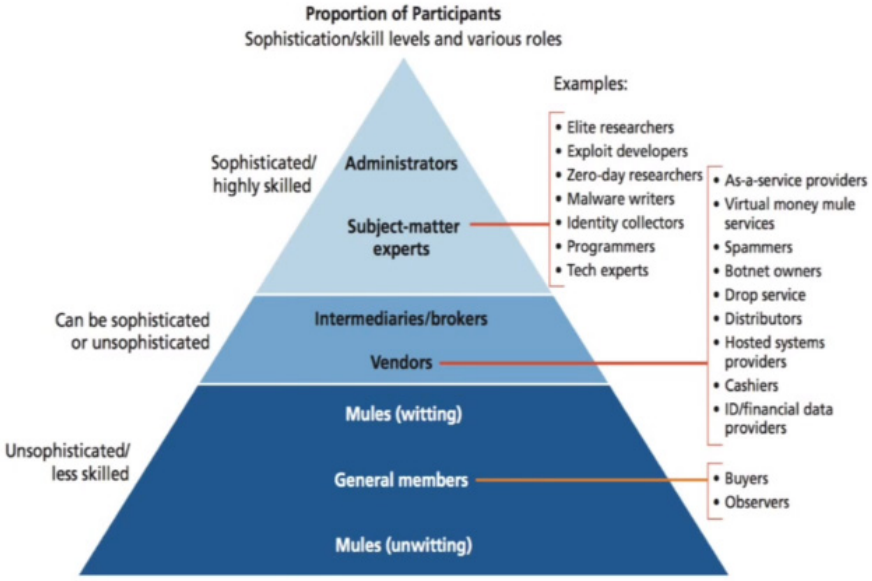
Kolejnym wyzywaniem, przed jakim stają odpowiedzialni za bezpieczeństwo urzędów informatycy, jest kwestia złożoności współczesnego oprogramowania oraz tego konsekwencji w postaci błędów w coraz bardziej rozbudowanym oprogramowaniu. Znalezione i nieusunięte błędy w oprogramowaniu wykorzystywane są do opracowania ataków klasy „Zero-day exploit". Skuteczność ataków tego typu spowodowała powstanie rynku usług poszukiwań

podatności, którego najbardziej znanym przedstawicielem jest firma Zerodium [9], skupująca informację dotyczącą podatności i oferująca spore wynagrodzenie, co przedstawia rysunek 2. 2.

Usługi oferowane przez firmę Zerodium to oficjalna, w miarę „jasna strona" rynku usług związanego z wyszukiwaniem i wykorzystywaniem podatności w oprogramowaniu. Ma ona jednak swoją „ciemną stronę" – rynek usług cyberprzestępczych działających w modelu CaaS (*Crime as a Service*). Oferty CaaS, czyli cyberprzestępstwa jako usługi oferowanej na zlecenie, dostępne są w tzw. „sieci DarkNet", zasobów sieci Internet niedostępnych dla przeciętego użytkownika, niemającego styku np. z przeglądarkami anonimizującymi sieci TOR [11].

Na skale i wagę zjawiska CaaS zwrócił uwagę Europol, który już w roku 2014 w raporcie *Internet Organised Crime Threat Assessment* [12] poświęcił problematyce CaaS cały rozdział.

Współcześni cyberprzestępcy to już nie pojedynczy hakerzy szukający sławy, gdyż według analityków tego zjawiska, 80% hakerów tworzy grupy przestępcze, zorganizowane niemalże w „korporacyjne" w struktury, których przykład pokazano na rysunku 2. 3.



Rys. 2. 3. Struktura zorganizowanej grupy cyberprzestępczej [13]

Profesjonalizacja cyberprzestępstwa ma również wymiar dotyczący prowadzonej przez niech analizy biznesowej, czego efektem jest zmiana modelu działań poszerzona o ataki skierowane na użytkowników, skutkująca nasilającym się zjawiskiem phishin'gu (podszywania się pod inną osobę lub instytucję, w celu wyłudzenia np. danych logowania). Plaga phishin'gu, w większości odfiltrowywana przez działy bezpieczeństwa dużych korporacji, dotyka przede wszystkim użytkowników końcowych podmiotów administracji publicznej, małe i średnie firmy, czy wreszcie wszystkich użytkowników sieci Internet. Wiadomości phishingowe nie przypominają już tych z przed kilku lat, będących maszynowo tłumaczonymi e-mailami, które podejrzane są na pierwszy rzut oka, lecz są coraz bardzie sprofilowane do użytkowników polskiego internetu, jak również wykorzystują elementy psychomanipulacji (zaciekawienie, przestraszenie).

Bardzo dobrym przykładem jest przytoczona poniżej autentyczna korespondencja, z nadawcą podszywającym się pod kancelarię komorniczą, której celem jest zastraszenie użytkownika tak, aby pobrał na swój komputer zainfekowany plik.

> Witam Panstwa.
> Nadal nie otrzymalismy platnosci za fakture FV 11/06/2015. Mogla do Panstwa nie dotrzec dlatego teraz wrzucilem ja na hosting dokumentow tutaj http://downloaded.pl/pobierz/fv-11062015 **(NIE KLIKAĆ - przyp. A.M)** Prosze pobrac i uregulowac naleznosc. W przeciwnym wypadku sprawe skierujemy do windykacji.
> Dokument zabezpieczony jest haslem przypisanym do Panstwa numeru telefonu.
> Aby uniknac problemow prosze o pilne zalatwienie sprawy.
> Pozdrawiam
> Tomasz z Lubicz Inkasso

Rys. 2. 4. Phishing prawie doskonały – „na dług" [14]

Powyższe zagrożenia nie wyczerpują oczywiście całego spektrum, jakie należy rozważyć podczas przygotowania analizy ryzyk.

Wyzwania audytu w dobie współczesnych zagrożeń

Współczesne zagrożenia w zakresie bezpieczeństwa wymagają zmiany w zakresie audytu, w szczególności w zakresie pracy audytu wewnętrznego będącego trzecią liną obrony organizacji. Szacując ryzyko w obszarze IT, w trakcie regularnych audytów bezpieczeństwa organizacje powinny ocenić m.in. (co oczywiście nie wyczerpuje całego spektrum zagadnień):

- czy w ramach zidentyfikowanych incydentów bezpieczeństwa zostały podjęte działania mające na celu identyfikacje źródeł ich powstania oraz czy podjęto działania zabezpieczające organizację w przyszłości przed wystąpieniem podobnych zagrożeń;
- czy określone zostały role i odpowiedzialności w zakresie szacowania ryzyka teleinformatycznego oraz czy role te wynikają z kompetencji uczestników procesu;
- czy proces szacowania ryzyka teleinformatycznego obejmuje wszystkie istotne dla organizacji aktywa;
- w jaki sposób tworzony jest plan postępowania ze zidentyfikowanymi ryzykami oraz w jaki sposób plan ten jest uzgadniany z interesariuszami (np. właścicielami systemów informacyjnych wykorzystujących infrastrukturę teleinformatyczną);
- czy prowadzony jest monitoring środowiska teleinformatycznego, a jeżeli tak, to czy zastosowano wskaźniki umożliwiające ocenę bezpieczeństwa środowiska teleinformatycznego;
- czy procesy obsługi teleinformatycznej z wykorzystaniem usług zewnętrznych (outsourcing) uwzględnione są w procesie szacowania ryzyka, a jeżeli tak, to czy uwzględniają łańcuch poddostawców.

Jako przykład, biorąc pod uwagę ostatnie z zadanych powyżej pytań, ocenie należy poddać m.in. „stare" i „nowe" zjawiska związane z szeroko rozumianym outsourcingiem np.:

- „Shadow IT" – nieautoryzowane przez dział IT organizacji użycie zewnętrznych usług zarówno na poziomie użytkownika (np. Google Docs, Dropbox, etc.), jak również na poziomie jednostek organizacyj-

nych (problem „Shadow IT" to głównie bolączka sektora komercyjnego, ale w trakcie dyskusji na ostatniej konferencji „SEcurity MAnagement Audit FORum 2016" przedstawiono przykład jednego z ministerstw, które również korzystało z nienadzorowanych usług IT);
- ryzyk związanych z zastosowaniem rozwiązań chmur publicznych i hybrydowych modeli Cloud Computing;
- ryzyk outsourcingu usług IT (np. prawnych dotyczących przetwarzania danych osobowych), jak również analizy łańcucha podwykonawców (np. zewnętrzna usługa utrzymania strony internetowej urzędu wykorzystuje podwykonawcę centrum przetwarzania danych, w których alokowane są serwery firmy hostingowej, z kolei firma utrzymująca centrum przetwarzania danych najczęściej korzysta z podwykonawców obsługujących np. systemy odpowiedzialne za klimatyzację techniczną) oraz konieczności dokonania audytu podwykonawców.

Bardzo dobrym przykładem badania zagrożeń związanych z outsourcingiem może być analiza powszechnego wykorzystywania usług hostingowych oraz utrzymania u dostawcy zewnętrznego serwerów pocztowych. Usługi tego typu są ogólnie dostępne i tanie, dlatego też niewiele instytucji decyduje się na utrzymanie serwerów pocztowych w ramach własnej infrastruktury. Analiza publicznie dostępnych w sieci internet rekordów MX serwerów dla drobnej próby instytucji z domeny *.gov.pl przynosi interesujące wyniki, zobrazowane w tabeli 2. 1.

Tabela 2. 1. Analiza rekordów MX

IP serwera pocztowego	REV serwera pocztowego	Outsourcer
91.217.242.17	radio2.wizja.net	WizjaNet sp. z o.o.
77.55.38.239	abm239.rev.netart.pl	nazwa.pl sp. z.o.o
93.157.100.76	s48-mx.ogicom.net	Ogicom "Spider" Sp. z o.o. S.K.A.
91.217.242.17	radio2.wizja.net	WizjaNet sp. z o.o.
91.217.242.17	radio2.wizja.net	WizjaNet sp. z o.o.
93.157.99.126	mail29-mx.ogicom.net	Ogicom "Spider" Sp. z o.o. S.K.A.
85.128.222.209	ann209.rev.netart.pl	nazwa.pl sp. z.o.o

IP serwera pocztowego	REV serwera pocztowego	Outsourcer
85.128.155.237	aky237.rev.netart.pl	nazwa.pl sp. z.o.o
93.157.100.76	s48-mx.ogicom.net	Ogicom "Spider" Sp. z o.o. S.K.A.
79.96.156.226	cloudserver090650.home.net.pl	home.pl S.A.
85.128.245.90	aok90.rev.netart.pl	nazwa.pl sp. z.o.o
91.217.242.17	radio2.wizja.net	WizjaNet sp. z o.o.
89.25.214.162	host8925214162.*.3s.pl	3S S.A.
89.161.135.46	cloudserver022144.home.net.pl	home.pl S.A.
91.211.221.206	gabriel-221-206.trustnet.pl	Trustnet Babicz Agnieszka
91.211.221.207	gabriel-221-207.trustnet.pl	Trustnet Babicz Agnieszka
194.110.77.143	koral.iplus.com.p	INTERNET PLUS s.c.
89.146.221.150	mail4.lh.pl	LH.PL SP. Z O.O.

Wśród przedstawionych powyżej firm świadczących usługi dla podmiotów z domeny *.gov.pl można znaleźć dużych masowych dostawców usług, jak i mniejsze firmy.

Pierwsze pytanie, jakie warto tu zadać, dotyczy tego, czy – zakładając, że w ramach usługi poczty elektronicznej przetwarzane są dane osobowe (nawet w postaci niezamówionych CV potencjalnych kandydatów do pracy) – z powyższymi firmami podpisano umowę o powierzeniu przetwarzania danych osobowych. Jeżeli tak, to jak w warunkach administracji publicznej zapewnić możliwość audytu u jednej z powyższych firm, która zachwalając bezpieczeństwo swoich usług reklamuje na swojej stronie: „Firma dysponuje dwoma szafami 42U znajdującymi się w jednym z najnowocześniejszych Data Center w Europie (Niemcy)" [15].

Drugie pytanie – czy zgodnie z przepisami dotyczącymi Biuletynu Informacji Publicznej zapewniono archiwizację BIP zgodnie z wymaganiami zawartymi w przepisach oraz w sposób zapewniający ciągłość działania w przypadku przerwy działania outsourcera (na skutek licznych błędów i zaniechań w zakresie mechanizmów odpowiedzialnych za ciągłość działania), czego głośny ponad dwutygodniowy przypadek jednej z firm był ostatnio

przedmiotem licznych dyskusji w środowisku osób odpowiedzialnych za bezpieczeństwo.

W kolejnym etapie należy przeanalizować mechanizmy zabezpieczające, jakie stosuje outsourcer w zakresie ochrony przed spamowaniem poczty, co jest jedną technik wykorzystywanych przez cyberprzestępców w ramach phishingu.

W tym celu autor zwrócił się do powyższych firm z zapytaniem:

> Zapytanie ofertowe – usługa hostingu i poczty elektronicznej
>
> *Dzień dobry*
>
> *W związku z planami zmiany firmy hostingowej dla jednego z naszych klientów, proszę o informację, jakich mechanizmów zabezpieczających przed niechcianą pocztą używacie Państwo.*

Analiza odpowiedzi pozyskanych od firm mogłaby być tak naprawdę pierwszą fazą zaawansowanego ataku ukierunkowanego (APT), czyli rozpoznaniem, wykonanym bez użycia jakichkolwiek narzędzi hakerskich.

Smaczku temu dodaje fakt, iż wszystkie wymienione powyżej instytucje publiczne, zatrudniające łącznie kilka tysięcy pracowników, powiązane są ze sobą podległością służbową, umożliwiającą wypracowanie wspólnej polityki związanej z usługami poczty elektronicznej.

W ramach mitygacji ryzyk związanych z phishingiem warto też odpowiedzieć sobie na pytanie, czy – ze względu na stopień zagrożenia i bardzo duże prawdopodobieństwo materializacji zagrożenia – naprawdę wszyscy urzędnicy w ramach wykonywania obowiązków służbowych muszą posługiwać się kontem e-mail umożliwiającym wymianę danych w sieci Internet?

Na zakończenie warto polecić lekturę specjalistycznych portali poświęconych bezpieczeństwu, które powinny być źródłem inspiracji dla audytorów odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych.

Przykładowo można tu wskazać informację, którą na pierwszy rzut oka można potraktować jako ciekawostkę:

> „(…) w październiku 2015 r. eksperci odnotowali ogromną liczbę żądań HTTP (do 20 000 żądań na sekundę) pochodzących z kamer telewizji przemysłowej. Badacze zidentyfikowali około 900 kamer na świecie, które tworzyły botnet wykorzystywany do ataków DDoS" [16].

Jednakże lektura artykułu, z którego pochodzi powyższa informacja, powinna spowodować próbę odpowiedzi na pytania:

- Czy nasza organizacja wykorzystuje technologię monitoringu z wykorzystaniem sieci TCP/IP jako medium transmisyjne (co jest standardem współczesnych systemów monitoringu w odróżnieniu od poprzedniej generacji monitoringu analogowego opartego o dedykowane okablowanie koncentryczne)?
- Jeżeli tak, to czy w sieci LAN wydzielono dedykowane podsieci odseparowane od sieci LAN w sposób zapewniający minimalizację ryzyk wynikających z podatności systemów monitoringu?
- Czy istnieją sformalizowane arkusze ruchu sieciowego opisujące prawidłową konfigurację sieci monitoringu?
- Czy był przeprowadzony audyt bezpieczeństwa, gwarantujący, że konfiguracja jest zgodna z założeniami?

Ryzyka

Jak wynika z wytycznych Ministerstwa Cyfryzacji oraz współczesnego trendu zarządzania bezpieczeństwem, podstawą do właściwego zabezpieczenia jest dobrze przeprowadzona analiza ryzyka. Zarządzanie ryzykiem wynika również wymogów wprowadzonej w administracji publicznej Kontroli Zarządczej. Aby właściwie wykonać analizę ryzyka, należy oprzeć się na jednej z ugruntowanych metodyk.

Szacowanie ryzyka w oparciu o normy ISO

W rozporządzeniu dotyczącym KRI znajdziemy odwołanie do normy Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania [17] oraz komplementarnej do niej normy Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji [18], która jest normą dedykowaną do zagadnień zarządzania ryzykiem.

Faktem jest, że rozporządzenie dotyczące KRI odnosi się do nieaktualnej już wersji normy, gdyż rok 2013 przyniósł zasadnicze zmiany w zakresie filozofii zarządzania systemami bezpieczeństwa informacji nakreślonym przez twórców norm z zakresu 2700X (mowa o ISO – Międzynarodowej Organizacji Normalizacyjnej oraz IEC – Międzynarodowej Komisji Elektrotechnicznej). W roku 2013 Międzynarodowa Organizacja Normalizacyjna wydała nową wersję normy ISO/IEC 27001, która uzależniła stworzenie systemu zarządzania bezpieczeństwem informacji (SZBI) od efektów uzyskanych w ramach prac nad analizą ryzyk, wykonanych zgodnie z wytycznymi zawartymi w normie ISO/IEC 27005.

Polski Komitet Normalizacyjny opublikował polskie wersje norm 27001/27005 w roku 2014 [19] i od tego momentu wszystkie jednostki administracji publicznej, które dokumenty polityki bezpieczeństwa wzorowały na modelu SZBI zawartym w poprzedniej wersji normy PN-ISO/IEC 27001:2007 [17] powinny niezwłocznie dostosować do modelu SZBI zgodnego z PN-ISO/IEC 27001:2014-12 [19].

W praktyce oznacza to rozpoczęcie działania od analizy ryzyk, a nie jak poprzednio – od inwentaryzacji zasobów i aktywów. Taka zmiana optyki w odniesieniu do SZBI wynika zapewne z doświadczeń, które wskazują, że współczesne organizacje w obliczu coraz większej liczby zagrożeń nie są w stanie sprostać im wszystkim. Nawet jeżeli organizacje miałyby zasoby, aby przeciwdziałać wszystkim zagrożeniom, to z ekonomicznego punktu widzenia nie warto angażować sił do obrony przed każdym zagrożeniem. Rozsądniejszym wyjściem jest oszacowanie potencjalnych strat, jakie mogą nastąpić i skoncentrowanie się na obronie newralgicznych punktów. Wykorzystując normę PN-ISO/IEC 27005 [18] należy:

- zidentyfikować aktywa organizacji (zgodnie z normą są to procesy i informacje, czyli aktywa podstawowe, a także sprzęt, oprogramowanie, sieć, personel, siedziba i struktura organizacyjna, czyli aktywa wspierające);
- dokonać wartościowania, czyli ustalić skalę oraz kryteria przyporządkowania wszystkim aktywom określonego miejsca na zdefiniowanej skali – zalecane jest przeprowadzenie analizy kosztów poniesionych

w wyniku utraty poufności, integralności i dostępności, co jest następstwem incydentu bezpieczeństwa;
- zidentyfikować zagrożenia, które mogą stanowić potencjalną przyczynę utraty lub niedostępności aktywów (np. informacji, procesów lub systemów), a w konsekwencji doprowadzić do strat dotkliwych dla całej organizacji. Źródłami zagrożeń mogą być zjawiska naturalne (np. burza, powódź) lub ludzkie (przypadkowe – np. błąd użytkownika lub rozmyślne – np. sabotaż);
- przeanalizować zidentyfikowane potencjalne źródła ryzyk organizacji oraz oszacować skutki materializacji (wystąpienia) ryzyka.

Doskonałym uzupełnieniem normy PN-ISO/IEC 27005:2014-01 jest norma Zarządzanie ryzykiem – Zasady i wytyczne [20], zawierająca zasady i ogólne wytyczne dotyczące zarządzania ryzykiem, która również powinna być wykorzystana w procesie analizy ryzyka.

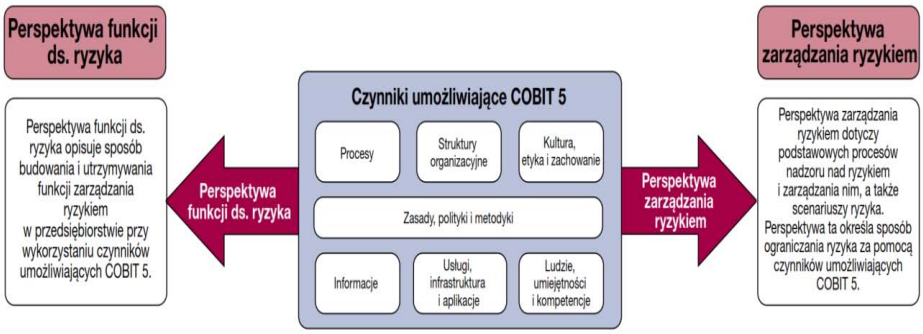
Zarządzanie ryzykiem w oparciu o COBIT 5 for RISK

Interesującą propozycją oceny i zarządzania ryzykiem w obszarze teleinformatycznym jest element kompleksowej metodyki zarządzania ładem informatycznym w organizacji „COBIT 5" (Control Objectives for Information and related Technology [21], dostępny również w języku polskim [22].

Warto podkreślić, że COBIT wykorzystuje model COSO, przygotowany przez Komitet Organizacji Sponsorujących Komisję Treadway'a [23], który jest również jednym z elementów ustawy z 27 sierpnia 2009 roku o finansach publicznych [24], nakładającej na jednostki sektora finansów publicznych obowiązek prowadzenia „Kontroli Zarządczej".

Spojrzenie na ryzyka IT z perspektywy „COBIT 5" obrazuje rysunek 2. 5.

