Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

Adam Mizerski

ISACA Katowice Chapter
Getin Noble Bank S.A.
adam@mizerski.net.pl

ZGODNE Z RODO ZARZĄDZANIE BEZPIECZEŃSTWEM OPARTE NA RYZYKU

Streszczenie: Od 25 maja 2018 r. wymagania w zakresie zastosowanych środków bezpieczeństwa w systemach informatycznych przetwarzających dane osobowe powinny być uzależnione od rzetelnie przeprowadzonej analizy ryzyk. Risk Based Approach oznacza, że regulator nie narzuca ściśle określonych środków i procedur w zakresie bezpieczeństwa, obliguje jednak do samodzielnego przeprowadzania analizy prowadzonych procesów przetwarzania danych i dokonywania samodzielnej oceny ryzyka. W tym kontekście celem artykułu jest przedstawienie oceny aktualnego stanu przygotowania organizacji do procesu szacowania ryzyk na podstawie sektora finansowego, jak również jednostek samorządu terytorialnego oraz prezentacja metody szacowania ryzyka dla organizacji, które zmuszone będą zmierzyć się z tematyką ochrony danych osobowych i zarządzania bezpieczeństwem na podstawie oceny ryzyka.

Słowa kluczowe: RODO, bezpieczeństwo informacji, zarządzanie ryzykiem technologicznym, ochrona danych osobowych.

JEL Classification: M15.

Wprowadzenie

Wprowadzone Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; GDPR/RODO) diametralnie zmieniło wymogi w zakresie bezpieczeństwa systemów informatycznych przetwarzających dane osobowe. Ilustracją tych zmian jest między innymi fakt, że od 25 maja 2018 r. (data, po której nastąpi egzekwowanie zasad zdefiniowanych w GDPR/RODO) m.in.

przestanie obowiązywać wymóg dotyczący zastosowania środków bezpieczeństwa na poziomie wysokim systemów informatycznych, służący do przetwarzania danych osobowych, zdefiniowany w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wspomniany wymóg dotyczy minimalnej długości hasła do systemu informatycznego połączonego z Internetem oraz przetwarzającego dane osobowe na poziomie minimum 8 znaków zawierających małe i wielkie litery oraz cyfry lub znaki specjalne. Dla każdego specjalisty ds. bezpieczeństwa jest jasne, że zabezpieczenie to jest co najmniej nieadekwatne do współczesnych zagrożeń, jednakże brak takiego zapisu wprost u wielu administratorów danych zapewne zrodzi pytanie: jak powinno wyglądać hasło po 25 maja 2018 r. – konieczne będą dwudziestopięcioznakowe hasła w postaci „AFBDHr4ExxNV48o9Q84xJAaxa", czy może wystarczy najczęściej stosowana kombinacja „123456", jak wynika z analizy *Hasła ponad 10 milionów polskich kont email dostępne do pobrania w sieci*[1]? Odpowiedzią, choć wprawdzie nie wprost, jest koncepcja zarządzania bezpieczeństwem w postaci Risk Based Approach, która sprowadza się do uzależnienia zakresu obowiązków nałożonych na administratora danych od specyfiki przetwarzania danych w organizacji tego administratora oraz od ryzyka, jakie może wiązać się z ewentualnym naruszeniem bezpieczeństwa danych.

Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w celu zachowania bezpieczeństwa i zapobiegania niewłaściwemu przetwarzaniu informacji, konieczne jest oszacowanie ryzyka przetwarzania oraz trzeba wdrożyć środki ograniczające ryzyko. By sprostać temu wyzwaniu, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych oraz dotyczące zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych [Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.].

Zdaniem części specjalistów zajmujących się bezpieczeństwem przetwarzania danych osobowych powyższy zapis GDPR/RODO wiąże się z nałożeniem na administratorów danych zadania wstępnej analizy ryzyka. Ze względu na złożoność zadania jego wykonanie wymaga specjalistycznej wiedzy i wsparcia specjalistów[2].

---

[1] Hasła ponad 10 milionów polskich kont email dostępne do pobrania w sieci [www 1] .

[2] Podejście oparte na ryzyku, czyli Risk Based Approach [www 2] .