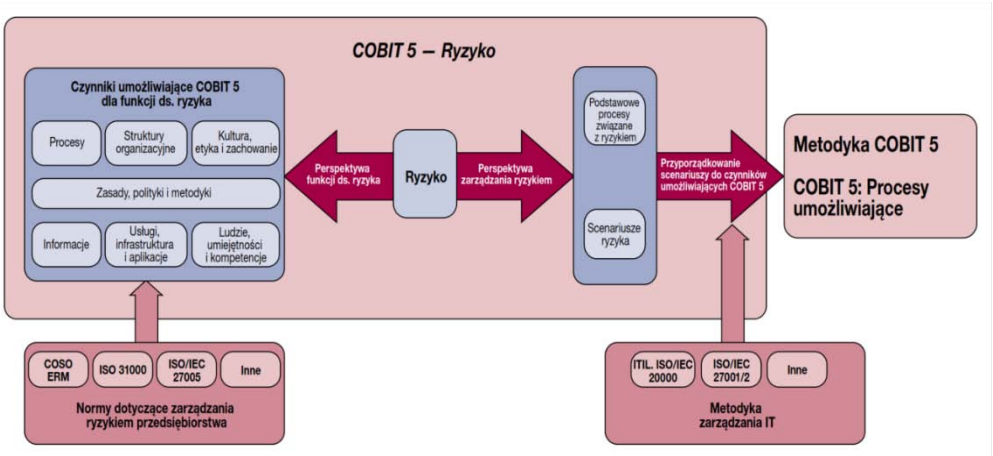
W metodyce „COBIT 5" nadzór nad ryzykiem i zarządzanie nim uznaje się za element ogólnego nadzoru nad technologiami informatycznymi wykorzystywanymi w organizacji i zarządzania nimi tj. sposobu identyfikowania i analizowania ryzyka oraz reagowania na nie.



Rys. 2. 5. Perspektywy ryzyka IT [25: 19]

Zarządzanie ryzykiem zgodne z „COBIT 5" oparte jest o *The Risk IT Framework* [26], który swoją pierwszą odsłonę miał w roku 2009.

Metodyka zarządzania ryzykiem ujęta w ramach „COBIT 5" jest dostosowana do współpracy z normami ISO i innymi metodykami zarządzania IT oraz ryzykami w zakresie obszaru odpowiedzialności IT, co ilustruje rysunek 2. 6.



Rys. 2. 6. Współpraca COBIT 5 z normami ISO i innymi metodykami [25: 21]

Zarządzanie ryzykiem zgodnie z „COBIT 5" obejmuje kompleksowo wszystkie procesy organizacji, co obrazuje poniższe zestawienie w tabeli 2. 2.

Tabela 2. 2. Procesowe zarządzanie ryzykiem zgodnie z „COBIT 5" – przykłady.

Proces	**Opis**
Zapewnienie i utrzymanie ładu w organizacji	Nadzór nad ryzykiem i zarządzanie nim wymaga ustanowienia odpowiedniej metodyki nadzoru w celu wdrożenia struktur, zasad, procesów i praktyk.
Zapewnienie przejrzystości dotyczącej interesariuszy	Zarządzanie ryzykiem w organizacji wymaga przejrzystego pomiaru wydajności i zgodności za pomocą celów i mierników zatwierdzonych przez interesariuszy.
Zarządzanie budżetem i kosztami	Niezbędne jest określenie budżetu związanego z szacowaniem ryzyka.
Zarządzanie zasobami ludzkimi	Zarządzanie ryzykiem wymaga właściwej liczby osób posiadających kompetencje i doświadczenia.
Zarządzanie jakością	Proces zarządzania ryzykiem powinien być oceniany zgodnie z systemem zarządzania jakością w organizacji.
Zarządzanie wiedzą	W procesie zarządzania ryzykiem należy zapewnić wiedzę wymaganą do wspierania pracowników w ich działaniach.
Monitorowanie, ocena i oszacowanie systemu kontroli wewnętrznej	Wewnętrzne mechanizmy kontrolne odgrywają kluczową rolę w monitorowaniu i ograniczaniu ryzyka, tak aby nie stało się ono problemem.
Zapewnienie optymalizacji zasobów	Zarządzanie ryzykiem musi zoptymalizować sposób wykorzystania zasobów IT.
Zarządzanie metodyką zarządzania IT	Zarządzanie ryzykiem musi wspierać metodyki zarządzania IT.
Zarządzanie architekturą korporacyjną IT	Zarządzanie ryzykiem powinno wykorzystywać architekturę korporacyjną IT jako kluczowe źródło informacji wspierających oceny ryzyka dotyczącego użytkowanych technologii informatycznych.
Zarządzanie innowacjami	Zarządzanie ryzykiem powinno zawsze wiązać się z poszukiwaniem nowych metodologii, technologii oraz narzędzi, które mogą wspierać nadzór nad ryzykiem i zarządzanie nim w organizacji.
Zarządzanie umowami o świadczeniu usług	Zarządzanie ryzykiem powinno uwzględniać wewnętrznych i zewnętrznych dostawców usług
Zarządzanie bezpieczeństwem	Zarządzanie ryzykiem powinno dotyczyć bezpieczeństwa, którym należy zarządzać.
Zarządzanie zasobami	Zarządzanie ryzykiem powinno uwzględniać zarządzanie zasobami IT.
Zarządzanie konfiguracją	Zarządzanie ryzykiem musi obejmować zarządzanie konfiguracją IT wraz z działem IT.

Proces	Opis
Zarządzanie eksploatacją	Zarządzanie ryzykiem jest wspierane przez narzędzia oraz aplikacje IT i musi być poddane właściwemu zarządzaniu.
Zarządzanie zgłoszeniami serwisowymi i incydentami	Zarządzanie ryzykiem musi zadbać o działania następcze w odniesieniu do zgłoszeń serwisowych oraz incydentów dotyczących zasobów IT.
Zarządzanie problemami	Zarządzanie ryzykiem musi zadbać o działania następcze w odniesieniu do problemów dotyczących zasobów IT.
Zarządzanie usługami bezpieczeństwa	Zarządzanie ryzykiem musi przestrzegać polityk bezpieczeństwa w odniesieniu do zasobów IT.

Źródło: opracowanie na podstawie [27].

Inne metodyki szacowania ryzyk

Zarówno normy ISO, jaki i *COBIT 5 for Risk* nie wyczerpują katalogu metodyk szacowania ryzyka.

Wśród innych, alternatywnych metod szacowania ryzyka można wymienić m.in.:

- metodę Mehari;
- metodę delficką;
- metody drzewiaste ETA (Analiza Drzew Zdarzeń), FTA (Analiza Drzewa Błędów).

Z badania PTI wynika, że pomimo wymogów zarządzania ryzykiem wynikających z Kontroli Zarządczej, wśród przedstawicieli samorządu istnieje spory potencjał do doskonalenia w zakresie metodyk zarządzania ryzykiem, gdyż respondenci nie umieli ustalić, bądź nie znali nazw użytych metodyk. Wymieniali następujące nazwy, niebędące nazwami metodyk analizy ryzyka:

- „burza mózgów" (Starostwo Powiatowe w W…),
- Prince 2 (Starostwo Powiatowe w S…),
- arytmetyczna (Starostwo Powiatowe w K…),
- CMMI for Services v. 1.3,
- PMI (Urząd Gminy N…),
- indukcyjna (Urząd Miasta i Gminy T…, Urząd Gminy w L…),
- ręczna (Urząd Miejski w Ł..)" [3: 27-28].

Rekomendacje

Biorąc pod uwagę powstawanie coraz bardziej wyrafinowanych zagrożeń, przed którymi muszą stanąć naprzeciw jednostki administracji publicznej, należy:

- w skali makro:
  - dokonać grupowania jednostek administracji publicznej realizujących analogiczne usługi publiczne w celu standaryzacji wykonywanych procesów oraz idącej za tym unifikacji systemów informacyjnych wspomagających przetwarzanie danych;
  - w oparciu o Architekturę Korporacyjną Państwa opracować katalog usług IT wspólnych dla urzędów realizujących analogiczne usługi publiczne;
  - wypracować wspólne standardy dotyczące systemów teleinformatycznych;
  - zgodnie z Założeniami Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej [28] opracować wspólny katalog ryzyk oraz zapewnić proces cyklicznego regularnego przeglądu ryzyk w odniesieniu do zmieniającego się otoczenia zagrożeń;
  - zgodnie z rekomendacjami zawartymi w raporcie CERT *System bezpieczeństwa cyberprzestrzeni RP* [29] powołać zespoły CSIRT (Computer Security Incident Response Team – zespoły ekspertów do spraw bezpieczeństwa komputerowego) w ramach stworzenia centrów usług wspólnych dla jednostek administracji publicznej;
  - zapewnić uregulowania prawne umożliwiające w ramach krajowego CERT powołanie zespołów tzw. „Red Team" odpowiedzialnych za testy bezpieczeństwa infrastruktury jednostek administracji publicznej, które byłyby upoważnione do prowadzenia ofensywnych testów bezpieczeństwa.
- w skali mikro – poszczególnej jednostki administracji publicznej:
  - dokonać analizy ryzyk związanych z przetwarzaniem danych przez systemy teleinformatyczne z wykorzystaniem

jednej z uznanych metodyk i na jej podstawie podjąć działania ograniczające największe zidentyfikowane ryzyka;
- zapewnić regularne zewnętrzne audyty bezpieczeństwa dotyczące systemów teleinformatycznych (warto tu wspomnieć o wspólnej inicjatywie Instytutu Audytorów Wewnętrznych IIA Polska [30], Stowarzyszenia OWASP Polska [31] oraz ISACA Katowice – Stowarzyszenie audytu, bezpieczeństwa i kontroli systemów informacyjnych [32] stworzenia „Białej Księgi" dobrych praktyk dotyczących zamawiania usług szeroko rozumianego audytu: operacyjnego, finansowego, IT i bezpieczeństwa);
- zapewnić szkolenia z zakresu bezpieczeństwa dla wszystkich biorących udział w procesie przetwarzania danych.

Literatura

[1] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526 z późn. zm., http://isap.sejm.gov.pl/Download;jsessionid=9271E8D05793FE55BDC292E691794F74?id=WDU20120000526&type=2

[2] *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu*, Naczelna Izba Kontroli, Warszawa 2015, https://www.nik.gov.pl/kontrole/P/14/004/

[3] Przemysław Jatkiewicz, *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego. Raport z badań*, Polskie Towarzystwo Informatyczne, Warszawa 2016, http://pti.org.pl/content/download/5703/44536/file/BR%20PTI%20tom%203%20druk%20final.pdf

[4] Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego, Naczelna Izba Kontroli, Warszawa 22 lutego 2016 r.
[5] Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, Ministerstwo Cyfryzacji, Warszawa 15 grudnia 2015 r., http://mc.bip.gov.pl/wytyczne/wytyczne-dla-kontroli-dzialania-systemow-teleinformatycznych-uzywanych-do-realizacji-zadan-publicznych.html
[6] Baza wiedzy o WCAG, http://wcag.pti.org.pl/
[7] Malware, portal The AV-TEST Institute, zakładka Statistics, https://www.av-test.org/en/statistics/malware/
[8] serwis VirusTotal, https://www.virustotal.com/
[9] portal firmy Zerodium, https://www.zerodium.com/
[10] portal firmy Zerodium, zakładka Program, ZERODIUM Payout Ranges, https://www.zerodium.com/program.html
[11] portal Tor, https://www.torproject.org/
[12] *Internet Organised Crime Threat Assessment*, Europol, Hague 29 September 2014, https://www.europol.europa.eu/content/organised-crime-groups-exploiting-hidden-internet-online-criminal-service-industry
[13] Jarosław Sordyl, *CaaS (Crime-as-a-Service) – czy każdy może zostać cyberprzestępcą?*, relacja z konferncji CONFidence2015, Kraków 27-29 maja 2015 r., https://www.youtube.com/watch?v=L7EV2YK_w9o
[14] *Phishing prawie doskonały – „na dług"*, portal TSecurity24.info, http://www.itsecurity24.info/?q=node/28
[15] *O firmie*, strona internetowa LH.pl, https://www.lh.pl/o-firmie
[16] *Raport Kaspersky DDoS Intelligence dla IV kwartału 2015 roku*, portal SecureList.pl, zakładka Analizy, http://securelist.pl/analysis/7349,raport_kaspersky_ddos_intelligence_dla_iv_kwartalu_2015_roku.html
[17] Norma Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PN-ISO/IEC 27001
[18] Norma Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, PN-ISO/IEC 27005

[19] Norma Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PN-ISO/IEC 27001:2014-12 – wersja polska
[20] Norma Zarządzanie ryzykiem – Zasady i wytyczne, PN-ISO 31000:2012 – wersja polska
[21] *What is COBIT 5?*, portal ISACA, zakładka COBIT, http://www.isaca.org/cobit/pages/default.aspx
[22] *COBIT 5 Polish*, portal ISACA, ZAKŁADKA COBIT, PODSTRONA COBIT 5 Polish, http://www.isaca.org/COBIT/Pages/COBIT-5-polish.aspx
[23] *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa*, The Committee of Sponsoring Organizations of the Treadway Commission, 2014, http://www.coso.org/documents/coso_erm_executivesummary_polish.pdf
[24] Ustawa z 27 sierpnia 2009 roku o finansach publicznych, Dz.U. z 2009 r. nr 157, poz. 1240
[25] *COBIT 5 Ryzyko*, http://www.isaca.org/COBIT/Pages/COBIT-5-polish.aspx
[26] *The Risk IT Framework*, portal ISACA, zakładka Knowledge Center, podstrona Research, zakładka Research-Deliverables, strona The Risk IT Framework, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx
[27] *COBIT 5 for Risk*, ISACA, Rolling Meadows 2013
[28] *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf
[29] *System bezpieczeństwa cyberprzestrzeni RP. Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji*, NASK/CERT POLSKA, Warszawa 2015, https://mc.gov.pl/files/nask_rekomendacja.pdf
[30] strona internetowa Instytutu Audytorów Wewnętrznych IIA Polska, https://www.iia.org.pl/

[31] strona internetoiwa OWASP Poland, https://www.owasp.org/index.php/Poland
[32] strona internetowa ISACA Katowice – Stowarzyszenie audytu, bezpieczeństwa i kontroli systemów informacyjnych, http://www.isaca.org/chapters8/Katowice/Pages/default.aspx
[33] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 roku w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych, Dz.U. 2010 nr 177 poz. 1195, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20101771195

Materiały pomocnicze

Wykaz certyfikatów uprawniających do przeprowadzania kontroli w rozumieniu art. 25 Ustawy z dnia 17 lutego 2005 r. O Informatyzacji Działalności Podmiotów Realizujących Zadania Publiczne [34]

1) Audytor systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001 lub jej odpowiednika międzynarodowego.
2) Audytor systemu zarządzania usługami informatycznymi według normy PN ISO/IEC 20000 lub jej odpowiednika międzynarodowego.
3) Audytor systemu zarządzania jakością według normy PN ISO/IEC 9001 lub jej odpowiednika międzynarodowego.
4) Certified Information System Auditor (CISA).
5) Certified in the Governance of Enterprise IT (CGEIT).
6) Certified Internal Auditor (CIA).
7) Certified Information Systems Security Professional (CISSP).
8) Europejski Certyfikat Umiejętności Zawodowych Informatyka — EUCIP Professional specjalizacja Audytor Systemów Informacyjnych.
9) Systems Security Certified Practitioner (SSCP).

Metodyki i standardy wspierające audytowanie systemów IT

- COBIT 4.1 (Control Objectives for Information and related Technology) – dostępny bezpłatnie dla wszystkich – wersja przetłumaczona na język polski, http://www.isaca.org/knowledge-center/cobit/documents/cobit-4.1-polish-version.pdf
- COBIT 5 (Control Objectives for Information and related Technology) – dostępny bezpłatnie dla członków ISACA, http://www.isaca.org/COBIT/Pages/COBIT-5-polish.aspx
- GTAG® 4 (Global Technology Audit Management): *Zarządzanie Audytem IT* – opracowanie dostępne bezpłatnie dla audytorów zrzeszonych w Stowarzyszeniu Instytut Audytorów Wewnętrznych IIA Polska, https://www.iia.org.pl/czlonkostwo/ksiegarnia/gtagr-4-zarzadzanie-audytem-it%20%20%20
- GTAG® 17 (Global Technology Audit Management): *Audytowanie ładu informatycznego* – opracowanie dostępne bezpłatnie dla audytorów zrzeszonych w Stowarzyszeniu Instytut Audytorów Wewnętrznych IIA Polska, https://www.iia.org.pl/czlonkostwo/ksiegarnia/gtagr-17-audytowanie-ladu-informatycznego%20
- NIST SP 800-30 Rev. 1 – *Guide for Conducting Risk Assessments*, dostępny bezpłatnie dla wszystkich, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- NIST SP 800-37 Rev. 1 – *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* – dostępny bezpłatnie dla wszystkich, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, dostępny bezpłatnie dla wszystkich, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- NIST SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, dostępny bezpłatnie dla wszystkich http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Streszczenie

Czy w dobie nowych zagrożeń „zapewniający" model audytu skoncentrowany na zgodności jest wystarczający? W artykule poruszono kwestie:

- oceny stanu bezpieczeństwa podmiotów administracji publicznej jaki wynika z raportów Najwyższej Izby Kontroli oraz Polskiego Towarzystwa Informatycznego;
- wytycznych do audytowania systemów informatycznych opublikowanych przez Ministerstwo Cyfryzacji w styczniu 2016;
- nowych wyzwań w zakresie bezpieczeństwa (np. nieskuteczności mechanizmów antywirusowych, zmiany modelu działania cyberprzestępców CaaS (Crime as a Service), nieautoryzowane przez dział IT organizacji użycie zewnętrznych usług „shadow IT", „łańcuchy podwykonawców" outsourcingu IT), na jakie muszą być przygotowani audytorzy;
- analizy ryzyka jako podstawowego „narzędzia" audytora.

Słowa kluczowe: *bezpieczeństwo, cyberbezpieczeństwo, audyt, ryzyko IT*

Nota o autorze

Adam Mizerski – audytor systemów teleinformatycznych w Departamencie Audytu Wewnętrznego jednego z 10 największych banków w Polsce, ekspert ds. bezpieczeństwa oraz metod zintegrowanej analizy ryzyka, jak również zarządzania IT. Wieloletni szef Oddziału Informatycznego, pełniący funkcję Głównego Administratora Bezpieczeństwa Systemów w Sądzie Rejonowym Katowice-Zachód w Katowicach. Rzeczoznawca Izby Rzeczoznawców PTI oraz biegły ds. informatyki przy Sądzie Okręgowym w Katowicach. Członek Zarządu Głównego Polskiego Towarzystwa Informatycznego, wiceprezes Oddziału Górnośląskiego PTI oraz prezes ISACA Katowice Chapter – Stowarzyszenia Audytu, Bezpieczeństwa i Kontroli Systemów Informacyjnych (afiliowanego w ISACA International).

Przemysław Jatkiewicz

Zarządzanie bezpieczeństwem w jednostkach samorządowych

Uzasadnienie tematu

Instytucje samorządowe pełnią istotną rolę w życiu społeczno-gospodarczym społeczeństwa. Przetwarzają najbardziej szeroki zakres informacji dotyczący obywateli. To właśnie z nimi mieszkańcy mają najczęstszy kontakt, który wraz z rozwojem usług e-administracji powoli zaczyna przenosić się w sferę wirtualną. Ponad 2500 instytucji samorządowych począwszy od urzędów na szczeblu województwa po urzędy gminne wraz z wieloma dodatkowo powołanymi przez nie jednostkami pomocniczymi to najbardziej liczna grupa instytucji publicznych.

Wykonywanie zadań przez organizacje, niezależnie od ich formy organizacyjnej czy prawnej, wymaga zazwyczaj przetwarzania zbiorów danych, które związane jest z zaangażowaniem zasobów o wymiernej wartości. Straty, jakie mogą wiązać się z naruszeniem bezpieczeństwa informacji, są trudne do określenia. Wiążą się one nie tylko z utratą płynności funkcjonowania organizacji oraz koniecznością zaangażowania dodatkowych środków w celu usunięcia ich skutków, lecz także utratą własności intelektualnej, odszkodowaniami oraz konsekwencjami prawnymi.

Systemy informacyjne są coraz bardziej narażone na niepożądane ingerencje w miarę wzrostu świadomości o wartości rynkowej informacji, jak i jej oddziaływanie na przewagę konkurencyjną. Szacuje się, iż wartość pojedynczego rekordu zawierającego podstawowe dane osobowe, takie jak imię, nazwisko, telefon lub adres e-mail, wynosi 50-60 gr [1]. Ta niewygórowana kwota pomnożona przez liczbę mieszkańców średniego miasta daje

dziesiątki, a nawet setki tysięcy złotych. Pieniądze takie stanowić mogą nieodpartą pokusę dla przestępców, którymi mogą się także stać nieuczciwi urzędnicy.

Niebagatelny wpływ na stopień bezpieczeństwa ma wielkość oraz złożoność systemów informacyjnych. Od pierwszych prostych systemów ewidencyjno-transakcyjnych lat 50. zeszłego wieku ewoluowały do zintegrowanych systemów informatycznych (ZSI), zajmujących się wszystkimi sferami działalności przedsiębiorstwa. Nie bez wpływu pozostaje również rozwijający się Internet i upowszechnienie usług on-line, jak również dostępna poprzez niego wiedza o słabych ogniwach produktów informatycznych.

Mając na uwadze rosnące znaczenie systemów informacyjnych instytucji publicznych oraz odmienność celów administracji i biznesu, celowym wydaje się przeprowadzenie analizy stanu bezpieczeństwa informacji w jednostkach samorządowych oraz sformułowanie na ich podstawie wniosków oraz potencjalnych zaleceń.

Obowiązujące przepisy

Ochrona zapisów księgowych

Przepisy związane z bezpieczeństwem informacji odnaleźć można w licznych aktach prawnych, między innymi w rozdziale 2 ustawy o rachunkowości [2], dotyczącym prowadzenia ksiąg rachunkowych. Znajduje się w nim przepis mówiący o konieczności posiadania przez jednostkę dokumentacji opisującej zasady (politykę) rachunkowości. Wyszczególnia między innymi dokumentację systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów.

Wspomniana ustawa o rachunkowości poświęca cały 8 rozdział ochronie danych. Podkreślono w nim konieczność zabezpieczenia danych przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem. Zdefiniowano także system ochrony danych, który powinien polegać na:

- stosowaniu odpornych na zagrożenia nośników danych,
- doborze stosownych środków ochrony zewnętrznej,
- systematycznym tworzeniu rezerwowych kopii zbiorów danych,
- zapewnieniu trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych,
- utrzymywaniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości,
- stosowaniu rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem.

Zawarty w omawianym rozdziale art. 75 określa sposób udostępniania księgowych zbiorów danych osobom trzecim. Mogą być one udostępnione jedynie za zgodą kierownika jednostki lub osoby przez niego upoważnionej. Jeśli mają być wyniesione poza siedzibę jednostki, konieczne jest pozostawienie potwierdzonego spisu przejętych dokumentów.

Tajemnica przedsiębiorstwa

Jednostki samorządowe zobligowane są także do ochrony informacji, stanowiących tajemnicę przedsiębiorstwa. W ustawie o zwalczaniu nieuczciwej konkurencji [3] rozumiana jest ona jako nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Za tajemnicę handlową można byłoby więc przyjąć tajemnicę związaną z informacjami posiadającymi wartość gospodarczą. Jednakże dalszy wymóg podjęcia niezbędnych działań przez ich właściciela w celu zachowania ich poufności wydaje się nieścisły [4].

Słuszniejsze byłoby przyjęcie następującej, opracowanej przez autora definicji: „Tajemnica handlowa obejmuje informacje uzyskane w toku prowadzenia działalności gospodarczej, a których ujawnienie może narazić biorące w niej strony na straty lub utratę korzyści".

Najbardziej popularnymi tajemnicami przedsiębiorstwa są:

- prognozy biznesowe,
- plany marketingowe,
- relacje biznesowe,
- technologie,
- algorytmy,
- rozwiązania systemowe i konceptualne [5].

Działalność gmin w świetle ustawy o samorządzie gminnym jest jawna, w związku z tym nie dotyczy ich wiele tajemnic handlowych, jak np. relacje biznesowe czy plany marketingowe. Natomiast szczegóły technologii, algorytmów, rozwiązań systemowych i konceptualnych, których znajomość wynika z ich funkcjonowania, nadal nimi pozostają i winny być odpowiednio zabezpieczone przed niepowołanym dostępem.

Informacja publiczna

Zasada jawności związana jest z pojęciem informacji publicznej, a więc każdej informacji o sprawach publicznych, a w szczególności o:

1) organach władzy publicznej,
2) zasadach funkcjonowania podmiotów, organów władzy publicznej
3) danych publicznych, w tym:
    a) treść i postać dokumentów urzędowych,
    b) stanowiska w sprawach publicznych zajęte przez organy władzy publicznej i przez funkcjonariuszy publicznych,
4) treści innych wystąpień i ocen dokonywanych przez organy władzy publicznej,
5) informacji o stanie państwa, samorządów i ich jednostek organizacyjnych,
6) majątku publicznym [6].

Prawo dostępu do informacji publicznej przysługuje każdemu. Podlega ono ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, jak również ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy.

Udostępnienie informacji publicznej następuje w drodze publikacji w Biuletynie Informacji Publicznej (BIP), wyłożenia czy wywieszenia w miejscach ogólnie dostępnych, zainstalowania w tych miejscach urządzenia umożliwiającego zapoznanie się z tą informacją, jak również udzielenie jej w formie pisemnej lub ustnej. Dotyczy to również udostępniania materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących posiedzenia kolegialnych organów władzy publicznej.

Wydaje się, iż informacje publiczne, ze względu na swój charakter, nie wymagają specjalnej ochrony. Jednakże waga ich treści jest na tyle istotna, że wymagają podjęcia działań mających na celu zapobieżenie manipulacji nimi oraz ograniczeniom dostępności. Wymagania odnośnie koniecznych środków bezpieczeństwa zostały zawarte w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji [7].

Rozporządzenie wymaga między innymi, aby informacje publiczne zawarte w BIP dostępne były dla odwiedzających przez całą dobę bez przerwy, z wyjątkiem sytuacji awaryjnych. W przypadku awarii, brak dostępności dla odwiedzających strony podmiotowe BIP nie może przekraczać 24 godzin. Strony te muszą mieć zaimplementowane rozwiązania chroniące przed celowym spowolnieniem lub uniemożliwieniem dostępu do ich zasobów.

Dane archiwalne

Aktem prawnym definiującym materiały archiwalne oraz sposób postępowania z nimi jest ustawa o narodowym zasobie archiwalnym i archiwach [8]. Materiałami archiwalnymi są wszelkiego rodzaju akta i dokumenty, korespondencja, dokumentacja finansowa, techniczna i statystyczna, mapy i plany, fotografie, filmy i mikrofilmy, nagrania dźwiękowe i wideofonowe oraz inna dokumentacja, bez względu na sposób jej wytwarzania. Mają one znaczenie jako źródło informacji o wartości historycznej o działalności Państwa Polskiego, jego poszczególnych organów i innych państwowych jednostek organizacyjnych a także o działalności jednostek samorządu terytorialnego i innych samorządowych jednostek organizacyjnych.

Ustawa wspomina o dokumentach elektronicznych. Nie precyzuje jednak ich struktury, sposobu postępowania z nimi, jak również wymagań technicznych, odsyłając do aktów prawnych wydanych przez ministra do spraw informatyzacji.

Sposób postępowania z dokumentami w postaci elektronicznej został określony w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 30 października 2006 roku [9]. I tak przechowywanie dokumentów ewidencjonowanych do czasu przekazania ich do archiwum państwowego albo brakowania wymaga opracowania i aktualizowania szczegółowych procedur przechowywania w czasie nie krótszym niż 10 lat, przy uwzględnieniu bieżącego stanu wiedzy. Procedury te powinny obejmować przeprowadzanie corocznych przeglądów próbek dokumentów oraz przenoszenie ich w razie konieczności na inne nośniki danych.

System informatyczny służący do ewidencjonowania wspomnianych dokumentów musi zapewnić ich integralność oraz zabezpieczyć je przed usunięciem i zmianami. Może to być wykonane jedynie na podstawie określonych procedur lub na podstawie odpowiednich przepisów prawa, jak również na skutek działań mających na celu usunięcie zagrożeń dla prawidłowego działania systemu.

Dla każdego dokumentu oraz jego metadanych system prowadzi rejestr uprawnień użytkowników oraz zmian, jakich oni dokonywali. Oprócz oczywistych funkcji, takich jak wyszukiwanie i odczytywanie dokumentów i metadanych, wspomaga proces brakowania i przekazywania do archiwów państwowych. Prawodawca zadbał również o kompatybilność różnych systemów informatycznych, narzucając konieczność posiadania przez nie funkcji eksportu dokumentów, metadanych, rejestru zmian wraz z powiązaniami do formatu XML.

Wymagania odnoszące się do przekazywania dokumentów elektronicznych do archiwów państwowych zostały określone w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 2 listopada 2006 roku [10]. Według rozporządzenia nośniki danych przeznaczone do tego celu powinny być oznakowane informacjami zawierającymi:

1) nazwę podmiotu przekazującego,

2) tytuł określający zawartość,
3) datę zapisu,
4) oznaczenie ustawowej ochrony informacji lub jej brak
5) nazwę oprogramowania i urządzenia użytego do zapisu.

Koniecznym jest aby były one odczytywane przez urządzenia produkowanych przez różnych producentów, właściwych dla danego typu nośnika. Określone zostały również środowiskowe warunki przechowywania poprzez podanie zakresu temperatur (18^{O}C–22^{O}C) oraz wilgotności względnej (40%–50%).

Materiały archiwalne przekazuje się w postaci niezaszyfrowanej, a ich metadane w formie XML o strukturze podanej w załączniku do ustawy. Załącznik ten definiuje także strukturę samego zapisu. Najwyższym jej poziomem są foldery:

- „dokumenty", zawierający przynajmniej jeden plik,
- „metadane" z plikami metadanych odpowiadającym dokumentom elektronicznym zamieszczonym w folderze dokumenty oraz
- „sprawy" z metadanymi dotyczącymi grupy dokumentów.

Całość spakowana w jeden nieskompresowany plik zwany „paczką archiwalną", o strukturze uzgodnionej z archiwum państwowym podpisywana jest podpisem elektronicznym.

Wątpliwości może budzić zapis w ustawie o nieszyfrowaniu przekazywanej dokumentacji. Może ona zawierać, jak wynika z samej formy opisu nośnika, materiały prawnie chronione. Niejasny jest również cel braku kompresji. Jak wiadomo istnieją powszechnie stosowane algorytmy kompresji bezstratnej, które nie powodują utraty informacji ani pogorszenia jakości przekazywanych materiałów.

Informacje niejawne

Termin informacja niejawna został zdefiniowany w ustawie o ochronie informacji niejawnych [11] jako informacja wymagająca ochrony przed nieuprawnionym ujawnieniem, stanowiąca tajemnicę państwową lub służbową, niezależnie od formy i sposobu jej wyrażania. Za tajemnicę państwową

uważana jest informacja, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów kraju. Tajemnica służbowa to informacja niejawna, która nie jest tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie może narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej.

Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej, która je przetwarza, oraz powołany przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany skrótowo pełnomocnikiem ochrony. Do zadań pełnomocnika ochrony, jego zastępcy oraz wyspecjalizowanej komórki zwanej pionem ochrony należy w szczególności:

1) zapewnienie ochrony informacji niejawnych, w tym ich ochrony fizycznej,
2) zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne,
3) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
4) okresowa kontrola ewidencji, materiałów i obiegu dokumentów,
5) opracowywanie planu ochrony informacji niejawnych w jednostce organizacyjnej i nadzorowanie jego realizacji,
6) szkolenie pracowników w zakresie ochrony informacji niejawnych.

Informacje niejawne o przyznanej klauzuli tajności mogą być wytwarzane, przetwarzane, przekazywane oraz przechowywane w warunkach, które uniemożliwiają ich nieuprawnione ujawnienie. Warunki te zostały sprecyzowane w rozporządzeniu Rady Ministrów w sprawie organizacji i funkcjonowania kancelarii tajnych [12].

Dostęp do informacji niejawnych mogą mieć jedynie osoby uprawnione, posiadające odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa, po przeprowadzeniu postępowania sprawdzającego, które przeszły odpowiednie szkolenie, oraz jednostki organizacyjne

wykonujące umowy związane z ich przetwarzaniem. Jednostki te mają jednak obowiązek zapewnienia odpowiednich warunków ochrony, potwierdzonych dokumentem zwanym świadectwem bezpieczeństwa przemysłowego, wydawanym przez Służbę Kontrwywiadu Wojskowego lub Agencję Bezpieczeństwa Wewnętrznego.

Cały rozdział dziesiąty ustawy [11] poświęcony jest bezpieczeństwu systemów i sieci teleinformatycznych. System teleinformatyczny, w myśl ustawy, składa się z urządzeń, narzędzi, metod postępowania i procedur stosowanych przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji. Sieć teleinformatyczna to organizacyjne i techniczne połączenie systemów teleinformatycznych. Sieci i systemy służące do przetwarzania informacji niejawnych podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

Certyfikat akredytacyjny dla sieci i systemów wydawany jest na podstawie postępowań sprawdzających wobec osób mających do nich dostęp oraz – zatwierdzonych przez właściwą służbę ochrony państwa – dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji. Konieczne jest także wykonanie audytu bezpieczeństwa systemu lub sieci teleinformatycznej, polegającego na weryfikacji poprawności realizacji wymagań i procedur, określonych we wspomnianych dokumentach.

Organy samorządu terytorialnego mają do czynienia z informacjami stanowiącymi tajemnicę państwową o klauzuli tajne. Dotyczą one przede wszystkim obrony cywilnej, programów mobilizacji, systemów przekazywania informacji niejawnych oraz rezerw państwowych usytuowanych na terenach podlegających ich jurysdykcji. Ściśle tajne informacje posiadane przez samorządy terytorialne odnoszą się do obiektów militarnych położonych na podległych im obszarach.

Dane osobowe

Zagadnienia związane z ochroną danych osobowych poruszane są w licznych aktach prawnych takich jak:

- Konstytucja Rzeczypospolitej Polskiej,
- Kodeks cywilny,
- Kodeks pracy,
- Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (UODO) [13; 14] i akty wykonawcze ustawy.

Definicja danych osobowych zawarta w ustawie stanowi, że są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Ta szeroka definicja ma jedno ograniczenie. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Żadne przepisy nie określają ilościowo kosztów i czasu, które moglibyśmy uznać za nadmierne.

Ustawa obejmuje dane osobowe, zawarte w:

- kartotekach,
- skorowidzach,
- księgach,
- wykazach,
- innych zbiorach ewidencyjnych,
- systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

Za zbiór danych uważa się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Przez pojęcie system informatyczny rozumie się zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Organem do spraw ochrony danych osobowych jest powoływany i odwoływany przez Sejm Rzeczypospolitej Polskiej, za zgodą Senatu, Generalny Inspektor Ochrony Danych Osobowych (GIODO). GIODO wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. W przypadku naruszenia przepisów o ochronie danych osobowych wykrytych w skutek prowadzonej w drodze decyzji administracyjnej kontroli, nakazuje przywrócenie stanu zgodnego z prawem.

UODO zobowiązuje administratora danych do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności wyróżnia zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem [15]. Wspomniane środki zostały opisane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych [16].

Diagnoza stanu obecnego

Szczegółowe wytyczne dla instytucji publicznych odnośnie budowy systemu zarządzania bezpieczeństwem informacji zawarte są w Rozporządzeniu Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanym w dalszej części jako KRI [17]. Realizuje ono art. 18 ustawy z 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne [18], który zobowiązuje Radę Ministrów do określenia w drodze rozporządzenia, wymagań mających na uwadze zapewnienie między innymi sprawnej i bezpiecznej wymiany informacji w postaci elektronicznej.

W § 20.1. KRI czytamy, iż „Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność".

Następny ustęp rozporządzenia precyzuje działania związane ze wspomnianym systemem: „§ 20. 1. 1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia" [17]. Poszczególne jego punkty stanowiły przedmiot badań prowadzonych w 2015 roku przez Polskie Towarzystwo Informatyczne [19]. Ankietowano 339 instytucje, począwszy od Urzędów Marszałkowskich, po Urzędy Gminne. Badano czy ankietowane instytucje posiadają aktualną Politykę bezpieczeństwa.

Ponad 88% urzędów posiada Polityki bezpieczeństwa informacji jednakże aż 62% z nich jest nieaktualnych. Ponieważ ostatnie zmiany w ustawie z 29 sierpnia 1997 roku o ochronie danych osobowych, wniesione ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej [20], obowiązują od dnia 1 stycznia 2015 roku, uznano, iż wszystkie polityki wydane przed rokiem 2014 i nieaktualizowane w latach 2014-2015 są nieaktualne.

Kolejny paragraf KRI stanowi: „§ 20. 1. 2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację". Wykonanie inwentaryzacji aktywów teleinformatycznych zadeklarowało 159 urzędów (46,9%), przy czym aktualną, nie starszą niż dwa lata, posiadały 103 jednostki (30,38%). Pomimo deklaracji 46 urzędów nie potrafiło podać liczby aktywów, zaś kolejnych 40 podało liczbę mniejszą od sumy aktywnych węzłów sieci i baz danych. Dodatkowo 5 następnych określiło liczbę aktywnych węzłów sieci znacząco mniejszą niż liczba pracowników. Szczegóły zostały przedstawione w tabeli 3. 1. Ponieważ niemal każdy z pracowników urzędu wykonuje pracę biurową i dysponuje zapewne komputerem, wydaje się mało prawdopodobne, by liczba aktywnych węzłów sieci (komputery, laptopy, przełączniki, rou-

tery, serwery, drukarki sieciowe) stanowiła 90% lub mniej liczby pracowników urzędu. Reasumując, wiarygodną i aktualną inwentaryzację posiadało jedynie 3,54% badanych organizacji.

Tabela 3.1. Inwentaryzacje aktywów teleinformatycznych w badanych instytucjach

Stan inwentaryzacji	Liczba instytucji	% populacji
Brak inwentaryzacji	180	53,10
Nieaktualna inwentaryzacja	56	16,52
Niewiarygodna inwentaryzacja	91	26,84
Aktualna i wiarygodna inwentaryzacja	12	3,54

W § 20. 1. 3) Krajowych Ram Interoperacyjności czytamy: „przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy" [17]. Jednakże niewiele instytucji opracowało analizę ryzyka. Z deklaracji wynika, że analizę ryzyka wykonało 81 jednostek (23,89%). Jedynie 61 analiz można było uznać za aktualne. Respondenci nie umieli, bądź nie znali nazw użytych metodyk. Wymieniali często nazwy, których większość, nie jest nazwami metodyk, lecz metod badawczych lub metodyk zarządzania projektami. Wśród nich znalazły się:

- burza mózgów,
- Prince 2,
- arytmetyczna,
- PMI,
- delficka,
- indukcyjna,
- ręczna.

Kolejny zapis KRI to § 20. 1. 6): „zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji" [17]. W zakresie stosowania odpowiednich norm PN-ISO/IEC, które zostały wprost wymienione w § 20. 3.,

dokonano 2 973 szkoleń przypadających na pojedynczego urzędnika co stanowi ok. 11% zatrudnionych (niektórzy urzędnicy byli jednak szkoleni z kilku norm). Szczegółowe dane odnośnie szkoleń zamieszczono w tabeli 3. 2.

Tabela 3. 2. Szkolenia w zakresie stosowania norm PN-ISO/IEC

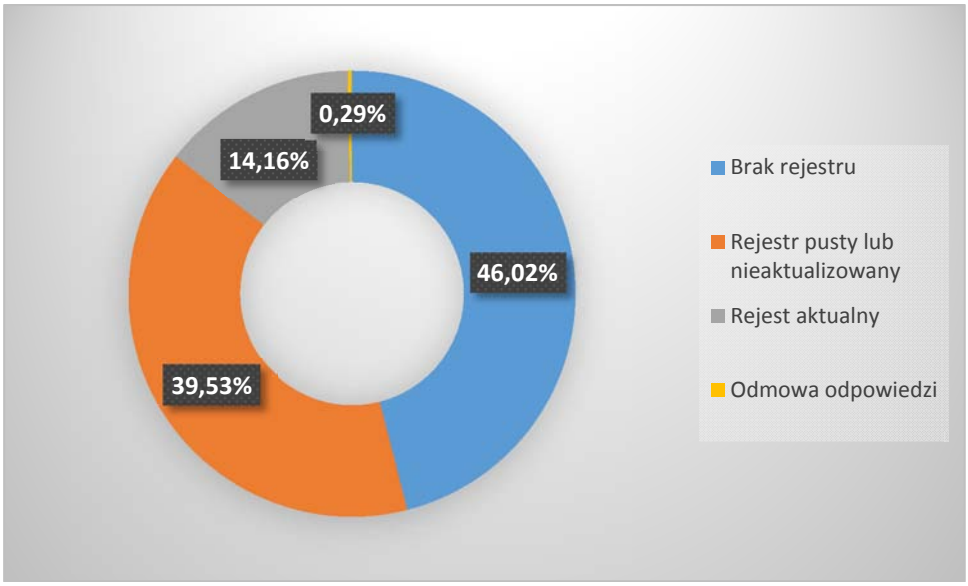
Norma	Liczba przeszkolonych	Liczba urzędów realizujących szkolenia
PN-ISO/IEC 20000 [21; 22]	106	6
PN-ISO/IEC 27001 [23]	2 564	23
PN-ISO/IEC 27005 [24]	160	11
PN-ISO/IEC 24762 [25]	143	6

Nie można również mówić o samoszkoleniu, gdyż badane urzędy zakupiły łącznie 31 wspomnianych norm, przy czym najmniejszym zainteresowaniem cieszyła się norma PN-ISO/IEC 20000 [21, 22], dotycząca zarządzana usługami realizowanymi przez systemy teleinformatyczne. Zdecydowana większość instytucji, tj. 309, co stanowi ponad 91% badanych, nie zakupiła ani jednej z nich.

Kolejny zapis KRI, § 20. 1. 12) h), nakazuje „kontrolę zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa" [17]. Jedynie 7 urzędów przeprowadziło audyt na zgodność z normą PN-ISO/IEC 20000. Audyt dotyczący normy PN-ISO/IEC 27001 wykonało trochę więcej organizacji tj. 24. Znacznie mniej uzyskało certyfikat, odpowiednio 3 i 10 urzędów przy czym oba posiadały tylko 2 urzędy. Prawie połowa instytucji (48,08%) przeprowadziła audyt swojej Polityki bezpieczeństwa.

W § 20. 1. 13) Krajowych Ram Interoperacyjności czytamy: „bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących" [17]. Spełnienie powyższego przepisu kontrolowane było jedynie pośrednio poprzez weryfikację prowadzenia rejestru incydentów. Ponad połowa (53,69%) respondentów zadeklarowała jego prowadzenie, jednakże 134

rejestry pozostają puste gdyż nie zarejestrowano w nich żadnego incydentu. Szczegółowe informacje zostały zaprezentowane na rysunku 3. 1.



Rys. 3. 1. Rejestry prowadzone przez badane instytucje

Cześć z incydentów było na tyle poważnych, iż 13 urzędów zgłosiło je do zespołu CERT, Agencji Bezpieczeństwa Wewnętrznego lub prokuratury. Warto zauważyć, że 3 instytucje dokonały takiego zgłoszenia, lecz nie prowadziły rejestru incydentów.

Kolejny, § 20. 1. 14), punkt KRI dotyczy „zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok" [17]. Pomimo że 205 ankietowanych deklarowało roczny lub krótszy okres aktualizacji, to ponad 39% z nich aktualizowało swoje Polityki po co najmniej dwuletnim okresie czasu. Audyty na zgodność z normą PN-ISO/IEC 27001, która dotyczy zarządzania bezpieczeństwem informacji, jak już wspomniano wykonało zaledwie 7% badanej populacji. Większość tj. 75% z nich wykonana było w przeciągu ostatniego roku.

Wnioski i spostrzeżenia

Tylko nieliczne jednostki samorządu terytorialnego posiadają system zarządzania bezpieczeństwem informacji zgodnie z przepisami KRI. Procedury dotyczące wdrażania, wycofania, bieżącej eksploatacji oraz testowania aktywów – o ile w ogóle istnieją – mają charakter niesformalizowany. Liczba jednostek, w których funkcjonuje przynajmniej jedna z poszczególnych rodzajów procedur, została zaprezentowana w tabeli 1. 3.