1. Zarządzanie ryzykiem w sektorze finansowym oraz administracji publicznej

Analizując treść GDPR/RODO, należy podkreślić istotność właściwego szacowania ryzyka naruszenia praw i wolności, których dane są przetwarzane. Kwestia ryzyk poruszona jest w wielu motywach preambuły RODO (np. motywie 76, 77, 84, 86, 89) oraz przepisach (np. art. 30, 34, 35, 36). W motywie 76, 77 i 83 użyto również określeń związanych z „minimalizowaniem" i „szacowaniem" ryzyka („ryzyko należy oszacować na podstawie obiektywnej oceny", „najlepsze praktyki pozwalające zminimalizować ryzyko", „administrator i podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko"), co oznacza, że ryzyko jest pewnego rodzaju miarą wspomnianego naruszenia praw i wolności osób fizycznych.

Teoretycznie zarządzenie bezpieczeństwem oparte na ryzyku dla sporej części polskich organizacji nie powinno stanowić problemu, gdyż koncepcja ta jest od dawna zakorzeniona w krajowych regulacjach:

I. Dla sektora finansowego i ubezpieczeniowego – od stycznia 2013 r. w postaci Rekomendacji D Komisji Nadzoru Finansowego dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, w której napisano wprost, że: „Niniejsza Rekomendacja ma na celu wskazanie bankom oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami" oraz „Rekomendacja powinna być traktowana jako uzupełnienie »Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach« w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego), ale również m.in. z ryzykiem utraty reputacji i ryzykiem strategicznym", a przede wszystkim w zakresie rekomendacji nr 5 „Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach" [Rekomendacja D Komisji Nadzoru Finansowego, 2013].
II. Dla sektora publicznego:
   a) od grudnia 2012 r. w ramach Kontroli Zarządczej na podstawie Komunikatu nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie plano-

wania i zarządzania ryzykiem [Komunikat Nr 6 Ministra Finansów z dnia 6 grudnia 2012 r.]. Zarządzanie ryzykiem wynikające z Kontroli Zarządczej opiera się na jednej z uznanych metodyk kompleksowego zarządzania ryzykiem organizacji, jakim jest dokument przygotowany przez Komitet Organizacji Sponsorujących Komisję Treadwaya (COSO) [COSO, 2004].

b) od kwietnia 2012 w ramach Rozporządzenia 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. z 2012 r., poz. 526.

O ile w sektorze finansowym – zarówno w efekcie dostosowania się Banków i instytucji finansowych do rekomendacji D, jak również w wyniku intensywnych kontroli inspektorów KNF – zarządzanie bezpieczeństwem systemów informatycznych jest standardem, o tyle z autopsji autora posiadającego doświadczenie zawodowe w sektorze publicznym, a także bankowym wynika, że sektor publiczny, pomimo regulacji obligujących go od 2012 r. do stosowania analizy ryzyk jako podstawy zarządzania bezpieczeństwem, ma przed sobą jeszcze wiele wyzwań związanych z Risk Based Approach.

Subiektywną negatywną ocenę stanu zarządzania ryzykiem w jednostkach administracji publicznej pogłębia analiza danych pozyskanych w ramach grantu badawczego sfinansowanego przez Polskie Towarzystwo Informatyczne (PTI) zrealizowanego pod kierownictwem dr inż. Przemysława Jatkiewicza „Stan wdrożenia wybranych wymagań Krajowych Ram Interoperacyjności w serwisach samorządowych" [Jatkiewicz, 2016]. Badanie przeprowadzono w 2015 r. i objęto nim 339 jednostek samorządu terytorialnego (183 Urzędów Gmin, 70 Urzędów Miast i Gmin, 38 Urzędów Miejskich, 36 Urzędów Powiatowych, 2 Urzędy Dzielnicy [Warszawa], 8 Urzędów Miejskich w mieście na prawach powiatu oraz 2 Urzędu Marszałkowskie). Z wyników przeprowadzonego badania obejmującego m.in. pytania dotyczące zastosowanej analizy ryzyka wynika, że „[…] niewiele instytucji opracowało analizę ryzyka. Z deklaracji wynika, że zrobiło to 81 jednostki (23,89%)" oraz „Jedynie 61 analiz można uznać za aktualne" [Jatkiewicz, 2016]. Czarny obraz nie stosowania analizy ryzyk w jednostkach administracji publicznej najlepiej obrazuje fakt, że respondenci nie znają metod zarządzania ryzykiem i proponują w tym zakresie stosowanie metod zorientowanych na inne problemy. Respondenci podali, że znają następujące metody:

– burza mózgów,
– FMEA,

- Prince 2,
- arytmetyczna,
- CMMI for Services v. 1.3,
- PMI,
- CRAMM,
- delficka,
- indukcyjna,
- MEHARI,
- ręczna.