Tabela 3. 3. Jednostki posiadające procedury zarządzania aktywami teleinformatycznymi

Kryterium – przynajmniej 1 udokumentowana procedura dotycząca:	Liczba jednostek	% badanej próby
wdrażania aktywów	90	26,55
eksploatacji aktywów	134	39,53
wycofania aktywów	93	27,43
testowania aktywów	61	17,99

Pomimo niskich kompetencji służb informatycznych, o których świadczą przytoczone przykłady nieznajomości metodyk oraz pytania o znaczenie terminologii zadawane przez respondentów, zauważono niechęć do wspomagania się zewnętrznymi wykonawcami analizy ryzyka czy audytu Polityki bezpieczeństwa. Skorzystało z tej możliwości odpowiednio 11 i 77 instytucji.

Zauważono jednak, że zewnętrzny wykonawca nie gwarantuje wykonania wysokiej jakości prac. Należy zastanowić się nad możliwością certyfikacji tego typu usług, analogicznie jak w propozycji stosowania certyfikowanego sprzętu i oprogramowania w systemach teleinformatycznych w podmiotach publicznych, zawartej w Założeniach do Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej [26].

Obowiązki dotyczące między innymi bezpieczeństwa informacji zostały narzucone instytucjom publicznym poprzez przepisy rozdziału IV KRI. Nieokreślony jednak został termin ich wdrożenia, gdyż w § 23 czytamy:

„Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o których mowa w rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia" [17]. Rozporządzenie nie definiuje pojęcia „istotna modernizacja", co w połączeniu z niskim tempem wymiany systemów informatycznych w instytucjach może spowodować, iż faktyczne wejście w życie wspomnianych przepisów będzie odwlekane jeszcze przez długie lata. Pomimo, że rozporządzenie wydano w roku 2012, nadal tylko nieliczne jednostki samorządowe podjęły starania związane z wdrożeniem przepisów KRI.

Wyjątkiem jest przepis §19 KRI, dotyczący spełnienia wymagań Web Content Accessibility Guidelines (WCAG 2.0) na poziomie AA przez systemy teleinformatyczne eksploatowane przez podmioty realizujące zadania publiczne i służące prezentacji zasobów informacji. Termin jego wdrożenia został ustalony w § 22 KRI, o treści: „Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od dnia wejścia w życie niniejszego rozporządzenia" [17].

Już pobieżna inspekcja portali BIP badanych organizacji wykazała, że podjęły one działania dostosowujące je do wytycznych WCAG 2.0. Jednoznaczne określenie terminu wdrożenia stymulująco wpływa na podjęcie działań. Z tego też względu zapis § 22 należy uznać za szkodliwy. Nie skorzystano z możliwości jego skorygowania przy okazji wydania rozporządzenia Rady Ministrów z 27 listopada 2014 roku zmieniającego rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych [27]. Z niewiadomych względów przedkłada się skądinąd niezwykle ważne zagadnienie dostępu do informacji osób niepełnosprawnych nad bezpieczeństwo informacji i odpowiednie nią zarządzanie.

Systemowi zarządzania informacją poświęcono w KRI znaczną część rozdziału IV. Celem zawartych w nim przepisów było określenie minimalnych wymagań związanych z bezpieczeństwem informacji przetwarzanych przez podmioty publiczne. Jednocześnie utworzono niejako furtkę pozwalającą na odsuwanie w czasie ich stosowania.

Jednostki samorządowe, zdają sobie sprawę z niejasnej sytuacji, stąd właśnie niechęć do udzielania informacji opisana w części poświęconej przebiegowi badań. Dodatkowo brak nadzoru i kontroli, wytknięty już przez Najwyższą Izbę Kontroli [28], w połączeniu z sygnalizowanymi w badaniach barierami finansowymi powodują, iż wdrożenie przepisów KRI będzie się przeciągało. Warto zauważyć, że działania Generalnego Inspektora Ochrony Danych Osobowych polegające na popularyzacji przepisów oraz kontroli ich przestrzegania przynoszą rezultaty. Niemalże wszystkie urzędy posiadają Politykę bezpieczeństwa dotyczącą ochrony danych osobowych.

Literatura

[1] Jakub Wątor, I*le kosztują twoje dane osobowe? Mniej niż ci się wydaje*, Wyborcza.biz, http://wyborcza.biz/biznes/1,147881,17592085,Ile_kosztuja_twoje_dane_osobowe__Mniej_niz_ci_sie.html

[2] Ustawa z 29 września 1994 r. o rachunkowości, Dz.U. 1994 nr 121 poz. 591

[3] Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. 1993 nr 47 poz. 211

[4] Arkadiusz Michalak, *Nowelizacja Kodeksu cywilnego. Ochrona tajemnic handlowych w trakcie negocjacji*, „Monitor Prawniczy" 2003, nr 13

[5] Arkadiusz Michalak, *Ochrona tajemnicy przedsiębiorstwa*, Kantor Wydawniczy Zakamycze, Kraków 2006

[6] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2001 nr 112 poz. 1198

[7] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej, Dz.U. 2007 nr 10 poz. 68

[8] Ustawa z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, Dz.U. 1983 nr 38 poz. 173
[9] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi, Dz.U. 2006 nr 206 poz. 1518
[10] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i in-formatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych, Dz.U. 2006 nr 206 poz. 1519
[11] Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U. 1999 nr 11 poz. 95
[12] Rozporządzenie Rady Ministrów z 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych, Dz.U. 2005 nr 208 poz. 1741
[13] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133 poz. 883
[14] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 czerwca 2014 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych, Dz.U. 2014 poz. 1182
[15] Przemysław Jatkiewicz, *Ochrona danych osobowych. Teoria i praktyka*, Polskie Towarzystwo Informatyczne, Warszawa 2015
[16] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. 2004 nr 100 poz. 1024
[17] Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526

[18] Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565
[19] Przemysław Jatkiewicz, *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego. Raport z badań*, Polskie Towarzystwo Informatyczne, Warszawa 2016
[20] Ustawa z 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, Dz.U. 2014 poz. 1662
[21] Norma Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja, PN-ISO/IEC 20000-1:2007
[22] Norma Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania, PN-ISO/IEC 20000-2: 2007
[23] Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PN-ISO/IEC 27001:2014
[24] Norma Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, nieaktualna PN-ISO/IEC 27005:2014, zastąpiona przez PN-ISO/IEC 27001:2007
[25] Norma Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie, PN-ISO/IEC 24762:2010
[26] *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf
[27] Rozporządzenie Rady Ministrów z 27 listopada 2014 r. zmieniające rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2014 poz. 1671
[28] *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz krajowych ram interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na*

prawach powiatu, KAP-4101-002-00/2014, Najwyższa Izba Kontroli, Warszawa luty 2015

Streszczenie

W artykule omówiono przepisy dotyczące bezpieczeństwa informacji w systemach informatycznych instytucji publicznych. Przedstawiono również wyniki badań związanych z systemem zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego.

Słowa kluczowe: *bezpieczeństwo informacji, Krajowe Ramy Interoperacyjności, zarządzanie bezpieczeństwem, instytucje publiczne*

Notka o autorze

Przemysław Jatkiewicz – dr inż., wiceprezes Oddziału Pomorskiego PTI, rzeczoznawca PTI, wykładowca Uniwersytetu Gdańskiego, audytor ISO 27001, biegły sądowy w zakresie informatyki obejmującej zagadnienia bezpieczeństwa informacji, wdrażania technologii informatycznych, zarządzania systemami informatycznymi oraz informatyki śledczej przy Sądzie Okręgowym w Gdańsku, biegły skarbowy przy Izbie Skarbowej w Gdańsku.

Tomasz Klasa

Monitorowanie bezpieczeństwa informacji jako proces

W rezultacie rewolucji informacyjnej w gospodarce znajdujemy się w sytuacji, gdy w wielu obszarach informacja jest kluczowym czynnikiem przewagi konkurencyjnej. Utrata lub przejęcie informacji może mieć (bezpośredni lub pośredni) negatywny wpływ na działanie organizacji. Stąd konieczne stało się zapewnienie bezpieczeństwa informacji.

United States Code definiuje bezpieczeństwo informacji jako „ochronę informacji i systemów informacyjnych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem" [1: § 3542]. Zgodnie z tą definicją, przedmiotem ochrony jest zarówno informacja, jak i system informacyjny ją przetwarzający. Jednocześnie definicja wskazuje przed czym chronione są informacje, enumeratywnie wymieniając sześć podstawowych zagrożeń. Zagrożeniem jest potencjalna możliwość naruszenia, uszkodzenia zasobów [2], „okoliczność lub zdarzenie, które może potencjalnie wpłynąć na działania organizacji, jej zasoby, członków, inne organizacje lub państwo poprzez nieautoryzowany dostęp, zniszczenie, wyjawienie lub modyfikację informacji albo odmowę obsługi w ramach systemu informatycznego"[3: 8].

Zagrożenie jest definiowanie ogólnie, a więc jest niezależne od cech własnych zasobu czy zabezpieczenia tego zasobu. Czynnikiem umożliwiającym wystąpienie danego zagrożenia w konkretnym zasobie, zabezpieczeniu tego zasobu lub innym komponencie systemu, jest podatność. Definiuje się ją na przykład jako „związek trzech składowych: wrażliwości systemu lub błędu, dostępu napastnika do luki, możliwości wykorzystania luki przez atakującego" [4].

Podatność stanowi cechę danego zasobu, wynikającą z jego budowy lub implementacji. Może być skutkiem przyjętych założeń lub błędu w projektowaniu czy implementacji. Znana podatność może zostać usunięta (zneutralizowana) w ramach poprawki oprogramowania lub modernizacji urządzenia/zasobu. Z tego powodu – choć dla wygody zwykle grupuje się podobne zasoby – należy zawsze zwracać uwagę, czy całej grupy dotyczą te same podatności. W przeciwnym razie dojdzie do sytuacji, gdy jedna z podatności może zostać pominięta (dotycząca np. tylko jednego niezaktualizowanego zasobu w grupie i przeoczona, mimo, że jest znana jako podatność), albo szereg zasobów będzie zabezpieczany przed nieistniejącą podatnością (np. usuniętą przez poprawkę oprogramowania).

Istniejąca podatność oznacza, że może dojść do rzeczywistego naruszenia bezpieczeństwa. Elementem inicjującym podatność jest przyczyna (ang. *cause*), czyli sposób wykorzystania (użycia) danej podatności. Wśród przyczyn wykorzystania podatności można wskazać m.in:

- złożoność systemu – im większa, tym wyższe prawdopodobieństwo błędów;
- rozbudowaną łączność – liczne kanały komunikacyjne;
- błędy w zarządzaniu hasłami – słabe hasła lub niewłaściwe ich przechowywanie;
- błędy oprogramowania;
- brak kontroli danych wejściowych [5; 6].

Odpowiedzią na występowanie znanych podatności jest zastosowanie zabezpieczeń (zwykle oznaczających mechanizm techniczny, sprzętowy lub programowy) lub rozwiązań organizacyjnych, np. procedur, których stosowanie ma na celu poprawić poziom bezpieczeństwa.

Należy tu zwrócić uwagę na fakt, że zapewnienie całkowitego bezpieczeństwa nie jest możliwe [7], nawet kosztem całkowitego zablokowania wszelkiej działalności operacyjnej organizacji. Oznacza to, że można wdrożyć zabezpieczenia, które uniemożliwią użycie chronionego zasobu, a nadal będzie istniała co najmniej jedna podatność możliwa do wykorzystania. W rezultacie poziom bezpieczeństwa nadal będzie niższy niż 100%.

Dla ochrony bankomatu przed kradzieżą zwykle stosuje się zabezpieczenie fizyczne w postaci wmurowania go (wbetonowania) w ścianę lub do podłoża. Mimo to, jak pokazuje praktyka, nadal można go wyrwać za pomocą odpowiednio dużego pojazdu albo wysadzić ładunkiem wybuchowym. Zastosowanie zabezpieczenia w postaci zalania całego bankomatu betonem nie tylko uniemożliwi normalne użytkowanie go, ale też nie wyeliminuje zagrożenia kradzieży, choć konieczne będzie zaangażowanie znacznie większych środków (jeszcze większy samochód, więcej ładunków wybuchowych), aby atak się powiódł.

Dokładnie te same mechanizmy działają w odniesieniu do systemów teleinformatycznych – nie istnieją zabezpieczenia, których nie da się złamać, choć wielu z nich nie można pokonać w akceptowalnym z punktu widzenia próby włamania czasie.

Zgodnie z § 3542 United States Code [1], bezpieczeństwo informacji stanowi wypadkową trzech podstawowych domen bezpieczeństwa, realizowanych jako kombinacja rozwiązań sprzętowo-programowych:

- poufności,
- integralności,
- dostępności.

Poufność oznacza zapewnienie, że żaden nieautoryzowany podmiot nie uzyska dostępu do informacji objętej kontrolą. Jednocześnie należy zapewnić, że informacja ta nie zostanie wyjawiona stronie nieuprawnionej w jakikolwiek inny sposób (np. przekazanie przez osobę posiadającą odpowiednie prawa dostępu). Co więcej, zapewnienie poufności obejmuje także ochronę prywatności i wynikających z niej informacji [1].

Choć definicja ta jest powszechnie znana i rozumiana, ze względu na dość częste niedocenianie wagi informacji nie zawsze jest sumiennie stosowana. W rezultacie wiele przepływów informacji odbywa się bez należytej kontroli, a więc przyrost wiedzy przez nie wywołany i jej dalsze wykorzystanie mają miejsce w sposób niekontrolowany przez właściciela procesów biznesowych organizacji.

Integralność należy rozumieć jako zapewnienie ochrony przed niewłaściwą modyfikacją lub zniszczeniem informacji i zawiera w sobie zapewnienie jej autentyczności i niezaprzeczalności [1]. Wynika stąd, że dane zostały faktycznie wygenerowane przez uprawnionego autora (jednego z uczestników komunikacji, komponent systemu lub zaufaną stronę trzecią) i nie zostały zmodyfikowane w jakikolwiek niepożądany sposób. Niezauważona zmiana posiadanych danych może mieć poważne konsekwencje jeśli są one używane jako argumenty w procesie decyzyjnym. W takim przypadku modyfikacja danych wpływająca na brzmienie informacji może wpłynąć na podjęcie odmiennej decyzji (lub na wynik obliczeń). Dlatego podejmowanie decyzji oraz obliczenia należy opierać na pewnych danych lub w sposób świadomy działać w warunkach ograniczonej niepewności – wszelkie błędy możliwe do wykrycia i zniwelowania powinny być usunięte przed rozpoczęciem procesu decyzyjnego (lub obliczeń). Zapewnienie integralności danych pozwala zrealizować to wymaganie: zidentyfikować nieautoryzowane modyfikacje i wyeliminować je, zanim wpłyną na decyzje czy obliczenia.

Mimo iż znaczenie tej cechy bezpieczeństwa jest dość powszechnie znane, podobnie jak w przypadku poufności jest często marginalizowane wskutek przeświadczenia o bardzo małym prawdopodobieństwie (lub wręcz niemożliwości) wystąpienia takiego przypadku akurat w danej organizacji. Innym powodem jest wiara, że ewentualny błąd zostanie łatwo i szybko wykryty, więc poświęcanie energii na zapewnienie integralności jest bezcelowe.

Dotyczy to nie tylko mikroprzedsiębiorstw. Okazuje się, że nawet duży bank (co prawda w Rosji, ale jednak bank) przyjął od klienta i podpisał umowę o zmodyfikowanej treści. W efekcie za pożyczenie pieniędzy to bank będzie musiał płacić klientowi (a nie klient bankowi), w dodatku zmodyfikowane zapisy umowy zapewniają klientowi setki tysięcy USD kar za zerwanie umowy [8; 9]. Przykład ten pokazuje skutki celowego działania człowieka (klienta), ale skutki będą analogiczne także w przypadku działania niezamierzonego lub będącego następstwem błędu programu czy zakłóceń w transmisji danych.

Jako szczególny przypadek integralności w systemach bazodanowych występuje parametr spójności, będący przedmiotem badań [10; 11; 12]. Zapewnienie spójności oznacza zagwarantowanie, że nie naruszono zależności pomiędzy wartościami zapisanymi w poszczególnych tabelach bazy danych. Na przykład w środowisku SAP R/3 dokonując ręcznej modyfikacji pozycji dokumentu księgowego w tabeli BSEG, polegającej na zmianie kwoty księgowanej na koncie kosztowym i koncie kontrahenta (zachowując bilans dokumentu), spowodujemy naruszenie spójności danych, ponieważ wartość dokumentu jest równolegle przechowywana w szeregu innych tabel, w postaci dokumentów powiązanych.

W rezultacie, aby uniknąć utraty spójności danych, przeprowadzenie ręcznej korekty kwoty na pozycjach w tabeli BSEG wymaga zmodyfikowania dokumentów w szeregu tabel w bazie danych. Ze względu na tą właściwość system SAP R/3 posiada szereg mechanizmów wymuszających zapewnienie spójności, w tym mechanizmy kontrolujące zgodność danych dotyczących tego samego dokumentu, przechowywanych w różnych tabelach bazy danych. Przytoczona ręczna zmiana jedynie bezpośrednio w tabeli BSEG spowoduje zwrócenie błędu spójności danych podczas pierwszego użycia tego dokumentu, np. podczas wykonywania raportu pozycji pojedynczych albo sald kont (SAP_FI).

Dostępność oznacza zapewnienie niezawodnego i bezzwłocznego dostępu do informacji oraz jej wykorzystania [1]. Wynika z tego, że informacje muszą być dostępne na każde żądanie. Ten obszar bezpieczeństwa jest zwykle najbardziej niedoceniany. Podczas gdy wiele organizacji jest świadomych faktu istnienia szpiegostwa przemysłowego oraz skutków przypadkowych wycieków lub uszkodzenia danych, dbają one o restrykcyjne zapewnienie dostępności tych informacji. Utrata zasilania czy awaria sprzętowa mogą spowodować niedostępność potrzebnych danych w czasie, gdy mają być przetwarzane lub uwzględnione w procesie decyzyjnym. W takim przypadku może okazać się, że instytucja jest zmuszona podejmować decyzje w zwiększonym obszarze niepewności (co samo w sobie zwiększa prawdopodobieństwo podjęcia niewłaściwych działań) albo wręcz nie jest w stanie zrealizować swoich procesów biznesowych i musi wstrzymać

działalność aż do odzyskania dostępu do danych. Ponieważ taka przerwa może skutkować niezrealizowaniem nadarzającej się okazji, a więc wymiernymi stratami, dlatego zwykle dokonuje się klasyfikacji zasobów i procesów biznesowych ze względu na ich wrażliwość na naruszenie ciągłości działania [13].

Z bezpieczeństwem blisko związane jest pojęcie ryzyka. Zależność ta kształtuje się w ten sposób, że wzrost ryzyka zwykle współistnieje z pogorszeniem bezpieczeństwa i ma charakter uniwersalny. Dotyczy w takim samym stopniu rynków finansowych (obligacje skarbu państwa są bezpieczniejszą inwestycją niż akcje, bo ryzyko że przyniosą straty jest niższe), ruchu drogowego (ostra i szybka jazda zwiększa ryzyko wypadku, więc jest mniej bezpieczna), co sektora ICT (np. im więcej osób ma nadmierne uprawnienia, tym większe ryzyko, że któraś z nich spowoduje szkody, co obniża bezpieczeństwo danych w systemie).

Dominująca w literaturze definicja ryzyka wywodzi się z nauk ekonomicznych i nauk o zarządzaniu, gdzie ryzyko rozumiane jest jako możliwość zrealizowania się zagrożenia, a więc „zobiektywizowana niepewność wystąpienia niepożądanego zdarzenia"[14: 6], albo niepożądanego zdarzenia uniemożliwiającego osiągnięcie postawionych celów[15]. Zgodnie z definicją ISO, wprowadzoną w roku 2009, ryzyko definiuje się jako wpływ niepewności na cele – pozytywne lub negatywne odstępstwo od wartości oczekiwanej [16]. Cele mogą reprezentować różne aspekty organizacji (np. finansowy lub środowiskowy) i dotyczyć różnych poziomów (np. strategiczny, operacyjny). Ponieważ ryzyko wiązane jest z potencjalnym zdarzeniem lub jego konsekwencjami i uwzględnia prawdopodobieństwo wystąpienia takiego zdarzenia, mianem niepewności określono każdy brak informacji w zakresie możliwych zdarzeń, ich konsekwencji, czy prawdopodobieństwa wystąpienia [16]. Analogicznie do przytoczonej definicji ISO, sformułowano pojęcie ryzyka w zakresie bezpieczeństwa informacji [3].

Zrealizowanie się ryzyka zawsze związane jest ze skutkiem negatywnym. Na przykład, jeśli obciążenie zasobu (sieci komputerowej, serwera, bazy danych, pracownika etc.) jest znacząco niższe niż zaplanowane (co w pierwszej chwili wydaje się mieć pozytywny skutek, bo nie jest przeciążony), okazuje

się, że zasób ten nie jest optymalnie wykorzystany. Można było wybrać inne (generujące niższe koszty stałe) rozwiązanie, które także poradziłoby sobie z takim obciążeniem (tańszy silnik bazy danych, mniej zasobów dedykowanych bazie danych, sieć komputerowa o niższych parametrach etc.).

Innym, z pozoru pozytywnym, przykładem może być, wyższa niż zakładana, popularność jednej z usług w systemie (np. sklepu internetowego). W pierwszej chwili większa liczba użytkowników jest korzystna (większe przychody). Niestety, skutkiem ubocznym jest spadek komfortu obsługi systemu (zasoby przeznaczone do obsługi tej usługi okazują się niewystarczające, więc dochodzi np. do zauważalnego kolejkowania zgłoszeń). To prowadzi do niezadowolenia użytkowników lub wręcz spadku (zaniku) zainteresowania usługą.