Wymienione metody skuteczne są dla zarządzania projektami i wspomagają prace badawcze. Respondenci przyznali, że mimo braku wiedzy odnośnie do analizy i oceny ryzyka nie korzystają z pomocy doradczych jednostek zewnętrznych, a niejednokrotnie prowadzona przez nich analiza ryzyka nie była poprzedzona inwentaryzacją aktywów teleinformatycznych [Jatkiewicz, 2016].

Warto w tym miejscu podkreślić konsekwencje nieadekwatnego oszacowania ryzyk lub zastosowania mechanizmów, które nie zmniejszą zidentyfikowanych ryzyk, co w efekcie doprowadzi do urzeczywistnienia ryzyka w postaci incydentu bezpieczeństwa, czego efektem będzie naruszenie praw osób, których dane są przetwarzane. W takiej sytuacji jednostka biznesowa powinna zwrócić baczną uwagę na te konsekwencje, albowiem Regulacje GDPR/RODO w artykule 83. odnoszącym się do ogólnych warunków nakładania administracyjnych kar pieniężnych określają, że naruszenia przepisów podlegają karze pieniężnej w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, choć zastosowanie może mieć kwota znacznie wyższa [Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.].

2. Szacowanie ryzyk technologicznych

Nasuwa się zatem pytanie, jak oszacować ryzyka związane z przetwarzaniem danych osobowych przez systemy teleinformatyczne? Podstawą jest inwentaryzacja zasobów teleinformatycznych, tj. przeprowadzenie analizy procesów biznesowych organizacji oraz zidentyfikowanie wszystkich systemów, które przetwarzają dane osobowe ze wskazaniem interfejsów wejścia i wyjścia danych z każdego systemu. Dopiero po przeprowadzeniu takiej analizy i zinwentaryzowaniu wszystkich aktywów teleinformatycznych przetwarzających dane osobowe w organizacji możliwe jest przejście do następnego kroku – analizy ryzyk.

W Rozporządzeniu GDPR/RODO nie została wskazana konkretna, jedna metodyka przeprowadzania szacowania ryzyka lub procesu zarządzania ryzykiem. Próbując zmierzyć się z wyzwaniem stworzenia systemu zarządzania ryzykiem technologicznym, warto w pierwszej kolejności zajrzeć do norm:

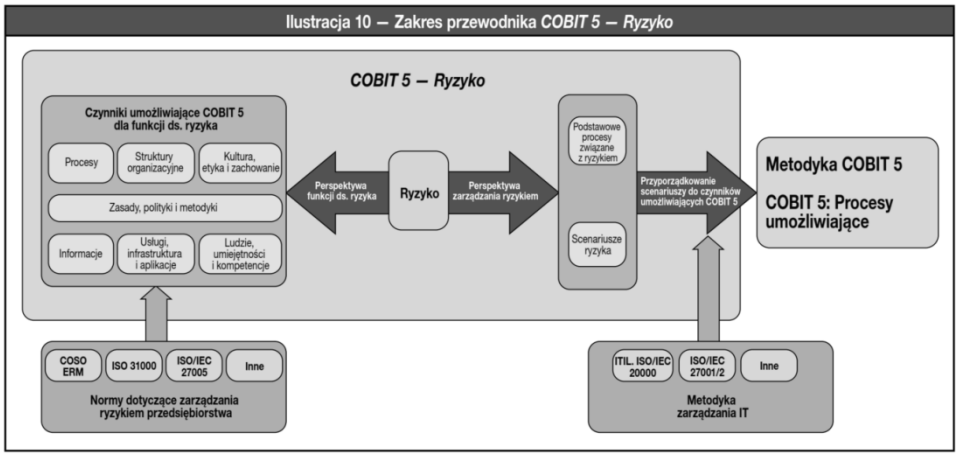
a) PN-ISO/IEC 31000 (wersja polska) – Zarządzanie ryzykiem – Zasady i wytyczne,
b) PN-ISO/IEC 27005:2014-01 (wersja polska) – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