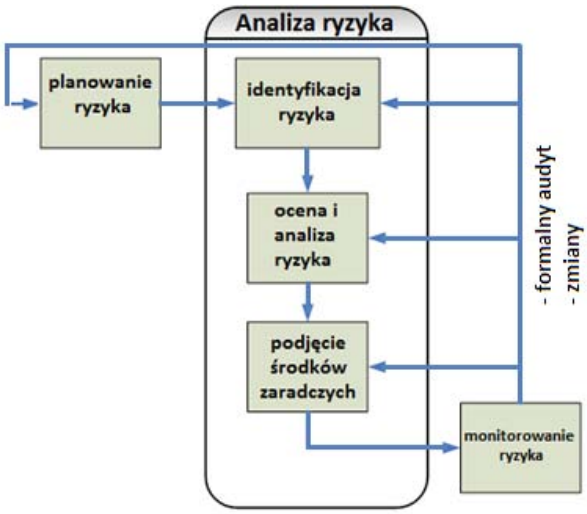
Choć ryzyko tradycyjnie definiuje się jako blisko związane z niepewnością [14; 16; 17], pojęcia te nie są tożsame. Jak wskazuje Pablo Guerron-Quintana, ryzyko można wyznaczyć tam, gdzie uda się ograniczyć niepewność i wskazać konkretne zagrożenia wobec określonych zasobów czy procesów. Brak wiedzy o możliwym rozwoju sytuacji (np. jakie są możliwe skutki zdarzenia X) nie pozwala na określenie ryzyka, tylko stanowi obszar niepewności, utrudniający zarządzanie i podejmowanie decyzji [18]. Stan bezpieczny można więc traktować jako przeciwieństwo niepewności. To stan, w którym badany obiekt zachowuje się w przewidywalny i oczekiwany sposób, co więcej – akceptowany i uznawany za poprawny.

Ze względu na związek między pojęciami ryzyka i bezpieczeństwa, proces zarządzania bezpieczeństwem nie może być rozpatrywany w oderwaniu od procesu zarządzania ryzykiem. Literatura z zakresu nauk ekonomicznych i nauk o zarządzaniu, poświęcona zagadnieniu zarządzania ryzykiem, wskazuje, że ma ono na celu ograniczenie stanu niepewności i zastąpienie go stanem znanym (pewnym), a ponadto bezpiecznym [18; 19].

Zarządzanie ryzykiem jest więc procesem ekonomicznej minimalizacji nieprzewidzianych skutków[20] oraz ograniczenia wpływu niepewności na realizowane cele biznesowe [21]. Proces zarządzania ryzykiem można podzielić na kilka podstawowych kroków. W polskiej literaturze [15; 22] wyróżnia się etapy:

- planowanie ryzyka (jako czynność wstępna, określająca cele do osiągnięcia);
- identyfikacja ryzyka;
- ocena ryzyka;
- zastosowanie środków zaradczych;
- monitorowanie ryzyka.

Podział ten pokazano na rysunku 4. 1. Strzałki obrazują możliwe przejścia między poszczególnymi etapami procesu – należy zwrócić uwagę na jego ciągły charakter wynikający z cyklicznego powtarzania poszczególnych kroków (z wyjątkiem planowania). Planowanie definiuje cele do zrealizowania poprzez zarządzanie bezpieczeństwem, a także wszelkie stałe ograniczenia tego procesu. Kolejne kroki natomiast służą realizacji postawionych celów.



Rys. 4. 1. Proces zarządzania ryzykiem, na podstawie [15; 23]

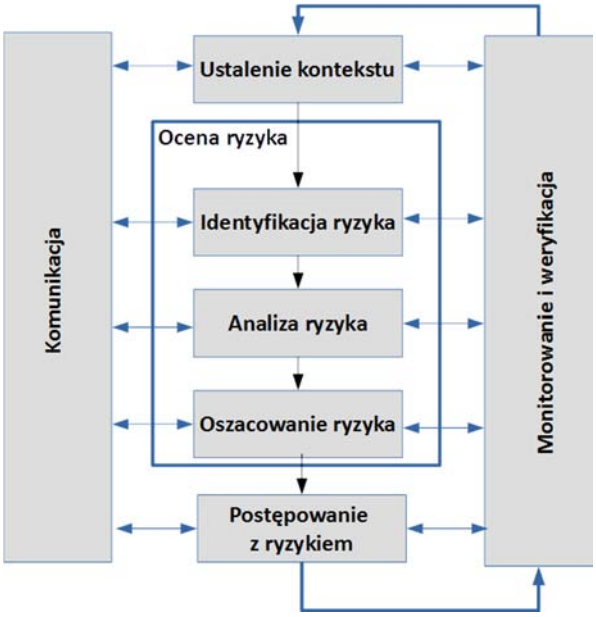
Podział ten jest zbliżony do przyjętego w opracowaniach i standardach zagranicznych [3; 23]. W roku 2009 zarządzanie ryzykiem zostało ustandaryzowane przez ISO w ramach normy ISO31000, przetłumaczonej następnie na język polski jako PN-ISO31000:2012 [24].

Zgodnie z tą normą, proces zarządzania ryzykiem dzieli się na:

1. ustalenie kontekstu;

2. ocena ryzyka (ang. *Risk assessment*) przy czym (podobnie jak w [22]), tu wyróżnia się etapy:
   a) identyfikacja ryzyka
   b) analiza ryzyka
   c) oszacowanie ryzyka (ang. *Risk evaluation*)
3. postępowanie z ryzykiem;
4. monitorowanie i weryfikacja;
5. komunikacja.

Podczas gdy kroki 1-3 (wraz z 2a-2c) są realizowane sekwencyjnie, monitorowanie i weryfikacja oraz komunikacja są realizowane równolegle do nich, na każdym z pozostałych etapów niezależnie. Wyniki monitorowania mogą wpływać na ustalenie kontekstu, inicjując zmiany w procesie zarządzania ryzykiem, np. gdy bieżąca procedura okaże się niewystarczająca. Całość pokazano na rysunku 4. 2.



Rys. 4. 2. Proces zarządzania ryzykiem [21]

W obu przypadkach widoczne jest podobieństwo do cyklu Deminga zwanego PDCA lub PDSA [25]. Planowanie zarządzania ryzykiem jest odpowiednikiem kroku Plan (P). Cała analiza ryzyka (wszystkie trzy kroki wchodzące w jej skład) stanowią odpowiednik kroku Do (D), a monitorowanie stanowi odpowiednik kroku Check (C) i dostarcza podstawę dla ewentualnego podjęcia działań udoskonalających proces zarządzania bezpieczeństwem (np. wskutek wykrycia nowych podatności albo nieskuteczności podjętych działań), czyli kroku Act (A) z cyklu PDCA.

Za odpowiednik analizy ryzyka w procesie zarządzania bezpieczeństwem informacji można przyjąć (w pewnym zakresie) audyt bezpieczeństwa informacji. Analogicznie, na podstawie przyjętych celów i założeń, dokonuje się identyfikacji zagrożeń oraz podatności z nich wynikających. Następnie poddaje się je ocenie aby ustalić, czy podatności te mają istotny wpływ na bezpieczeństwo. Jeśli tak, spośród dostępnych środków zaradczych dobiera się rozwiązania właściwe dla poszczególnych podatności. Wyróżnia się cztery rodzaje postępowania z ryzykiem [3; 26; 27]:

- akceptacja;
- unikanie;
- przeniesienie – jego przypadkiem szczególnym jest dzielenie ryzyka wyróżnione w [3] jako odrębny rodzaj postępowania z ryzykiem;
- ograniczenie.

Akceptacja oznacza pogodzenie się ze skutkami wystąpienia ryzyka i przyjęcie ich (obsłużenie) przez samą organizację w ramach bieżącej działalności operacyjnej. Takie postępowanie wybiera się z reguły, gdy stwierdzone ryzyko jest niskie lub gdy jego niwelowanie w jakikolwiek inny sposób jest ekonomicznie nieracjonalne (tzn. koszty są niewspółmierne do ewentualnych strat).

Na przykład wskutek zapisów prawnych i umownych (w tym w zakresie odpowiedzialności oraz konstrukcji ścieżki certyfikacji) ryzyko szczątkowe wynikające z niewłaściwego działania centrum certyfikacji jest oceniane jako niskie i powszechnie akceptowane. Nie stosuje się dodatkowych zabezpieczeń np. na wypadek utraty zaufania do wystawcy certyfikatów w wyniku zmiany jego właściciela, m.in. dlatego, że unieważnienie dotychczasowych

certyfikatów i zmiana ich dostawcy nie są ani procesem nadmiernie drogim ani zbyt skomplikowanym.

Przykładem wysokiego ryzyka, które jest powszechnie akceptowane, jest monitorowanie infrastruktury krytycznej, np. sieci energetycznych. Ze względu na rozległość i konstrukcję systemu, w szczególności ilość i wiek sprzętu nadzorującego pracę infrastruktury, nie jest możliwe wdrożenie odpowiednich zabezpieczeń komunikacji (np. szyfrowania) i dane o stanie infrastruktury są przesyłane w postaci jawnej, co podkreślono w [28]. Oczywiście stanowi to duże ryzyko, ale ze względu na koszt modernizacji infrastruktury, koniecznej dla zabezpieczenia komunikacji, zwykle ryzyko to jest akceptowane.

Unikanie ryzyka oznacza, że organizacja wprowadza do swoich procedur i/lub procesów biznesowych zmiany, które uniemożliwiają wystąpienie danego ryzyka. Na przykład aby uchronić się przed ryzykiem kradzieży danych wrażliwych w stylu zaprezentowanym przez pracowników amerykańskiej armii i wywiadu [29], powszechną praktyką staje się zakaz stosowania pamięci przenośnych. Ponieważ komputer jest zabezpieczony (sprzętowo lub programowo) w ten sposób, że podłączony dysk przenośny nie jest udostępniany użytkownikowi, nie jest możliwe zapisanie na nim danych, a więc użycie go do kradzieży informacji.

Przeniesienie ryzyka oznacza, że odpowiedzialność za zaistniałe zdarzenie zostanie poniesiona przez stronę trzecią (zwykle firmę ubezpieczeniową lub podwykonawcę). Typowym przykładem przeniesienia ryzyka jest wykupienie opieki serwisowej w firmie zewnętrznej – w zamian za określoną opłatę miesięczną firma ta zobowiązuje się usunąć usterki w wyznaczonym w umowie terminie.

Ograniczenie ryzyka to sytuacja, w której organizacja podejmuje działania mające na celu ograniczenie prawdopodobieństwa i/lub skutku wystąpienia danego ryzyka. Na przykład chcąc ograniczyć skutki utraty zasilania urządzeń w serwerowni instaluje się zapasowe źródła zasilania (np. agregat prądotwórczy lub bateria).

W zależności od wybranego sposobu postępowania z ryzykiem odmienne jest zapotrzebowanie na monitorowanie poprawności działania

przyjętego postępowania z ryzykiem. W przypadku przeniesienia ryzyka wystarczy okresowo kontrolować, czy wszystkie ryzyka przeznaczone do przeniesienia są pokryte stosownymi ubezpieczeniami lub umowami. Godząc się na ryzyko, jedynie można zweryfikować, czy rzeczywista częstotliwość i skutki występowania danego ryzyka pokrywają się z wartościami oczekiwanymi. W przypadku unikania ryzyka, należy okresowo weryfikować, czy przyjęte mechanizmy mające na celu uniemożliwienie wystąpienia ryzyka faktycznie mu zapobiegają (tzn. czy nie powstał nowy sposób na obejście tych ograniczeń i zrealizowanie się ryzyka). W przypadku ograniczania ryzyka należy kontrolować, czy pomimo zastosowanych mechanizmów ryzyko nie zachodzi częściej i/lub nie wywołuje skutków większych niż jest to oczekiwane.

Proces zarządzania bezpieczeństwem informacji stanowi pochodną opisanego powyżej procesu zarządzania ryzykiem. Ze względu na specyfikę bezpieczeństwa informacji, w porównaniu z ryzykiem w ujęciu finansowym czy ekonomicznym, proces zarządzania bezpieczeństwem informacji jest opisany odrębnymi standardami. Jako przykład norm, które na przestrzeni czasu stanowiły podstawy obsługi tego procesu można wskazać m.in. [30; 31; 32].

Ze względu na wzajemne podobieństwa, prób kompleksowego podejścia do tematu można szukać wśród prac z zakresu zarządzania ryzykiem. Znaną metodą całościowego zarządzania ryzykiem w organizacji jest ERM, przedmiot publikacji zarówno krajowych [33; 34; 35], jak i zagranicznych [36; 37]. Ponieważ metoda ta służy do jednoczesnego zarządzania ryzykiem wywodzącym się z różnych obszarów organizacji, np. finansowym i operacyjnym, stanowi dobry punkt odniesienia dla budowy zintegrowanego systemu monitorowania bezpieczeństwa.

Podobnie jak w przypadku zarządzania bezpieczeństwem, dla każdego z obszarów (rodzajów) ryzyka istnieją dedykowane im rozwiązania, techniki i metody zarządzania (np. ryzykiem finansowym). Zintegrowane podejście ERM opiera się o definicje uniwersalnych metryk ryzyka oraz technik jego identyfikacji, niezależnych od obszaru funkcjonalnego. Niestety, podejście

takie ma zasadniczą wadę w postaci trudnych do określenia zależności między różnymi obszarami ryzyka [37]. Ponadto identyfikacja ryzyk różnego typu i przypisanie ich do poszczególnych obszarów organizacji w praktyce stanowi istotną barierę dla kadry zarządczej. Rozległość zagadnienia (prace analityczne muszą objąć całość organizacji, a nie jej poszczególne składowe z osobna) oraz jednoczesne dość słabe osadzenie metody w teorii organizacji [37] sprawiają, że dotyczy to w szczególności sektora mikro, małych i średnich przedsiębiorstw, zarówno w Polsce [35], jak i za granicą [38].

Próbą rozwiązania tego problemu jest np. usystematyzowanie budowy rozwiązania ERM zgodnego z ISO31000 za pomocą analizy dynamiki składowych systemu. Model systemu powstaje w tradycyjny sposób, ale zawiera informacje o sprzężeniu zwrotnym każdej operacji, a także opóźnieniach (tj. czasie trwania) poszczególnych operacji. Pozwala to na bardziej szczegółowe odwzorowanie analizowanego systemu, z naciskiem na sposób działania, a nie tylko jego strukturę [38].

Innym, poważnym problemem ERM jest wykładniczo rosnąca złożoność obliczeniowa – z każdym kolejnym rodzajem ryzyka rośnie liczba możliwych do zastosowania rozwiązań. Problem ten również dotyczy budowy zintegrowanego systemu monitorowania bezpieczeństwa. Gwałtowny wzrost liczby wymaganych obliczeń, wraz z każdym dodawanym ryzykiem czy zasobem, sprawia, że otrzymywana wydajność jest niewystarczająca dla większych, bardziej złożonych systemów. Wraz z rozwojem technik przetwarzania równoległego szukano więc sposobu zwiększenia wydajności analizy danych w zakresie bezpieczeństwa informacji [39].

Choć zrównoleglenie obliczeń niezaprzeczalnie zwiększa wydajność, nie stanowi rzeczywistego rozwiązania problemu, gdyż nie wpływa na faktyczną złożoność algorytmu, czyli liczbę obliczeń które trzeba wykonać. Ponieważ złożoność systemów i organizacji rośnie, tak jak i liczba ryzyk, które należy brać pod uwagę w trakcie analizy, zamiast zwiększania wydajności przetwarzania danych trzeba poszukiwać sposobów racjonalizacji zakresu danych podlegających przetwarzaniu. Oznacza to modyfikację zakresu, a więc wyeliminowanie parametrów zbędnych (nie wpływających na ocenę

stanu bezpieczeństwa), lub ograniczenie ilości danych, np. w wyniku zmiany częstotliwości próbkowania lub modyfikacji sposobu komunikacji.

Ponieważ podstawowym celem monitorowania ryzyka jest ciągłe kontrolowanie zagrożeń i wywoływanie zaplanowanych działań w reakcji na ich wystąpienie [21; 40], należy je prowadzić według stałego harmonogramu. Ponadto w literaturze można znaleźć także wskazania, że monitorowanie należy traktować jako proces ciągły lub cykliczny, którego nie można zakończyć. Zakończenie jednej iteracji (przebiegu) monitorowania nie stanowi zakończenia tego procesu, a jedynie zawiesza jego wykonanie do chwili ponownego wzbudzenia zgodnie z harmonogramem [15]. Kolejne iteracje monitorowania są wywoływane aż do zmiany harmonogramu (następuje przejście na nową sekwencję iteracji) lub do chwili zakończenia (przerwania) całego procesu zarządzania bezpieczeństwem [21].

Podsumowanie

Monitorowanie bezpieczeństwa informacji jest procesem pozwalającym na weryfikację, czy zastosowany w organizacji system zarządzania bezpieczeństwem działa poprawnie. Powinien także pomóc określić, czy nie zrealizowały się nowe, nieznane wcześniej zagrożenia. Osiągnięcie tych celów wymaga, by cały proces był odpowiednio zaplanowany i przygotowany. Trzeba uwzględnić wartość chronionych zasobów, a także obowiązującą kulturę organizacyjną, czy lokalizację źródeł danych. Proces monitorowania, zainicjowany jako składnik procesu zarządzania bezpieczeństwem/ryzykiem powinien trwać, przyjmując formę iteracyjną, przez cały okres zarządzania bezpieczeństwem. Fakt ten, wraz ze złożonością badanego systemu, powoduje stałe obciążenie organizacji, wymagając dodatkowych działań i obliczeń. Należy mieć to na uwadze, oprócz samych celów bezpieczeństwa, dobierając charakterystykę czy sposób realizacji tego procesu do danej organizacji.

Literatura

[1] *United States Code*, Title 44, Chapter 35, Subchapter III, Office of the Law Revision Counsel of the United States House of Representatives, Washington 2006

[2] Norma Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, ISO/IEC15408-1:2009

[3] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg: 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[4] *The Three Tenets of Cyber Security*, U.S. Air Force Software Protection Initiative, 2009, http://www.spi.dod.mil/tenets.htm

[5] Almantas Kakareka, *Chapter 23*, w: *Computer and Information Security Handbook*, (ed.) John R. Vacca, Morg14an Kaufmann Publications, Waltham 2009

[6] Jack Jones, *An Introduction to Factor Analysis of Information Risk (FAIR)*, 2006, http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

[7] Janusz Stokłosa, Tomasz Bilski, Tadeusz Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa – Poznań 2001

[8] Anna Plutecka, *Karta kredytowa z odsetkami 0 proc. i miliony odszkodowania. Jak pewien Rosjanin wykołował bank*, Wyborcza.biz, http://wyborcza.biz/biznes/1,101562,14408552,Karta_kredytowa_z_odsetkami_0_proc__i_miliony_odszkodowania_.html

[9] Оксана Грибкова, *Воронежец требует с банка 24 миллиона рублей компенсации за нарушение пунктов кредитного договора, заключенного на его условиях*, RIA Novosti, http://riavrn.ru/news/voronezhets-trebuet-s-banka-24-milliona-rubley-kompensatsii-za-narushenie-punktov-kreditnogo-dogovor/

[10] Silvana Castano, Maria Grazia Fugini, Giancarlo Martella, Pierangela Samarati, *Database Security*, ACM Press Books, Addison-Wesley, Wokingham 1995

[11] Andreas Geppert, Edward L. Wimmers, *Consistency Constraints in Database Middleware*, https://www.research.ibm.com/haifa/coopis/papers/p35.pdf

[12] Jan Jurjens, Eduardo B. Fernandez, *Secure database development*, w: *Encyclopedia of Database Systems*, (eds.) Ling Liu, Tamer M. Özsu, Springer US, New York 2009

[13] Krzysztof Białek, *Ciągłość działania w życiu codziennym*, „Zabezpieczenia" 2008, nr 3/4

[14] Martin R. Woodward, Michael A. Hennell, David Hedley, *A Measure of Flow Complexity in Program Text*, IEEE Transactions on Software Engineering 1979, Vol. SE-5, Iss. 1

[15] Zdzisław Szyjewski, *Zarządzanie projektami informatycznymi*, Wydawnictwo Placet, Warszawa 2001

[16] Norma Risk management – Vocabulary, ISO Guide73:2009

[17] Jerzy Kisielnicki, *Strategia informatyzowania organizacji w świetle ryzyka i niepewności*, mat. konf. Strategia Systemów Informacyjnych 1999, Akademia Ekonomiczna, Kraków 1999

[18] Pablo A. Guerron-Quintana, *Risk and uncertainty*, „Business Review" 2012, Q1

[19] Kazimierz Frączkowski, *Zarządzanie projektem informatycznym. Projekty w środowisku wirtualnym. Czynniki sukcesu i niepowodzeń projektów*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003

[20] Bogdan Lent, *Zarządzanie procesami prowadzenia projektów. Informatyka i Telekomunikacja*, Difin. Warszwa 2005

[21] Norma Risk management – Principles and guidelines, ISO/IEC31000:2009

[22] Mariusz Flasiński, *Zarządzanie projektami informatycznym*, Wydawnictwo Naukowe PWN, Warszawa 2007

[23] *A risk management standard*, Federation of European Risk Management Associations, Brussels 2003, http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf

[24] Norma Zarządzanie ryzykiem – Zasady i wytyczne, PN-ISO31000:2012

[25] Ronald Moen, Clifford Norman, *Evolution of the PDCA Cycle*, http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

[26] *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, (ed.) Cynthia A. Berg, Project Management Institute, Newtown Square 2000

[27] *A Guide to ISO 31000*, The Public Risk Management Association, Weston 2010, http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

[28] Bilal Al Baalbaki, Youssif Al-Nashif, Salim Hariri, Douglas Kelly, Autonomic Critical Infrastructure Protection (ACIP) System, *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications*, AICCSA, Ifrane 2013

[29] Kim Zetter, *Snowden smuggled documents from NSA on a thumb rive*, „Wired" 2013, 16 June, http://www.wired.com/2013/06/snowden-thumbdrive/

[30] Norma Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security, ISO/IEC TR13335-3

[31] Norma Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji, PN-ISO/IEC 17799:2007 – wersja polska

[32] Norma Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013

[33] Jadwiga Bizon-Górecka, *Modelowanie struktury systemu zarządzania ryzykiem w przedsiębiorstwie – ujęcie holistyczne*, Towarzystwo Naukowe Organizacji i Kierownictwa, Bydgoszcz 2007

[34] Anna Korombel, *What is ERM – Enterprise Risk Management?*, w: *Changes and Risk in Knowledge Based Economy*, (red.) R. Lescroart, A. Pachura, M. Kozak, Haute Ecole „Blaise Pascal", Arlon 2008

[35] Anna Korombel, *Enterprise Risk Management in Practice of Polish Small Business – Own Research Results*, w: *Business and Management 2012, The 7th International Scientific Conference. Selected Papers*, Vol. 2., VGTU Publishing House „Technika", Vilnius 2012

[36] Mark Nelson, James Ambrosini, *Enterprise Risk Management and Controls-Monitoring Automation Can Reduce Compliance Costs*, „Bank Accounting & Finance" 2007, February-March

[37] Frank Schiller, George Prpich, *Learning to organise risk management in organisations: what future for enterprise risk management?*, "Journal of Risk Research" 2014, Vol. 17, Iss. 8

[38] Ghana Bharathy, Michael K. McShane, *Applying a Systems Model to Enterprise Risk Management*, "Engineering Management Journal" 2014, Vol. 26, Iss. 4

[39] Yoonsun Lim, Myung Kim, Kwang Hee Seo, Ho-Kun Moon, Jin Gi Choe, Yu Kang, *An Enterprise Security Management System as a Web-Based Application Service for Small/Medium Businesses*, Conference Paper, "Information Security and Cryptology" Vol. 4318, January 2006

[40] Marek Pawlak, *Zarządzanie projektami*, Wydawnictwo Naukowe PWN, Warszawa 2006

Streszczenie

Monitorowanie bezpieczeństwa informacji jest procesem wymagającym sumiennego przygotowania i zaplanowania. Złożoność organizacji oraz ich systemów informacyjnych nie pozwala na skuteczne monitorowanie bezpieczeństwa w sposób nieuporządkowany czy nieprzygotowany. Zły dobór zakresu, ale też metod czy technik monitorowania może negatywnie wpłynąć na skuteczność procesu, nie pozwalając na wykrycie części zagrożeń. Jednocześnie, wraz ze wzrostem zakresu monitorowania rośnie znacząco oddzia-

ływanie na zwykłe funkcjonowanie organizacji – w postaci obciążenia dodatkowymi czynnościami, ale też ruchem danych w infrastrukturze ICT. W rezultacie, istotne jest, by na podstawie analizy dostępnych rozwiązań oraz wymagań samej organizacji dobrać odpowiedni zestaw działań.

Słowa kluczowe: *monitorowanie bezpieczeństwa informacji, proces monitorowania bezpieczeństwa, zarządzanie ryzykiem*

Nota o autorze

Tomasz Klasa – na co dzień konsultant freelancer SAP (FI, TR, Authorisations) i bezpieczeństwa systemów we własnej firmie TK Systems Security. Wykładowca akademicki, organizator inicjatyw o charakterze społecznościowym, członek Zarządu Głównego Polskiego Towarzystwa Informatycznego oraz Zarządu Oddziału Zachodniopomorskiego PTI. Audytor wewnętrzny ISO27001. Prowadzi badania naukowe w zakresie monitorowania bezpieczeństwa informacji w organizacjach wirtualnych. Posiada wszechstronne doświadczenie zawodowe w różnych obszarach związanych z bezpieczeństwem informacji: od zapewnienia ciągłości działania sprzętu, przez zarządzanie bezpieczeństwem informacji, po projektowanie i wdrażanie systemów informatycznych klasy ERP.

Janusz Żmudziński

Cena incydentów bezpieczeństwa. Kilka wybranych przypadków

Wprowadzenie

Informacja jest coraz cenniejszym zasobem współczesnych organizacji. Zasobem, który determinuje przyszłość firmy. Menedżerowie nie zawsze mają pełną świadomość jego wartości, ale nie doceniają również stopnia uzależnienia organizacji od systemów informatycznych gromadzących i przetwarzających dane. Dzieje się tak do momentu pierwszego nadużycia lub incydentu związanego z bezpieczeństwem informacji. A te stają się coraz powszechniejsze. Ich rezultatem mogą być straty finansowe, utrata reputacji, a nawet upadłość firm.

Jeżeli firmy nie chcą tracić nakładów poniesionych na tworzenie aktywów informacyjnych, to muszą zapewnić im odpowiedni poziom bezpieczeństwa. Takie postępowanie wynika zarówno z dobrej praktyki, jak i (coraz częściej) z różnorakich wymogów prawnych. Każda organizacja lub przedsiębiorstwo wykorzystujące systemy teleinformatyczne jest potencjalną ofiarą cyberprzestępstw oraz nadużyć związanych z nieautoryzowanym dostępem do informacji gromadzonych i przetwarzanych w tych systemach.

Poniżej przedstawiono kilka spektakularnych przypadków utraty informacji przez firmy na skutek udanych ataków przeprowadzonych przez cyberprzestępców. Opisane sytuacje miały miejsce w ostatnich latach czy miesiącach, będąc tematem doniesień medialnych. Konsekwencje incydentów bezpieczeństwa informacji w tych firmach były różne i zależały od stopnia zabezpieczenia firmy oraz sposobu reagowania kadry zarządzającej na wydarzenia zachodzące w trakcie trwania incydentu. Przebieg niektórych z nich został dość szczegółowo wyjaśniony, a innych jeszcze nie.

Nikt nie powinien czuć się bezpieczny

Postronni obserwatorzy mogą domniemywać, że firmy/organizacje, które profesjonalne zajmują się bezpieczeństwem komputerowym nie powinny mieć problemów z właściwym zabezpieczeniem swoich zasobów. Jednakże doświadczenie pokazuje, że tak nie jest. Przykładem są incydenty bezpieczeństwa, których doznały takie firmy jak RSA Security, DigiNotar i Hacking Team czy też amerykańska National Security Agency.

Wyciek danych z RSA Security

Miliony użytkowników na świecie wykorzystują tokeny SecurID firmy RSA Security podczas uwierzytelniania do zasobów teleinformatycznych przedsiębiorstwa lub zdalnego dostępu do kont bankowych. W marcu 2011 roku firma RSA Security padła ofiarą ataku na system teleinformatyczny [1]. Intruzi dotarli do poufnych informacji związanych z zabezpieczeniami tokenów SecurID.

Był to jeden z pierwszych głośnych ataków typu APT (ang. *Advanced Persistent Threat*) [2]. Plan ataku na RSA Security był tyleż zuchwały, co prosty. Napastnicy na początek wzięli na cel najsłabsze (zazwyczaj) ogniwo systemu bezpieczeństwa – człowieka. Posłużyli się klasycznym *phishingiem* [3]. Wybrani pracownicy otrzymali e-maile z załączonym plikiem arkusza Excel o nazwie *2011 Recruitment plan.xls*. Nazwa dokumentu miała zachęcić odbiorców do jego bezrefleksyjnego otwarcia. I tak też się stało. Przesłany dokument był zainfekowany złośliwym oprogramowaniem. Po jego uruchomieniu hackerzy zyskali dostęp do stacji roboczych i dysków sieciowych. Następnym krokiem było uzyskanie dostępu do sieci korporacyjnej i przesłanie, za pośrednictwem protokołu FTP, pozyskanych z niej informacji na zewnątrz.

Firma RSA przyznała, że dane (nie ujawniła, jakie dokładnie) przechwycone przez napastników mogły zostać wykorzystane do osłabienia skuteczności systemu uwierzytelniającego SecurID. Kluczowym elementem tego systemu są tokeny generujące jednorazowe hasła. Łupem złodziei mogły paść m.in. algorytmy wykorzystywane do tworzenia haseł jednorazowych

lub informacje pozwalające określić klucz tokena na podstawie jego numeru seryjnego.

Specjaliści szacowali, że wymiana tokenów SecurID w samym tylko sektorze bankowym może kosztować od 50 do 100 milionów dolarów (a wszystkich urządzeń było wówczas na świecie w użytku około 40 milionów) [4]. Do tej kwoty należy dodać przekładające się na finanse skutki utraty reputacji firmy, co wyraźnie odzwierciedliły np. notowania giełdowe RSA i jej konkurentów w kolejnych dniach i tygodniach po wystąpieniu zdarzenia.

Atak na system teleinformatyczny RSA Security został stosunkowo szybko wykryty – najprawdopodobniej dzięki sprawnemu działaniu systemu monitorowania bezpieczeństwa i pracy zespołów zarządzania incydentami. Informacje o tym zajściu zostały niezwłocznie opublikowane, a użytkownicy tokenów otrzymali wsparcie producenta i możliwość wymiany tokenów na nowe. Takie podejście firmy powinno być wzorem do naśladowania dla innych. Niestety, zdarza się to stosunkowo rzadko.

W ciągu ostatnich kilkunastu miesięcy zagrożenia APT stały się częste i agresywne. Organizacje stają wobec konieczności stałej weryfikacji skuteczności stosowanych przez siebie zabezpieczeń. Przypadek napaści na RSA pokazuje, że nawet firmie bardzo zaawansowanej technologicznie nie udało się ustrzec przed wypływem ważnych poufnych informacji. Przebieg ataku wyraźnie wskazywał na niewystarczający poziom świadomości bezpieczeństwa danych u części pracowników oraz ich braku czujności. Możliwość nawiązania połączenia FTP z zewnętrznymi systemami przez zainfekowane firmowe komputery świadczyła o braku należytej ochrony sieci. Słaby poziom monitorowania serwerów i stacji roboczych użytkowników pozwolił zaś na uruchomienie podrzuconego szkodliwego oprogramowania.

Upadek DigiNotar

DigiNotar był publicznym holenderskim centrum certyfikacji. Wystawiał m.in. certyfikaty kwalifikowane i certyfikaty SSL. W sierpniu 2011 roku eksperci z firmy F-Secure wykryli włamanie do DigiNotar [5]. Incydent został

ujawniony dopiero półtora miesiąca po fakcie. Przez cały ten czas włamywacze (ponoć irańscy hakerzy) swobodnie korzystali z fałszywych certyfikatów SSL. Wystawiono ich aż 531, m.in. dla takich znanych firm jak Google, Facebook, Twitter, Yahoo czy Skype, a nawet dla agencji rządowych (CIA, MI6, Mossad). Fałszywe certyfikaty pozwalały intruzom podszywać się pod wybrane serwisy internetowe, a potem „podsłuchiwać" oraz dowolnie zmieniać wiadomości przesyłane szyfrowanym kanałem.

Firma DigiNotar nie dołożyła należytej staranności w zakresie zarządzania bezpieczeństwem informacji w swoim przedsiębiorstwie. Liczne błędy przedstawiono w raporcie firmy Fox-IT, która badała omawiany incydent. Wyliczono m.in.: źle zaprojektowaną sieć, niezabezpieczone serwery, brak ochrony przed złośliwym oprogramowaniem, nieaktualizowane i źle monitorowane oprogramowanie systemowe, słabe hasła [6]. W efekcie tych zaniedbań hakerzy mogli włamać się do systemu informatycznego DigiNotar nawet już w maju 2009 roku (wg. ustaleń firmyF-Secure) i od tego czasu mieli swobodny dostęp do poufnych danych.

Jednak najkosztowniejszym błędem DigiNotar okazało się ukrywanie informacji o włamaniu i jego skali. W takiej sytuacji konieczna jest bardzo szybka reakcja na zaistniały incydent i pełna otwartość ze strony instytucji, która padła ofiarą ataku. Szczegóły włamania powinny zostać ujawnione bezzwłocznie, umożliwiając zminimalizowanie szkód. Tego obowiązku firma dopełniła dopiero wiele dni później. W efekcie producenci większości przeglądarek internetowych zablokowali certyfikat główny DigiNotar. Rząd holenderski uznał, że to centrum certyfikacji nie jest już zaufane. Jego reputacja topniała w oczach. W takich okolicznościach firma VASCO, amerykański właściciel DigiNotar, 20 września 2011 roku ogłosiła złożenie wniosku o upadłość DigiNotar [7]. Dwa miesiące po ujawnieniu ataku hakerów to centrum certyfikacji przestało istnieć. Jest to bardzo kosztowny skutek incydentu bezpieczeństwa.

Hacking Team

Historia włoskiej firmy Hacking Team jest jednym z ciekawszych incydentów bezpieczeństwa ostatnich lat. Rzadko się zdarza, aby celem udanego ataku i kradzieży danych była organizacja, której podstawą działalności jest wytwarzanie narzędzi umożliwiających włamania do systemów informatycznych, a Hacking Team takie właśnie oprogramowanie sprzedawała rządom na całym świecie. I sama stała się celem skutecznego ataku [8]. Włamywacze ukradli i opublikowali w Internecie ponad 400 GB danych, w tym kody źródłowe oprogramowania, wiadomości e-mail zespołu firmy, faktury, umowy, licencje.

Z ujawnionej korespondencji i danych umieszczonych na portalu WikiLeaks [9] można było dowiedzieć się, kim byli klienci – w większości służby specjalne z wielu krajów. Wśród skradzionych danych była dokumentacja techniczna oprogramowania iRemote Control System (RCS), bardzo rozbudowanego systemu, służącego do zdalnej kontroli, zbierania informacji oraz atakowania sieci, komputerów i telefonów komórkowych. Był też kod źródłowy części oprogramowania wytwarzanego przez Hacking Team. Zaatakowana firma w oficjalnym oświadczeniu jednakże stwierdziła, że najważniejsze elementy kodów źródłowych ich systemu nie zostały wykradzione i pozostały pod ochroną.

Nigdy nie określono deficytu finansowego poniesionego przez Hacking Team na skutek opisywanego incydentu. Firma z pewnością poniosła duże straty wizerunkowe. Atak nie posłużył też klientom firmy. Świat dowiedział się, jakie instytucje i z jakich krajów wykorzystują oprogramowanie szpiegowskie oraz ile za to płacą. Pierwszym poważniejszym następstwem ujawnionych przez WikiLeaks informacji dotyczących Hacking Team, była dymisja Szefa Służby Wywiadowczej Cypru (KYP) – Andreasa Pentarasa [10]. Do innych należą konsekwencje wykorzystania udostępnionych przez hackerów *exploity zero-day*, które firma wykorzystywała. W rezultacie niektóre z nich rozpowszechniły się w świecie i zostały wykorzystane przez hackerów i cyberprzestępców.

Warto zwrócić uwagę, że sprawca tego ataku do dziś pozostaje nieznany. W kwietniu 2016 roku opublikował on w Internecie opis techniczny swoich działań [11].

Finanse na celowniku

W różnych zestawieniach obserwowanych incydentów bezpieczeństwa na czele stawki znajdują się te związane z sektorem finansowym. Systematycznie w mediach pojawiają się informacje o próbach ataków lub wręcz udanych atakach na banki lub konta zwykłych obywateli. Wynika to zarówno z faktu, że banki oferują swoim klientom coraz więcej możliwości funkcjonowania w cyberprzestrzeni, jak i ze stosunkowo niskiej (wciąż) świadomości użytkowników w obszarze bezpieczeństwa.

Carbanak

Informacja o tym jednym z największych cyberprzestępstw w historii obiegła świat w lutym 2015 roku. Według informacji podanych przez Kaspersky Lab, międzynarodowa grupa złodziei określana jako gang Carbanak, próbowała od 2013 roku atakować około 100 instytucji finansowych w 30 krajach na świecie. W wielu przypadkach ataki zakończyły się powodzeniem.

Do zarażenia systemów bankowych dochodziło po udanych atakach wykorzystujących technikę spear-phishing. Napastnicy przesyłali do wybranych pracowników banków odpowiednio przygotowane wiadomości, które zawierały szkodliwe załączniki lub linki. Przestępcom udało się wprowadzić do bankowych sieci złośliwe oprogramowanie (zwane później trojanem Carbanak), które umożliwiało śledzenie aktywności pracowników. Trojan przekazywał przestępcom zrzuty ekranów i zapis wideo z zarażonych komputerów. Przestępcy, dzięki dokładnej analizie zachowań pracowników, mogli wykonywać przelewy w taki sposób, aby wyglądały na normalne operacje bankowe i nie wzbudzały podejrzeń.

W niektórych przypadkach gang uzyskiwał informacje o systemach obsługujących operacje przelewów finansowych, obserwując administratorów

za pomocą systemów wideo zainstalowanych w bankach. Pozwalało to cyberprzestępcom uzyskać dokładne informacje o zachowaniu pracowników i procedurach bankowych, a to z kolei umożliwiło naśladowanie ich aktywności w celu ukrywania zleceń przelewów lub wypłat gotówki z banków.

Cyberprzestępcom z gangu Carbanak zdarzało się również przejąć kontrolę nad bankowymi systemami księgowania i dokonywać kradzieży sztucznie podwyższając stan kont na moment kradzieży. Taka technika kradzieży nie była wcześniej obserwowana. Napastnicy zwiększali saldo na koncie ofiary, a następnie z tego konta była podejmowana „dodana" wcześniej kwota. Dzięki temu właściciele kont wykorzystywanych w trakcie kradzieży nie zauważali żadnych nieprawidłowości. Przed i po kradzieży stan konta był identyczny, więc nikt nie alarmował banku o kradzieży. To dawało więcej czasu złodziejom na podjęcie wykradzionych środków.

Inną ciekawą techniką wykorzystywaną podczas tej serii ataków był atak na bankomaty. Przestępcy byli w stanie przejąć kontrolę nad wybranymi maszynami i wysłać do nich polecenia wypłaty gotówki w określonym momencie. Ich wspólnicy po prostu musieli w odpowiednim momencie stawić się przed bankomatem i odebrać gotówkę bez konieczności używania jakichkolwiek kart.

Pojedyncze ataki trwały zazwyczaj od 2 do 4 miesięcy. Podczas nich z każdej zaatakowanej organizacji kradziono zwykle od 2,5 miliona do 10 milionów dolarów. Analitycy z Kaspersky Lab szacują, że straty instytucji finansowych będących ofiarami opisywanego ataku wyniosły co najmniej 300 mln dolarów. Na taką kwotę opiewają potwierdzone przelewy. Natomiast są podejrzenia, że faktyczna wartość może być nawet trzykrotnie wyższa i sięgać nawet 1 miliarda dolarów [12], zwłaszcza, że w momencie publikacji raportu wciąż były obserwowane ataki gangu Carbanak.

Co gorsza, zaobserwowano również ewolucję tego ataku. Kontynuatorami są Metel, GCman i Carbanak 2.0 [13]. Niestety, do tych napaści wykorzystywane jest jeszcze bardziej wyrafinowane oprogramowanie.

Opisywany incydent pokazuje, że nawet instytucje bankowe, które bez wątpienia mają świadomość znaczenia bezpieczeństwa informacji i inwestują

duże środki w ochronę oraz zatrudniają najlepszych specjalistów od cyberbezpieczeństwa, mogą również stać się ofiarami ataków. I – analogicznie jak w omawianych wcześniej incydentach – najsłabszym ogniwem w systemie bezpieczeństwa wydaje się być człowiek.

Centralny Bank Bangladeszu

Inna próba kradzieży niemal 1 miliarda dolarów zakończyła się niepowodzeniem [14]. Ofiarą był bank centralny Bangladeszu. Hakerom udało się ukraść „tylko" 81 milionów dolarów.

Przestępcom udało się pozyskać wiedzę niezbędną dokonywania transakcji w imieniu banku centralnego Bangladeszu (rachunek prowadzony był w Banku Rezerwy Federalnej w Nowym Jorku) i za pomocą kilkudziesięciu przelewów próbowali przetransferować blisko 1 miliard USD na kontrolowane przez siebie konta na Filipinach i Sri Lance. Nie wzbudzając niczyich podejrzeń udało im się wykonać jedynie 4 przelewy, na sumaryczną kwotę około 81 milionów USD. Zablokowano dopiero piątą transakcję. Przyczyną alarmu była literówka w nazwie odbiorcy. Przestępcy zamiast „foundation" podali „fandation". Udało się odzyskać większą część skradzionej kwoty.

Pozafinansowym rezultatem opisywanej kradzieży była dymisja prezesa banku. Nastąpiła ona w dzień po tym, jak minister finansów Bangladeszu stwierdził, że nie został poinformowany o cyberataku na bank centralny i dowiedział się o nim z mediów dopiero w miesiąc po wydarzeniu.

Prognozy na przyszłość

Zagrożenia urządzeń mobilnych

Od kilku lat rośnie liczba incydentów związanych z naruszaniem bezpieczeństw urządzeń mobilnych, głównie smartfonów. Ma to niewątpliwie związek z tym, że coraz większa część ruchu internetowego pochodzi właśnie z tych urządzeń. W najbliższym czasie ten udział będzie szybko rósł, co wynika m.in. z coraz większego rozpowszechnienia Internetu Rzeczy

i dostępności tanich urządzeń oraz rozwoju nowych technologii przesyłania danych. Zachęca to zorganizowane grupy cyberprzestępcze do zwiększenia intensywności ataków w tym obszarze. Aplikacje mobilne są szczególnie atrakcyjne z punktu widzenia cyberprzestępców, bo ich wyposażenie i częste podatności oprogramowania dają szerokie możliwości kradzieży nie tylko danych, ale i pieniędzy.

Profesjonalizacja cyberprzestępców

Od co najmniej kilkunastu lat obserwujemy wzrost skali działania i stopniową profesjonalizację cyberprzestępców oraz coraz większy stopień skomplikowania popełnianych przez nich przestępstw. Rosnąca specjalizacja przestępców spowodowała, że dziś mamy już do czynienia z rynkiem cyberprzestępstw jako usługi (*ang. Cybercrime as a Service*). Nawet niezbyt zaawansowani użytkownicy Internetu mogą przeprowadzać ataki wykorzystując wiedzę i doświadczenie cyberprzestępców. Dzięki tzw. „ukrytej sieci" (*Deep Web*) można zdalnie zakupić złośliwe oprogramowanie (wirusy, trojany itp.), atak DDoS czy też dane kradzionych kart kredytowych. Mimo usilnych starań organów ścigania w wielu krajach, podziemie przestępcze ma się raczej dobrze. Przykładowe ceny usług cyberprzestępców przedstawia tabela 5. 1.