Normy jednak ze względu na swą uniwersalność, a co za tym idzie, pewną ogólność, wśród osób rozpoczynających przygodę z ryzykiem wywołują pewien niedosyt. Tu z pomocą może przyjść mniej znany, ale niezwykle praktyczny podręcznik *COBIT 5 for Risk* [ISACA, br.], który również został przetłumaczony na język polski. Wspomniane opracowanie to 250-stronicowe kompendium wiedzy z zakresu zarządzania ryzykiem, zawierające wytyczne dotyczące sposobu zarządzania ryzykiem, obejmujące zbiór mierników, np.:

a) odsetek projektów niezrealizowanych w wyznaczonym terminie lub przekraczających założony budżet,
b) liczbę i rodzaj odstępstw od planu infrastruktury technicznej,
c) liczbę incydentów spowodowanych przez niewystarczającą dokumentację techniczną oraz niedostateczne szkolenia.

Opracowanie *COBIT 5 for Risk* definiuje wytyczne w zakresie ustanowienia ról i odpowiedzialności w procesie zarządzania ryzykiem.

Modele zarządzania ryzykiem zgodnie z PN-ISO/IEC 27005:2014-01 oraz *COBIT 5 for Risk* są komplementarne, przy czym *COBIT…* zawiera bardziej rozbudowane wytyczne i obejmuje obszary pominięte w normie PN-ISO/IEC, np. nadzór nad ryzykiem i reagowanie na zdarzenia. PN-ISO/IEC 27005:2014-01 definiuje ryzyko naruszenia bezpieczeństwa informacji jako: „możliwość, że zagrożenie wykorzysta podatność zasobu informatycznego lub grupy zasobów informatycznych, powodując szkody w przedsiębiorstwie". Opracowanie *COBIT 5 for Risk* ryzyko informatyczne definiuje szerzej jako ryzyko biznesowe związane z wykorzystaniem, posiadaniem, obsługą, zaangażowaniem, wpływem i wdrożeniem rozwiązań IT w ramach przedsiębiorstwa.



Rys. 1. Współpraca COBIT 5 z normami ISO i innymi metodykami

Źródło: ISACA [br.].

Zarządzanie ryzykiem zgodnie z przytoczonym opracowaniem kompleksowo obejmuje wszystkie procesy organizacji, co przedstawiono w tabeli 1.

Tabela 1. Procesowe zarządzanie ryzykiem zgodnie z *COBIT 5 for Risk*

Proces	Opis
1	*2*
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

cd. tabeli 1

1	*2*
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
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 polityki bezpieczeństwa w odniesieniu do zasobów IT

Źródło: Opracowanie własne na podstawie *COBIT 5 for Risk* [ISACA, br.].

Jednak najcenniejszym elementem opracowania *COBIT 5 for Risk* jest tabelaryczne ujęcie scenariuszy ryzyka zarówno w zakresie scenariuszy negatywnych, jak i ich odpowiedników pozytywnych (por. tabela 2)