Tabela 5. 1. Ceny usług cyberprzestępczych

Usługa	**Cena**
Kradzione dane karty płatniczej	od kilku zł
Kradziony dostęp do konta bankowego	od kilkudziesięciu zł (cena zależy od stanu konta)
Wynajęcie botnetu	od ok. 200 zł za 1 dzień
Oprogramowanie do ataku ransomware	od ok. 4000 zł za miesiąc
Atak sieciowy DDoS	od kilkudziesięciu zł za 1 godzinę
Wysłanie miliona wiadomości SPAM	od kilkudziesięciu zł
Dostęp do panelu administracyjnego, przejęcie strony internetowej	od kilku zł
Dostęp do konta premium w serwisie streamingu filmów	kilka zł

Deficyt specjalistów

Wśród kluczowych problemów związanych zapewnieniem adekwatnego poziomu bezpieczeństwa jest brak wystarczającej liczby odpowiednio wykształconych specjalistów z dziedziny cyberbezpieczeństwa. Wielu ekspertów z tej dziedziny, którzy pojawiają się na rynku, trafia zazwyczaj do sektora prywatnego, który z reguły oferuje wyższe płace. Specjalizacja z zakresu bezpieczeństwa pojawia się w czołówce każdej listy najbardziej pożądanych umiejętności w branży IT. Szacuje się, że obecnie na świecie brakuje ok. 1 miliona specjalistów z tej dziedziny.

Podejście do ochrony

Czasy, w których jedynymi zabezpieczeniami systemów informatycznych były jedynie programy antywirusowe, a później jeszcze firewalle, to już zamierzchła przeszłość. Obecnie do ochrony systemów teleinformatycznych służy cała gama rozwiązań technicznych. Co ważniejsze, systematycznie się ona powiększa. W ramach szeroko rozumianej architektury bezpieczeństwa obok wspomnianych już systemów chroniących przed oprogramowaniem złośliwym, czy też popularnymi zaporami sieciowymi, IDS/IPS coraz częściej obserwujemy takie zabezpieczenia jak systemy chroniące przed wyciekiem informacji (ang. *Data Leakage Protection* –- DLP), systemy SIEM, systemy ochrony przed atakami APT, systemy wykrywania podatności, systemy monitorowania aktywności użytkowników uprzywilejowanych i inne wyspecjalizowane zabezpieczenia np. wykorzystujące analizy BigData lub uczenie maszynowe.

Obserwując skalę oraz ewolucję cyberzagrożeń należy przyjąć, że każda organizacja została lub zostanie zaatakowana. Droga do uzyskania adekwatnego poziomu bezpieczeństwa będzie wymagała przemyślanych działań w skali całej firmy lub organizacji, opartych na szacowaniu ryzyka, dopasowania strategii działania do celów biznesowych organizacji, efektywnego przygotowania do szybkiej reakcji na incydenty bezpieczeństwa oraz ciągłej edukacji i doskonalenia personelu.

Podsumowanie

Czy przedstawione powyżej przykłady naruszenia bezpieczeństwa związane z utratą kluczowych informacji były incydentalne?

Niestety, nie. Raporty niezależnych instytucji np. Gartner, Ponemon, Forrester, Verizon oraz producentów rozwiązań bezpieczeństwa, wyraźnie pokazują, że takich incydentów jest każdego roku więcej i że dotykają coraz większej liczby przedsiębiorstw. Zazwyczaj nie są one tak głośne, jak te przedstawione powyżej, ale ich stale rosnąca liczba powinna niepokoić.

Analizy zaobserwowanych przypadków utraty informacji nasuwają pytanie o możliwości uniknięcia utraty informacji i nie ponoszenia wszystkich wynikających z nich konsekwencji. Odpowiedź wydaje się jednocześnie prosta i skomplikowana. Należy wdrożyć odpowiednie zabezpieczenia wynikające z poprawnie stworzonej i zaprojektowanej architektury bezpieczeństwa. Trzeba zwrócić szczególną uwagę na procesy związane z monitorowaniem bezpieczeństwa. Przebieg incydentów bezpieczeństwa w przypadku włamań do DigiNotar wskazuje, że zarówno samo monitorowanie stanu bezpieczeństwa, jak i reagowanie na incydenty nie było tam wdrożone w sposób zapewniający niezbędny poziom bezpieczeństwa informacji. Wynika to w dużej mierze z faktu, że do niedawna ten obszar był często pomijany.

Obecnie systemy informatyczne wyposażone są w wiele rozwiązań z dziedziny bezpieczeństwa. Należy pamiętać, że nawet najlepsze zabezpieczenia nie są w stanie zagwarantować 100% bezpieczeństwa, zwłaszcza, gdy mamy do czynienia z dużymi środowiskami informatycznymi. Niestety, nie są rzadkością sytuacje, gdy wdrażane mechanizmy bezpieczeństwa – zarówno rozwiązania techniczne, jak i organizacyjno-proceduralne – nie są właściwie zarządzane. Często zapomina się, że wdrożenie mechanizmów bezpieczeństwa nie kończy jednocześnie prac nad zapewnieniem bezpieczeństwa informacji. Zapewnienie bezpieczeństwa powinno być procesem ciągłym, stanowiącym połączenie technologii i wiedzy. Musi być wspierane systematycznymi audytami, podnoszeniem kwalifikacji personelu, ciągłym

monitorowaniem i analizą zagrożeń, pozwalającymi na efektywne zmniejszenie ryzyka ataku.

Oznacza to, że należy liczyć się z przyszłą systematyczną rozbudową systemu bezpieczeństwa. Rozbudowa ta musi być uzależniona od tego, jak się rozwija środowisko teleinformatyczne i od identyfikacji pojawiających się nowych zagrożeń. Dość wspomnieć, że na poczatku roku 2016 niemiecka firma AV Test Institute [15] zanotowała dzienny przyrost złośliwych kodów oprogramowania na poziomie ponad 390 000 dziennie.

Często popełnianym błędem w zarządzaniu jest lekceważenie czynnika ludzkiego. Oprócz ataków z Internetu, zawsze należy się liczyć z możliwością działań własnych pracowników, którzy wykryją luki w istniejącym systemie bezpieczeństwa lub nadużyją swoich uprawnień i będą starali się wykorzystać je do własnych celów, niezgodnych z prawem i interesami firmy.

Czy w najbliższej przyszłości będzie bezpieczniej? Odpowiadając na to pytanie można posłużyć się słynną odpowiedzią, jakiej na temat przyszłości udzielił Stanisław Lem: „Będzie tak samo, ale więcej". Zagrożeń będzie więcej. Incydentów bezpieczeństwa będzie więcej, czyli będzie niebezpiecznie, ale bardziej. Prognozy na przyszłość nie są zbyt optymistyczne.

Literatura

[1] Art Coviello, *Open Letter to RSA Customers*, http://www.rsa.com/node.aspx?id=3872

[2] Stefanie Hoffman, *Advanced Persistent Threats: A Breakdown*, http://blog.fortinet.com/advanced-persistent-threats-a-breakdown/

[3] Uri Rivner, *Anatomy of an Attack*, http://blogs.rsa.com/rivner/anatomy-of-an-attack/

[4] Rachael King, *EMC's RSA Security Breach May Cost Bank Customers $100 Million*, http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html

[5] Michael Hypponen, *DigiNotar Hacked by Black.Spook and Iranian Hackers*, http://www.f-secure.com/weblog/archives/00002228.html

[6] FOX-IT, *DigiNotar Certificate Authority breach "Operation Black Tulip"*, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[7] VASCO, *VASCO Announces Bankruptcy Filing by DigiNotar B.V.*, http://www.vasco.com/company/about_vasco/press_room/news_archive/2011/news_vasco_announces_bankruptcy_filing_by_diginotar_bv.aspx

[8] Alex Hern, *Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim*, https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

[9] *Hacking Team*, https://wikileaks.org/hackingteam/emails/

[10] George Psyllides, *Intelligence chief resigns after spy tech revelations*, http://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/

[11] *Hack Bay! A DIY Giude*, http://pastebin.com/raw/0SNSvyjJ

[12] *CARBANAK APT THE GREAT BANK ROBBERY*, Kaspersky Lab HQ, Moscow 2015, https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

[13] *APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks*, https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

[14] Serajul Quadir, *How a hacker's typo helped stop a billion dollar bank heist*, http://www.reuters.com/article/usa-fed-bangladesh-typo-idUSL4N16I4A8

[15] *Malware statistics*, AV-Test Institute, http://www.av-test.org/en/statistics/malware

Streszczenie
W artykule przedstawiono omówiono biznesowe następstwa kilku poważnych naruszeń bezpieczeństwa informacji odnotowanych w ubiegłych latach.

Słowa kluczowe: *cyberprzestępczość, cyberbezpieczeństwo, incydenty bezpieczeństwa, skutki naruszeń bezpieczeństwa*

Nota o autorze

Janusz Żmudziński – projektant i architekt rozwiązań bezpieczeństwa IT w wiodących polskich firmach informatycznych. Od wielu lat zajmuje się rozwiązaniami związanymi z bezpieczeństwem informacji. Rzeczoznawca Polskiego Towarzystwa Informatycznego. Członek Polskiego Towarzystwa Informatycznego, ISACA, ISC2, Association of Enterprise Architects.

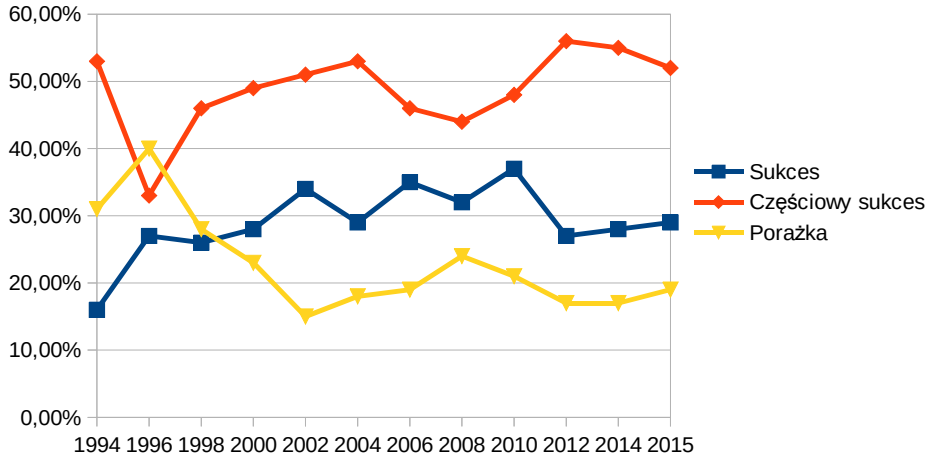
Andrzej Niemiec

Zastosowanie normy ISO/IEC 15504-5:2012 do doskonalenia procesów tworzenia oprogramowania

Ryzyka wdrażania systemów informatycznych

Publikowane od roku 1995 przez amerykańską grupę badawczą The Standish Group tzw. *Kroniki Chaosu* (*Chaos*) [1] wskazują, że część wdrożeń systemów informatycznych kończy się niepowodzeniem. Przez niepowodzenie autorzy tych raportów rozumieją znaczne przekroczenie budżetu lub czasu trwania przedsięwzięcia. W roku 1994 było ok. 31% niepowodzeń, a 52% wdrożeń miało ponad dwukrotnie przekroczony budżet lub czas. W roku 2015 niepowodzeniem skończyło się ok. 19% wdrożeń [2].

Dane te pochodzą z USA gdzie istnieje bardziej dojrzały rynek oprogramowania niż w Polsce. W naszym kraju podobne badania były prowadzone w latach 2002-2007 przez Mirosława Dyczkowskiego z Akademii Ekonomicznej we Wrocławiu i wykazały, że sukcesem kończyło się 60%-75% wdrożeń [3: 9, tab. 5]. Tak wysoki odsetek wynika jednak z przyjętych metod badawczych (innych niż stosowane przez The Standish Group) oraz z faktu, iż polski naukowiec zajął się jedynie analizą wdrażania gotowego oprogramowania (głównie klasy ERP), a w badaniach The Standish Group koncentrowano się przede wszystkim na rozwoju oprogramowania. Amerykańscy badacze za sukces uznali zrealizowanie projektu w założonym zakresie, zgodnie z budżetem i w uzgodnionym czasie. Częściowym sukcesem określono sytuację znacznego wydłużenia czasu, przekroczenie budżetu lub okrojenia funkcji. Porażka zachodziła, gdy projekt został skasowany bez uzyskania efektów.



Rys. 6. 1. Zmiany liczby porażek i sukcesów, na podstawie [4]

Poziom dojrzałości procesów softwarowych

Zarządzanie jakością tworzenia oprogramowania jest krytyczne zarówno dla aplikacji ważnych w skali kraju, jak i dla systemów, od których zależy bezpieczeństwo użytkowników (np. systemy sterowania aparaturą medyczną, oprogramowanie samochodów czy samolotów). Wymagania normy Systemy zarządzania jakością – Wymagania [5] nie oddają całej złożoności procesów związanych z tworzeniem oprogramowania. Norma ta definiuje podstawowe wymagania dla zapewnienia jakości produktu lub usługi, stanowiąc podstawę do certyfikacji zgodności systemu zarządzania z jej wymaganiami.

Jednakże dla wielu dziedzin przemysłu norma ta jest niewystarczająca. Przemysł samochodowy na całym świecie korzysta ze znacznie bardziej restrykcyjnych wymagań, opracowanych m.in. przez Niemieckie Stowarzyszenie Przemysłu Samochodowego (VDA 6.2), porozumienie Chrysler Ford GM (QS 9000) lub ich odpowiedniki. Podwyższone wymagania zostały zdefiniowane w normie ISO TS 16949 [6].

Podobnie jest w przypadku oprogramowania. Światowe firmy samochodowe żądają, aby dostawcy oprogramowania mieli wdrożone systemy zarządzania jakością zgodne z podwyższonymi wymaganiami.

Norma ISO/IEC 90003:2014 Software engineering – Guidelines for the application of ISO 9001:2008 to computer software [7] określa zasady stosowania ISO 9001 do zakupu, dostawy, opracowania, wdrożenia i utrzymania oprogramowania. Norma ta wymaga, aby system zarządzania jakością obejmował cały proces tworzenia oprogramowania, od negocjacji umowy aż do utrzymywania oprogramowania. Jako podstawę wskazuje ona normę ISO / IEC 12207:2008 [8] do zarządzania jakością tworzenia oprogramowania.

Norma Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes [9] określa zasady stosowania ISO 9001 do zakupu, dostawy, opracowanie, wdrożenie i utrzymanie systemów informatycznych. Jako podstawę wskazuję normę ISO/IEC 15288:2015 [10] do zarządzania jakością tworzenia systemów informatycznych.

Norma ISO IEC 15288:2015 Inżynieria Systemów – Procesy cyklu życia systemu [10 – *tłumaczenie tytułu normy autora, na razie (wiosna 2016 roku) nie opublikowano tej normy w języku polskim*] opisuje procesy związane z tworzeniem skomplikowanych systemów, wskazuje też na problemy związane z walidacją takich systemów. Norma określa techniczne, organizacyjne oraz umowne zasady zarządzania danym przedsięwzięciem.

Obecnie rozwój produktu programistycznego dokonuje się w wielu powiązanych przedsiębiorstwach, oprogramowanie zawiera dużo komponentów pochodzących z różnych źródeł. Często w skład oprogramowania komercyjnego wchodzą kody ze źródeł otwartych. Dostawca oprogramowania musi wziąć na siebie odpowiedzialność za wszystkie dostarczane komponenty. Dlatego dobór właściwych podwykonawców może decydować o rynkowym sukcesie lub porażce. Firmy potrzebują miarodajnych, obiektywnych kryteriów dla poprawnego wyboru dostawców. Typowe, istniejące na rynku kryteria obejmują takie obszary jak doświadczenie w produkcji oprogramowania i zaplecze techniczne, aspekty ekonomiczne, cele strategiczne, poziom dojrzałości, cena oferowanych rozwiązań, wsparcie techniczne. Po-

ziom dojrzałości jest szczególnie ważny, ponieważ od niego zależy bezpośrednio jakość oprogramowania, dostarczenie produktu w terminie i zgodnie z zaplanowanym budżetem.

Od lat 90. zeszłego wieku w USA tworzona jest tak zwana kronika chaosu. W latach 80. zaobserwowano serie błędów w oprogramowania o tragicznych konsekwencjach. Armia amerykańska wypracowała wtedy zasady tworzenia oprogramowania, ujęte później w normę ISO IEC 12207. Naturalną konsekwencją było stworzenie dla tej normy zasad oceny poziomu dojrzałości organizacji. Tak powstał model CMM (*Capabillity Maturity Model for software*), który ewaluował w CMMI (*Capabillity Maturity Model Integration*). Jest on utrzymywany przez amerykański Software Engineering Institute, działający przy Carnegie Mellon University.

Model ten opisuje pięć poziomów dojrzałości:

1) początkowy,
2) zarządzany (powtarzalny),
3) zdefiniowany,
4) zarządzany ilościowo,
5) optymalizujący.

Audytorzy i szkolenia z CMMI są nadzorowane Software Engineering Institute.

Zbliżony schemat certyfikacji poziomu dojrzałości procesów tworzenia oprogramowania w organizacji (stosowany głównie w instytucjach sektora bankowo-finansowego) wypracowano w modelach COBIT (*Control Objectives for Information and related Technology*), tworzonych przez organizację ISACA (pierwotnie skrót ten rozwijał się w nazwę Information Systems Audit and Control Association, aktualnie jest to akronim międzynarodowego stowarzyszenia osób zajmujących się zawodowo zagadnieniami dotyczącymi audytu, kontroli, bezpieczeństwa oraz innymi aspektami zarządzania systemami informatycznymi.

COBIT jest metodyką utworzoną poprzez zbiór celów kontrolnych dla technologii informacyjnych i z nimi powiązanych. Jest to zestawienie dobrych praktyk do zarządzania IT utworzone w roku 1992 przez stowarzyszenie ISACA oraz IT Governance Institute. Obecnie obowiązuje piąta edycja

tego pakietu. Metodyka COBIT służy jako pomoc w zarządzaniu, kontroli i audycie systemów informatycznych. W COBIT zarządzanie IT jest oglądane z trzech perspektyw: wymagań biznesowych, procesów zachodzących w organizacji IT, zasobów IT.

Pierwszy połączony komitet techniczny (JTC1) przy International Organization for Standardization (ISO) oraz International Electrotechnical Commission (IEC) opracował podobny do COBIT i CMMI standard oceny dojrzałości firmy programistycznej, ujęty w rodzinie norm ISO/IEC 15504 (*Software Process Improvement and Capability Determination* – SPICE) [11].

Szczegółowy opis całej rodziny norm z tej grupy wykracza poza ramy niniejszego opracowania. Dalej przedstawione zostaną jedynie wymagania normy ISO/IEC 15504-5:2012 [12].

Norma ta daje możliwość niezależnej i porównywalnej oceny poziomu dojrzałości organizacji – możliwości realizacji złożonych przedsięwzięć programistycznych. Stopień skomplikowania współczesnego oprogramowania jest bardzo wysoki. Zwykle są to systemy o wielu komponentach, działające na różnych platformach, integrujące podsystemy od licznych dostawców. Wielkość kodu współczesnego oprogramowania liczy się w setkach tysięcy, a nawet milionach linii kodu. Stworzenie go wymaga współdziałania wielu zespołów, co jest powiązane z organizacją pracy i wypracowaniem właściwych metod tworzenia oprogramowania.

Znane są różne modele tworzenia oprogramowania – od klasycznych modeli wodospadowych i przyrostowych, poprzez *extreme programming*, systemy Kanban dla oprogramowania, aż po metody zwinne (Agile, Scrum). Niezależnie od wybranej metody programowania, sensowna jest ocena poziomu dojrzałości organizacji, dopasowanie metod pracy do wymagań jakościowych właściwych dla tworzenia zaawansowanych aplikacji.

Norma [12] ma na celu doskonalenie procesów związanych z tworzeniem oprogramowania, szczególnie w dziedzinach, w których jakość i niezawodność mają krytyczne znaczenie. Jest obowiązującym standardem na przykład w przemyśle lotniczym i samochodowym, znajduje zastosowanie także w firmach tworzących oprogramowanie medyczne.

Norma definiuje pięć poziomów dojrzałości firmy. Na poziomie I procesy tworzenia oprogramowania są realizowane bez formalnego podejścia. Na poziomie II (ang. *managed*) procesy są zarządzane biernie i zorientowane na rozwiązywanie problemów. Poziom III (ang. *established*) charakteryzuje systematyczne podejście, oparte o zdefiniowane procesy. Poziom IV (ang. *predictable*) określa stałe doskonalenie i stosowanie pomiarów do osiągania celów. Poziom V (*optimising*) stosowany jest przez najlepsze organizacje światowe o wysokiej innowacyjności.

Omawiana norma odwołuje się do dwóch zbliżonych norm: ISO/IEC 12207:2008 [8] oraz ISO/IEC 15288 [10], zatytułowanych identycznie: Systems and software engineering – System life cycle processes. Definiują one procesy związane z tworzeniem oprogramowania lub systemu (rozumianego jako połączenie oprogramowania, sprzętu, procedur, przepisów itp.).

Norma [12] wyróżnia się tym, że pozwala na osobną ocenę poziomu każdego procesu wchodzącego w cykl życia oprogramowania lub systemu: grup procesów organizacyjnych, technicznych, uzgodnień, zarządzania przedsięwzięciem (ang. *project management*) i tworzenia oprogramowania. Wszystkie te procesy mogą osiągać różne poziomy dojrzałości.

Model dojrzałości zdefiniowany w rozważanej normie zakłada pięć następujących poziomów, podobnych do zdefiniowanych w wytycznych PN-EN ISO 9004:2010 [13], co pokazano w tabeli 6. 1.

Tabela 6. 1. 1 Poziomy dojrzałości organizacji wg [12; 13]

Poziom	ISO/IEC 15504-5:2012	PN-EN ISO 9004:2010, załącznik A.2
0	Nie zdefiniowany (*incomplete*)	Brak odpowiednika
I	Początkowy (*performed*)	Brak formalnego podejścia
II	Powtarzalny (*managed*)	Podejście bierne
III	Ustanowiony (*established*)	Stabilne podejście systemów
IV	Zarządzany ilościowo (*predictible*)	Nacisk na ciągłe doskonalenie
V	Optymalizujący (*optimizing*)	Najlepsze osiągnięcia w danej klasie

Wdrożenie poziomu początkowego nie daje gwarancji sukcesu. Tu zarządzanie jest niestabilne, nie ma zdefiniowanych procesów, tworzenie oprogramowania odbywa się bez planów. Wyniki procesów są osiągane, ale nie ma gwarancji jakości wyników.