Tabela 2. Pozytywne i negatywne scenariusze rozwoju ryzyka

Przykładowe negatywne scenariusze	**Przykładowe pozytywne scenariusze**
1	*2*
Realizacja programów/projektów kończy się niepowodzeniem w związku z nieuzyskaniem aktywnego zaangażowania wszystkich interesariuszy (w tym sponsora) w ramach całego cyklu życia programu/projektu	Zadbano o właściwe zarządzanie zmianą w całym cyklu życia programu/projektu, umożliwiające informowanie interesariuszy o postępach w realizacji oraz szkolenie przyszłych użytkowników
Do wdrożenia wybrano niewłaściwą infrastrukturę (pod względem kosztu, wydajności, funkcji, kompatybilności itd.)	Przeprowadza się wcześniejszą analizę i opracowuje uzasadnienie biznesowe, aby zapewnić wybór odpowiedniej infrastruktury
Istnieje niewystarczający zwrot z inwestycji w szkolenia w związku z utratą przeszkolonych pracowników działu IT (np. MBA)	Sformalizowano możliwości rozwoju kariery i określono indywidualne ścieżki, które zwiększają motywację pracowników działu IT, zachęcając ich do pozostania w przedsiębiorstwie przez dłuższy czas
Pracownicy działu IT lub użytkownicy systemów wprowadzają informacje w nieprawidłowy sposób	Stosuje się zasadę dwóch par oczu, zmniejszając tym samym możliwość nieprawidłowego wprowadzania informacji
Za pomocą poczty elektronicznej lub mediów społecznościowych ujawniono informacje wrażliwe	Pracownicy są nieustannie zachęcani do występowania w roli ambasadorów kultury przedsiębiorstwa, etyki i właściwego zachowania. Dotyczy to również praktyk związanych z rozpowszechnianiem informacji za pomocą poczty elektronicznej i mediów społecznościowych
Zainstalowano nową (innowacyjną) infrastrukturę i w rezultacie systemy stały się niestabilne, co doprowadziło do incydentów w trakcie eksploatacji (przykładem może być inicjatywa BYOD (ang. *bring your own device* – „przynieś własne urządzenie")	Przed zastosowaniem infrastruktury w środowisku produkcyjnym przeprowadza się odpowiednie testy w celu zapewnienia dostępności i właściwego funkcjonowania całego systemu

cd. tabeli 2

1	*2*
Brak dostępności kluczowego personelu w związku z akcja protestacyjną (np. strajk komunikacji, blokada dróg)	Elastyczna polityka pracy, umożliwiająca pracownikom pracę z innej lokalizacji niż budynek biura, daje im więcej swobody oraz stwarza pozytywną atmosferę w pracy

Źródło: Opracowanie własne na podstawie *COBIT 5 for Risk* [ISACA, br.].

Mając zidentyfikowane potencjalne źródła ryzyka organizacji biznesowej i oceniając scenariusze negatywne, w kolejnym kroku należy oszacować skutki materializacji (wystąpienia) ryzyka. Biorąc pod uwagę kryteria oceny ryzyk oraz skutki, szczególną uwagę należy zwrócić na:

- wymagania prawne,
- strategiczne dla organizacji procesy biznesowe wspomagane przez systemy informatyczne,
- krytyczne dla organizacji aktywa informacyjne,
- konieczność zapewnienia podstawowych atrybutów w zakresie bezpieczeństwa informacji (dostępności, poufności i integralności),
- negatywne następstwa dla wizerunku i reputacji organizacji, jakie mogą nastąpić w przypadku materializacji ryzyka,
- zakłócenia planów i terminów realizacji zadań biznesowych.

Na podstawie następujących danych:

- zidentyfikowanych ryzyk,
- analizy negatywnych scenariuszy,
- prawdopodobieństwa materializacji ryzyka,
- zastosowanych mechanizmów mitygujących ryzyka zarówno technicznych (np. w postaci klastrów HA, rozwiązań klasy UTM, systemów SIEM), jak również proceduralno-organizacyjnych (polityki, procedury i praktyki, struktury, przepływy informacji itd.),

można przejść do części najtrudniejszej, jaką jest ocena skutków urzeczywistnienia się negatywnego scenariusza, co jest m.in. wymogiem wynikającym z RODO. Wskazane jest, aby szacowanie skutków było prowadzone do określonych scenariuszy incydentów, w czym może pomóc wspomniane opracowanie *COBIT 5 for Risk* [ISACA, br.]. Można również korzystać z wiedzy eksperckiej lub przewrotnie zadać proste pytanie jednostkom biznesowym: ile kosztowałby jeden dzień przestoju np. systemu finansowego wspomagającego sprzedaż? Odpowiedzi są niezwykle trafne dla oceny wartości informacji. Dla wspomagania procesu szacowania ryzyka, w praktyce gospodarczej, stosowana jest metoda oceny skutków i jest to iloczyn prawdopodobieństwa i skutków wystąpienia danego incydentu, na podstawie którego opracowywana jest macierz ryzyka

umożliwiająca grupowanie poziomów ryzyk w celu podjęcia działań łagodzenia ryzyka.

Tabela 3. Macierz ryzyka i objaśnienia wartości w niej występujących

			Skutek				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
Stopień prawdo-podobieństwa	95%	5	Ś	**W**	**NW**	**NW**	**NW**
	75%	4	Ś	**W**	**W**	**NW**	**NW**
	50%	3	*N*	Ś	**W**	**W**	**NW**
	25%	2	*N*	Ś	Ś	**W**	W
	5%	1	*N*	*N*	Ś	**W**	W

Poziom ryzyka	**Ocena ryzyka / niezbędne działania**
N – Niski	*Zidentyfikowane ryzyka na poziomie akceptowalnym*
Ś - Średni	Zidentyfikowane ryzyka wymagają mechanizmów kontrolnych umożliwiających ich okresową ocenę i monitorowanie
W – Wysoki	**Zidentyfikowane ryzyka wymagają podjęcia działań naprawczych oraz objęcia procesem ciągłego monitorowania**
NW – Nieakceptowalnie Wysoki	**Zidentyfikowane ryzyka wymagają natychmiastowych działań umożliwiających obniżenie prawdopodobieństwa bądź skutków zmaterializowania się ryzyka**

Źródło: Opracowanie własne.

3. Estymacja ryzyk w oparciu o metodykę zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych

Szczególnie interesującą propozycją wspomagającą każdą organizację (nie tylko rządową lub reprezentującą administrację publiczną) jest opracowana przez Ministerstwo Cyfryzacji w 2015 r. [www 3]. Metodyka ta umożliwia organizacji oszacowanie/obliczenie:

a) estymacji pierwotnego poziomu ryzyka,
b) ograniczenia ryzyka / sterowania ryzykiem,

Estymacja pierwotnego poziomu ryzyka dokonywana jest zgodnie ze wzorem:

$$R_p = P \times (S_d + S_i + S_p)$$

gdzie:

R_p – pierwotny poziom ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia:

$$P \in \{0, 1,2,3,4\}$$

co oznacza:

0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),
1 – zdarzenie prawie nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

S_d – wartość przypisana skutkowi dla dostępności informacji,
S_i – wartość przypisana skutkowi dla integralności informacji,
S_p – wartość przypisana skutkowi dla poufności informacji,

$$(S_d, S_i, S_p) \in \{0, 1, 2, 3, 4\}$$

co oznacza:

0 – zdarzenie nie powoduje skutku (brak podatności),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

Zgodnie z metodyką zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych podczas ustalania wartości prawdopodobieństwa urealnienia zagrożenia należy przyjąć następujące zasady:

1. Wartość 0 należy przyjąć, jeśli zdarzenie jest wysoce nieprawdopodobne w odniesieniu do systemu lub informacji przetwarzanej w systemie bądź charakter zagrożenia jest nieadekwatny do specyfiki systemu.
2. Wartość 1 należy przyjąć, jeśli częstotliwość materializacji zagrożenia jest liczona co najmniej w dziesiątkach lat lub brak jest informacji, by zagrożenie zmaterializowało się w podobnych podmiotach w kraju lub na świecie.
3. Wartość 2 należy przyjąć, jeśli częstotliwość materializacji zagrożenia jest liczona w pojedynczych latach bądź zagrożenie z danej kategorii zmaterializowało się w podobnych podmiotach w kraju lub na świecie w pojedynczych przypadkach.
4. Wartość 3 należy przyjąć, jeśli materializacja zagrożenia może wystąpić kilka razy w roku.
5. Wartość 4 należy przypisać zagrożeniu, które wielokrotnie materializowało się w ciągu roku w danym podmiocie lub w podobnych podmiotach w kraju albo na świecie.