Poziom powtarzalny wymaga, aby wydajność procesów była nadzorowana (planowana, monitorowana i dopasowywana). Niezbędne jest na nim określenie odpowiedzialności i uprawnień w procesach oraz zapewnienie jakości i zarządzania konfiguracją. Jest on podstawą do dalszego doskonalenia.

Poziom trzeci – ustanowiony – wymaga opracowania standardowych procedur, przestrzegania ich w całej organizacji, we wszystkich przedsięwzięciach. Przyjęto, że odpowiada on sytuacji, gdy firma jest w stanie zagwarantować parametry jakościowe realizowanych produktów.

Dobrze wdrożony i utrzymywany system zarządzania jakością odpowiada poziomowi trzeciemu. Przykładowo, dla dostawców oprogramowania dla niemieckiego przemysłu samochodowego przyjęto, że dostawca na drugim poziomie dojrzałości nie jest w stanie realizować samodzielnie zlecenia i wymaga opieki ze strony odbiorcy. Według norm niemieckiego przemysłu samochodowego, dostawca z poziomem trzecim dojrzałości jest w stanie samodzielnie realizować oprogramowanie wykorzystywane w samochodach.

Poziom czwarty i piąty są dostępne jedynie dla niewielu najlepszych firm na świecie.

Na tworzenie oprogramowania mają wpływ różne procesy w organizacji: zarządzania przedsięwzięciem, sposób dokonywania uzgodnień z Klientem, sprawy związane z wymaganiami, zarządzanie konfiguracją, sposoby zarządzania wiedzą, jakością, kodowaniem, integracją i testowaniem. Każdy z nich oceniany jest niezależnie. Osiąganie każdego wyższego poziomu dojrzałości oprogramowania wymaga spełnienia wymagań dla podstawowych procesów zdefiniowanych dla danego poziomu dojrzałości (procesy generyczne).

Autor zna wiele firm programistycznych, w których wdrożono system zarządzania jakością zgodny z wymaganiami ISO 9001:2009 [5]. Natomiast

– zgodnie z wiedzą autora – żadna polska firma nie skorzystała się z normy PN ISO/IEC 90003:2007 Inżynieria oprogramowania – Wytyczne stosowania ISO 9001:2000 do oprogramowania komputerów [7].

Norma [5] jednakże zawiera w rozdziale 4 wytyczną:

„4.1 (…) b) Sekwencja i interakcja procesów:

Organizacja powinna określić sekwencje tych procesów i ich interakcje w:

1) modelach cyklu życia dla wytwarzania oprogramowania (…) i

2) planowaniu jakości wytwarzania, które powinno być oparte na modelu cyklu życia.

UWAGA

Dalsze informacje patrz następujące normy: ISO IEC 12207 Inżynieria oprogramowania – Procesy cyklu życia oprogramowania" [5] .

Podobne wytyczne zawiera norma ISO/IEC TR 90005:2008 Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes (Inżynieria systemów – Wytyczne stosowania ISO 9001:2000 do procesów cyklu życia systemu) [9], z tym że odnosi do procesów zdefiniowanych w normie ISO/IEC 15288 [10].

Dla procesów zdefiniowanych w obu normach można oceniać ich dojrzałość, korzystając z wytycznych w normie [12].

Korzyści dla producentów oprogramowania

Polski Holding Obronny (PHO) zatrudnia ok 14 tys. osób i w roku 2014 wygenerował przychody w granicach ok. 8 mld zł [14]. W firmie tej tworzone jest m.in. oprogramowanie o bardzo wysokich wymaganiach dotyczących jakości. Wydaje się naturalne wdrożenie w przedsiębiorstwach wchodzących w skład holdingu metodycznego doskonalenia procesów tworzenia oprogramowania.

Poza firmami wchodzącymi w skład PHO, potencjalnie zainteresowane doskonaleniem powinny być banki, instytucje tworzące oprogramowanie dla sektora państwowego oraz państwowe agendy tworzące oprogramowanie.

Wdrożenie ISO IEC 15504 może przynieść następujące korzyści:

- większą pewność realizacji ekonomicznych interesów firmy;

- możliwość zarządzania konfiguracją i zmianami;
- zapewnienie odpowiedniej jakości oprogramowania;
- istotne zmniejszenie liczby błędów w produkcie oddanym do użytkowania;
- lepsze planowanie i oszacowania;
- zmniejszenie kosztów produkcji i utrzymywania oprogramowania;
- możliwość planowania ponownego wykorzystania zasobów wiedzy i doświadczenia;
- przewidywalną wydajność organizacji w produkcji oprogramowania;
- poprawę wydajności pracy;
- lepsze testowanie produktów;
- liczne korzyści dla zamawiającego.

Zlecający wykonanie oprogramowania w firmie posiadającej trzeci poziom dojrzałości może być pewniejszy uzyskania zamówionego produktu w ustalonym czasie, cenie i spełniającego wymagania jakościowe.

Oczywiście wdrożenie trzeciego poziomu dojrzałości nie jest od razu gwarancją sukcesu, ale umożliwia większą pewność osiągnięcia założonych celów przedsięwzięcia. Niemieckie koncerny samochodowe przyjęły, że dostawca oprogramowania musi mieć trzeci poziom doskonałości, aby samodzielnie realizować oprogramowanie do samochodów.

Zamawiający oprogramowanie w firmie z wdrożonym systemem zarządzania jakością zgodnym z ISO/IEC 15504 może uzyskać:

- wyższe zaufanie do oprogramowania, co oznacza mniejszą liczbę błędów;
- dostawę oprogramowania na czas i w uzgodnionym budżecie;
- spełnienie wymagań umowy;
- lepsze reagowanie na zamiany wymagań;
- wyższe zaufanie do oszacowania czasu i wartości kontraktu;
- wczesne wykrywanie anomalii i błędów.

Oferta Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego

Izba Rzeczoznawców Polskiego Towarzystwa Informatycznego posiada grupę ośmiu certyfikowanych asesorów normy ISO/IEC 15504-5. Egzamin audytorski odbył się pod nadzorem ECQA. Izba oferuje następujące usługi:

- szkolenia z ISO/IEC 12207 i ISO IEC 15288;
- wdrożenia ISO/IEC 15504-5 na poziomach 2 i 3;
- ocenę poziomu dojrzałości oprogramowania bez akredytacji;
- ocenę poziomu dojrzałości oprogramowania z akredytacją – z udziałem kompetentnego lub głównego asesora;
- szkolenia dla działów obsługujących zamówienia (w tym publiczne) z zakresu oprogramowania.

Przedsięwzięcia w administracji państwowej

Analiza licznych przykładów nieudanych wdrożeń systemów zamawianych przez administrację państwową wskazuje, że posiadanie certyfikatu ISO 9001 nie jest wystarczającą gwarancją sukcesu skomplikowanego przedsięwzięcia programistycznego. Wprawdzie większość firm realizujących kontrakty rządowe posiadała takie certyfikaty, jednakże zdarzało się, że kontrakty były realizowane przez firmy zatrudniające ludzi o znikomym doświadczeniu.

Unowocześnienie procesów tworzenia oprogramowania poprzez wdrażanie innowacji technologicznych – takich jak poziomy dojrzałości firm w tworzeniu oprogramowania – może korzystnie wpłynąć na jakość systemów zamawianych przez administrację.

Zdaniem autora nie jest konieczne, by firmy biorące udział w przetargu dla administracji posiadały formalny certyfikat – wystarczy deklaracja firmy, iż wdrożyła dobre praktyki opisane w ISO IEC 15504 [12] lub w modelu równoważnym – np. COBIT lub CMMI.

Warto również wdrożyć dobre praktyki z poziomu trzeciego w agendach rządowych tworzących oprogramowanie i podległych różnym resortom, ze

szczególnym uwzględnieniem jakości i bezpieczeństwa w procesach tworzenia oprogramowania.

Bezpieczeństwo

Jakość kodu jest związana w dużej mierze z bezpieczeństwem informacji. Na jakość kodu źródłowego składają się jednak liczne procesy. Twórcy oprogramowania powinni zdawać sobie sprawę i odpowiednio udokumentować granice stosowalności i odporności oprogramowania. Dojrzałość procesów ma bezpośredni wpływ na aspekty bezpieczeństwa tworzonego oprogramowania. Norma ISO/IEC 15504-5:2012 definiuje następujące grupy procesów:

- procesy zarządzania przedsiębiorstwem (w tym zarządzanie zasobami ludzkimi i zarządzanie przedsięwzięciem),
- procesy cyklu życia oprogramowania oraz procesy wspomagające (m.in. szkolenia i zarządzanie wiedzą, zarządzanie informacją i zapewnienie jakości) [13].

Dojrzałość każdego z tych procesów ma bezpośredni związek z odpornością kodu źródłowego na podatności i ataki. Sprzyja temu wdrożenie praktyk opisanych w rozpatrywanej normie.

Literatura

[1] *Chaos*, The Standish Group, https://www.standishgroup.com/

[2] Steve Dean, *2015 Chaos Report on Software Development*, https://www.linkedin.com/pulse/2015-chaos-report-software-development-steve-dean

[3] Mirosław Dyczkowski, *Ocena przebiegu i efektów przedsięwzięć informatycznych*, w: „Systemy wspomagania organizacji SWO 2007", http://www.swo.ae.katowice.pl/_pdf/305.pdf

[4] Shane Hastie, Stéphane Wojewoda, *Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch*, http://www.infoq.com/articles/standish-chaos-2015

[5] Norma Systemy zarządzania jakością – Wymagania, PN-EN ISO 9001:2009
[6] Norma Zarządzanie Jakością w Przemyśle Motoryzacyjnym, ISO/TS 16949
[7] Norma oftware engineering -- Guidelines for the application of ISO 9001:2008 to computer software, ISO/IEC 90003:2014
[8] Systems and software engineering — Software life cycle processes, ISO/IEC 12207:2008
[9] Norma Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes, ISO/IEC 90005:2008
[10] Norma Systems and software engineering – System life cycle processes, ISO/IEC/IEEE 15288:2015
[11] Norma Systems and software engineering –System life cycle processes, ISO/IEC/IEEE 15288:2015
[12] Rodzina norm: Information technology – Process assessment, nazywana też Software Process Improvement and Capability Determination (SPICE), ISO/IEC 15504
[13] Norma Information technology — Process assessment — Part 5: An exemplar software life cycle process assessment model, ISO/IEC 15504-5:2012
[14] Norma Zarządzanie ukierunkowane na trwały sukces organizacji – Podejście wykorzystujące zarządzanie jakością, PN-EN ISO 9004:2010
[15] Strona internetowa Polskiego Holdingu Obronnego, zakładka *O nas*, http://www.pho.pl/o-nas/

Streszczenie

W artykule przestawiono korzyści z doskonalenia procesów tworzenia oprogramowania dla twórców oprogramowania i dla potencjalnych odbiorców.

Słowa kluczowe: *Jakość oprogramowania, SPICE, ISO/IEC 15504, ISO/IEC 15288, ISO/IEC 12207, bezpieczeństwo, cykl życia oprogramowania*

Nota o autorze

Andrzej Niemiec – dr nauk technicznych, członek oddział dolnośląskiego Polskiego Towarzystwa Informatycznego, rzeczoznawca Polskiego Towarzystwa Informatycznego, audytor ISO/IEC 15504, ISO/IEC 27001, ISO 9001.

Polskie Towarzystwo Informatyczne (PTI) zostało założone w roku 1981. Stowarzyszenie zrzesza zarówno osoby posiadające wysokie kompetencje i doświadczenie w zakresie informatyki, studentów ostatnich lat kierunków informatycznych, jak i specjalistów innych dziedzin intensywnie wykorzystujących technologie informatyczne.

Polskie Towarzystwo Informatyczne należy do Europejskiej Rady Stowarzyszeń Informatycznych CEPIS (Council of European Professional Informatics Societies). Stowarzysza informatyków zatrudnionych w administracji publicznej, środowiskach akademickich i biznesowych.

Podstawowe cele **Polskiego Towarzystwa Informatycznego**:

- wspieranie działalności naukowej i naukowo-technicznej we wszystkich dziedzinach informatyki i doskonalenia metod jej efektywnego wykorzystania w gospodarce narodowej,
- popularyzacja zagadnień i zastosowań informatyki w społeczeństwie,
- ułatwianie wymiany informacji w środowisku zawodowym,
- podnoszenie poziomu kwalifikacji i etyki zawodowej informatyków,
- reprezentowanie członków Towarzystwa, ich opinii, potrzeb, interesów i uprawnień wobec społeczeństwa, władz oraz instytucji w kraju i za granicą.

IZBA RZECZOZNAWCÓW Polskiego Towarzystwa Informatycznego

Działająca przy Polskim Towarzystwie Informatycznym **Izba Rzeczoznawców PTI** wspiera klientów profesjonalną wiedzą oraz doświadczeniem zrzeszonych w Polskim Towarzystwie Informatycznym przedstawicieli zawodowego i naukowego polskiego środowiska teleinformatycznego.

Izba Rzeczoznawców PTI świadczy usługi na rzecz podmiotów państwowych, samorządowych, organizacji publicznych, firm komercyjnych oraz osób fizycznych w sytuacjach, gdy odwołanie się do opinii niezależnego i obiektywnego autorytetu:

- podnosi szanse powodzenia zaplanowanego przedsięwzięcia informatycznego,
- jest niezbędne do zapewnienia przejrzystości wyboru,
- służy bezstronnemu rozstrzygnięciu dylematów wynikających z realizacji przedsięwzięcia.

Ekspertyzy Izby Rzeczoznawców PTI realizowane są przez zespoły specjalistów z wieloletnim doświadczeniem w branży IT. Ich kwalifikacje potwierdzone są akredytacjami i certyfikacjami zarówno niezależnych organizacji takich jak The Open Group (TOGAF), ISC2 (certyfikaty CISSP), ISACA (certyfikaty CISA, CRISC, CISM), CCTE (certyfikaty PRINCE2), PMI jak i czołowych krajowych i międzynarodowych producentów sprzętu i oprogramowania.

W obszarze zarządzania bezpieczeństwem informacji wśród naszych ekspertów znajdują się osoby posiadające kwalifikacje w zakresie prowadzenia testów penetracyjnych, certyfikaty Certified Ethical Hacker (CEH) wydane przez EEC-Council, certyfikaty audytorów wiodących systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC.

Izba Rzeczoznawców PTI oferuje doradztwo w zakresie zarządzania usługami informatycznymi, bezpieczeństwem informacji i ryzykiem teleinformatycznym.

Prace projektowe realizowane przez ekspertów **Izby Rzeczoznawców PTI** są oparte na powszechnie uznanych metodykach zarządzania.

Kluczowe obszary prac realizowanych przez **Izbę Rzeczoznawców PTI** to:

- opracowywanie strategii i koncepcji informatyzacji,
- wykonywanie ekspertyz i opinii,
- przeprowadzanie audytów, w tym audytów bezpieczeństwa systemów informatycznych,
- wsparcie merytoryczne przy przygotowywaniu SIWZ oraz przy prowadzeniu procesu przetargowego,
- wsparcie i udział w komitetach sterujących projektów informatycznych,
- badanie, analiza i ocena projektów informatycznych oraz systemów i rozwiązań informatycznych,
- pełnienie obowiązków biegłego instytucjonalnego.

Gwarancją ochrony interesów klientów **Izby Rzeczoznawców PTI** są:

- niezależność i obiektywizm rzeczoznawcy,
- rzetelność treści odniesiona do aktualnej wiedzy i najlepszych praktyk zawodowych,
- zachowanie poufności wszelkich otrzymanych informacji,
- recenzja wewnętrzna wytwarzanych opracowań.

Siłą **Izby Rzeczoznawców** są profesjonalni, bezstronni, obiektywni i niezależni eksperci oraz wysoka jakość świadczonych przez nich usług.

Oferta Izby Rzeczoznawców PTI w zakresie normy ISO/IEC 15504:2012

Analiza licznych przykładów nieudanych wdrożeń systemów informatycznych zamawianych przez instytucje publiczne wskazuje, że posiadanie certyfikatu ISO 9001 nie jest wystarczającą gwarancją sukcesu skomplikowanego przedsięwzięcia programistycznego. Większość firm realizujących kontrakty rządowe posiadała takie certyfikaty. Wymagania normy ISO 9001 „Systemy zarządzania jakością – Wymagania" nie oddają całej złożoności procesów związanych z tworzeniem oprogramowania.

Dojrzałość procesów wytwórczych ma bezpośredni wpływ na aspekty bezpieczeństwa tworzonego oprogramowania. Norma ISO/IEC 15504:2012 definiuje następujące grupy procesów: procesy zarządzania przedsiębiorstwem, procesy cyklu życia oprogramowania oraz procesy wspomagające. Dojrzałość każdego z tych procesów ma bezpośredni związek z odpornością kodu źródłowego na podatności i ataki. Sprzyja temu wdrożenie praktyk opisanych w normie ISO/IEC 15504.

Celowym jest zatem, aby firmy biorące udział w przetargach dla instytucji publicznych deklarowały wdrożenie dobrych praktyk opisanych w ISO/IEC 15504:2012 (SPICE) lub w innych modelach – np. COBIT 5 Foundation lub CMMI.

Izba Rzeczoznawców PTI
posiada certyfikowanych asesorów normy ISO/IEC 15504-5.

Izba Rzeczoznawców PTI oferuje:

- szkolenia z ISO/IEC 12207 i ISO / IEC 15288,
- wdrożenia ISO/IEC 15504-5 na poziomach 2 i 3,
- ocenę poziomu dojrzałości oprogramowania bez akredytacji,
- ocenę poziomu dojrzałości oprogramowania z akredytacją – z udziałem kompetentnego lub głównego asesora,
- szkolenia dla działów obsługujących zamówienia (w tym publiczne) z zakresu oprogramowania.

Oferta Izby Rzeczoznawców PTI w zakresie badań na zgodność z KRI / WCAG 2.0

W maju 2015 roku zaczęły obowiązywać przepisy Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie **Krajowych Ram Interoperacyjności (KRI)**, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych odnoszące się do dostępności portali informatycznych administracji publicznej.

Wspomniane rozporządzenie nakazuje między innymi dostosowanie wszystkich systemów teleinformatycznych, służących prezentacji zasobów informacji a eksploatowanych przez podmioty realizujące zadania publiczne do wymagań **WCAG 2.0** (Web Content Accessibility Guidelines) na poziomie nie mniejszym niż AA. **WCAG 2.0** zawiera 4 zasady oraz 12 przypisanych im wytycznych, które z kolei zawierają łącznie 61 podpunktów. Większość, tj. 39 z nich, dotyczy poziomu A lub AA, muszą więc być spełnione przez system, aby mógł być określony jako zgodny z odpowiednim przepisem KRI.

Instytucje publiczne nie mają zazwyczaj odpowiednich kompetencji, aby wykonać samodzielnie pełny audyt swoich systemów. Zakup i wdrożenie gotowego CMS-u, reklamowanego jako zgodnego z przepisami prawa nie rozwiązuje problemów. **Należy rozważyć możliwość przeprowadzania okresowego audytu przez niezależne organizacje.** Organizacją taką może być działająca przy Polskim Towarzystwie Informatycznym **Izba Rzeczoznawców PTI**.

Izba Rzeczoznawców PTI oferuje podmiotom realizującym zadania publiczne przeprowadzenie kontroli zgodności systemów informatycznych z przepisami rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI).

W ramach kontroli prowadzimy audyt na zgodność z normami PN-ISO/IEC 20000 oraz PN-ISO/IEC 27001 lub przepisami rozdziału 3 KRI „Minimalne wymagania dla systemów teleinformatycznych”.

Kontrolujemy poprawność dokumentacji:

- Polityka bezpieczeństwa danych osobowych i zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych,
- Analiza ryzyka,
- Polityka informatyzacji,
- Procedury zarządzania aktywami teleinformatycznymi,
- Procedury zarządzania ciągłością działania.

Dotychczas w serii
Biblioteczka Izby Rzeczoznawców PTI
nakładem Polskiego Towarzystwa Informatycznego
ukazały się następujące publikacje:

tom 1
Maciej SZMIT
Wybrane zagadnienia opiniowania sądowo-informatycznego
wydanie drugie, rozszerzone i poprawione 2014

tom 2
Przemysław JATKIEWICZ
Ochrona danych osobowych. Teoria i praktyka
2015

tom 3
Przemysław JATKIEWICZ
Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego. Raport z badań
2016

Polskie Towarzystwo Informatyczne (PTI) zostało założone w 1981 roku. Stowarzyszenie zrzesza zarówno osoby posiadające wysokie kompetencje i doświadczenie w zakresie informatyki, studentów ostatnich lat kierunków informatycznych, jak i specjalistów innych dziedzin intensywnie wykorzystujących technologie informatyczne.

Działająca przy Polskim Towarzystwie Informatycznym **Izba Rzeczoznawców PTI** wspiera klientów profesjonalną wiedzą oraz doświadczeniem zrzeszonych w Polskim Towarzystwie Informatycznym przedstawicieli zawodowego i naukowego polskiego środowiska teleinformatycznego.

Izba Rzeczoznawców PTI oferuje doradztwo w zakresie zarządzania usługami informatycznymi, bezpieczeństwem informacji i ryzykiem teleinformatycznym.

Kluczowe obszary prac realizowanych przez **Izbę Rzeczoznawców PTI** to:

- opracowywanie strategii i koncepcji informatyzacji,
- wykonywanie ekspertyz i opinii,
- przeprowadzanie audytów, w tym audytów bezpieczeństwa systemów informatycznych,
- wsparcie merytoryczne przy przygotowywaniu SIWZ oraz przy prowadzeniu procesu przetargowego,
- wsparcie i udział w komitetach sterujących projektów informatycznych,
- badanie, analiza i ocena projektów informatycznych oraz systemów i rozwiązań informatycznych,
- pełnienie obowiązków biegłego instytucjonalnego.

978 – 83 – 60810 – 85 – 9

35 lat PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Polskie Towarzystwo Informatyczne
Izba Rzeczoznawców
www.pti.org.pl