Należy zwrócić uwagę, że w omawianej metodyce prawdopodobieństwo przyjmuje wartości ze zbioru $\{0, 1, 2, 3, 4\}$ i nie jest miarą statystyczną pomiędzy

0 i 1. Wartości skutków oceniane są odrębnie w wyżej wymienionej metodyce. Mianowicie przyjmuje się, że jeśli urzeczywistnienie zagrożenia nie wywołuje wpływu na dany atrybut bezpieczeństwa, wtedy miary $S_{d,i,p}$ przyjmują wartość 0. W pozostałych przypadkach znajdują zastosowanie następujące zasady:

I. Dla skutku utraty dostępności S_d:
   1. Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany urzeczywistnieniem zagrożenia, mieści się w okresie założonym w planie zapewnienia ciągłości działania (RTO – *Recovery Time Objective*), a przywrócenie pełnego dostępu do informacji lub usług systemu nie wiąże się z dodatkowymi kosztami, należy przyjąć $S_d = 1$.
   2. Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania, ale przywrócenie dostępu do informacji wiąże się z dodatkowymi kosztami, należy przyjąć $S_d = 2$.
   3. Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, znacząco nie mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania, należy przyjąć $S_d = 3$.
   4. Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, wielokrotnie przekracza czas założony w planie zapewnienia ciągłości działania lub jeżeli spowodowana zagrożeniem utrata dostępności informacji jest nieodwracalna, należy przyjąć $S_d = 4$.

II. Dla skutku utraty integralności S_i:
   1. Jeżeli spowodowana zagrożeniem utrata integralności informacji jest łatwo wykrywalna i przywrócenie integralności nie powoduje nadmiernych kosztów, należy przyjąć $S_i = 1$.
   2. Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych, jednak istnieje możliwość skorygowania decyzji, należy przyjąć $S_i = 2$.
   3. Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych oraz nie istnieje możliwość skorygowania decyzji, należy przyjąć $S_i = 3$.
   4. Jeżeli spowodowana zagrożeniem utrata integralności informacji może okazać się niewykrywalna, należy przyjąć $S_i = 4$.

III. Dla skutku utraty poufności S_p:
   1. Jeżeli utrata poufności dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się z odpowiedzialnością karną albo

administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, należy przyjąć $S_p = 1$.

2. Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym (w rozumieniu słownikowym, a nie w kategoriach ustawy o ochronie danych osobowych) lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, należy przyjąć $S_p = 2$.
3. Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, wpływa w sposób znaczący na wizerunek urzędu i organu, który ten urząd obsługuje, jednak nie wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, jednak może wiązać się z odpowiedzialnością administracyjną, należy przyjąć $S_p = 3$.
4. Jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i może prowadzić do roszczeń odszkodowawczych ze strony tych osób, a także do odpowiedzialności karnej osób odpowiedzialnych za zapewnienie ochrony takiej informacji, należy przyjąć $S_p = 4$ [www 3].

Estymacja pierwotnego poziomu ryzyka dokonywana jest zgodnie ze wzorem:

$$R_k = Px\left(\frac{S_d}{C_d} + \frac{S_i}{C_i} + \frac{S_p}{C_p}\right)$$

gdzie:

R_k – końcowy poziom ryzyka,

P – wartość przypisana prawdopodobieństwu urealnienia zagrożenia, $P \in \{0, 1,2,3,4\}$

C – skuteczność środka sterowania ryzykiem (zabezpieczenia) w odniesieniu do atrybutu bezpieczeństwa informacji $(C_d, C_i, C_p) \in \{1, 2, 3, 4\}$ dla środka sterowania ryzykiem wynikającym z zagrożeń,

co oznacza:

1 – brak środka sterowania ryzykiem (zabezpieczenia),

2 – środek sterowania ryzykiem (zabezpieczenie) ogranicza poziom ryzyka,

3 – środek sterowania ryzykiem (zabezpieczenie) w istotny sposób ogranicza poziom ryzyka,

4 – środek sterowania (zabezpieczenie) w bardzo istotny sposób ogranicza poziom ryzyka.

Podczas doboru wartości wskaźnika skuteczności zabezpieczenia należy przyjąć następujące zasady:

1. Jeżeli brak jest możliwości zastosowania zabezpieczenia lub zastosowanie zabezpieczenia jest niecelowe (np. w przypadku $S = 0$), należy przyjąć $C = 1$.
2. Jeżeli zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o jeden stopień, należy przyjąć $C = 2$.
3. Jeżeli zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o dwa stopnie, należy przyjąć $C = 3$.
4. Jeżeli zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ o co najmniej trzy stopnie, należy przyjąć $C = 4$ [www 3].

Podsumowanie

Powyższe informacje oczywiście nie wyczerpują tematu zarządzania ryzykiem informacji w organizacji, stanowią tylko próbę przybliżenia zagadnienia czytelnikowi, który będzie musiał zmierzyć się z tematem zarządzania bezpieczeństwem opartym na ryzyku, jakie wymusza regulacja GDPR/RODO. Próbując ocenić, czy nasza organizacja świadomie zarządza ryzykiem technologicznym, należy spróbować odpowiedzieć sobie na kilka podstawowych pytań:

– Czy określone zostały role i odpowiedzialności w zakresie szacowania ryzyka teleinformatycznego oraz czy role te wynikają z kompetencji uczestników procesu?
– Czy zdefiniowano budżet związany z szacowaniem ryzyka technologicznego?
– 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 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 prowadzony jest monitoring środowiska teleinformatycznego, a jeżeli tak, to czy zastosowano wskaźniki umożliwiające ocenę bezpieczeństwa środowiska teleinformatycznego w celu identyfikacji potencjalnych ryzyk (np. w procesie zarządzania wydajnością i pojemnością infrastruktury IT)?

– Czy procesy obsługi teleinformatycznej z wykorzystaniem usług zewnętrznych (outsourcing) uwzględnione są w procesie szacowania ryzyka, a jeżeli tak, to czy uwzględniają łańcuch poddostawców?

Wymienione pytania mogą stanowić przyczynek do pogłębionej analizy zagadnienia zarządzania bezpieczeństwem opartym na ryzyku.

Literatura

COSO (2004), *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa*, http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Polish.pdf (dostęp: 15.02.2018).

ISACA (br.), *COBIT 5 for Risk*, https://www.isaca.org/COBIT/Pages/COBIT-5-polish.aspx (dostęp: 15.02.2018).

Jatkiewicz P. (2016), *Stan wdrożenia wybranych wymagań Krajowych Ram Interoperacyjności w serwisach samorządowych. Raport z badań*, Polskie Towarzystwo Informatyczne, Warszawa, http://ir.pti.org.pl/wp-content/uploads/2017/02/Biblioteczka-Izby-Rzeczoznawc%C3%B3w-PTI-Tom-3.pdf (dostęp: 15.02.2018).

Komunikat Nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem, Dz.U. Ministra Finansów, http://www.mf.gov.pl/documents/764034/1095334/Dz.+Urz.+Min.+Fin.+z+dnia+18+grudnia+2012+r.+-+poz.+56+- (dostęp: 15.02.2018).

PN-ISO/IEC 27005:2014-01 (wersja polska), *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*, http://sklep.pkn.pl/pn-iso-iec-27005-2014-01p.html (dostęp: 15.02.2018).

PN-ISO/IEC 31000 (wersja polska), *Zarządzanie ryzykiem – Zasady i wytyczne*, http://sklep.pkn.pl/pn-iso-31000-2012p.html (dostęp: 15.02.2018).

Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf (dostęp: 15.02.2018).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041001024 (dostęp: 15.02.2018).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 (dostęp: 15.02.2018).

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526 (dostęp: 15.02.2018).

[www 1] https://zaufanatrzeciastrona.pl/post/hasla-ponad-10-milionow-polskich-kont-email-dostepne-do-pobrania-w-sieci/ (dostęp: 15.02.2018).

[www 2] *Podejście oparte na ryzyku, czyli Risk Based Approach*, http://przetwarzanie danych.pl/podejscie-oparte-na-ryzyku-czyli-risk-based-approach/ (dostęp: 15.02.2018).

[www 3] *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, http://krmc.mc.gov.pl/download/50/12585/MetodykaZarzadzaniaRyzykiemCRP2015v18ZZKRMC.docx (dostęp: 15.02.2018).

GDPR RISK BASED APPROACH

Summary: Since 25th May 2018 requirements concerning personal data processing information system security should be dependent on risk analysis. Risk Based Approach means that regulation does not force to application of particular procedures and media, but it suggests to conduct autonomous analysis of risks. In that context, the paper aims to the presentation of actual situation in financial sector, as well as in public administration sector in the aspect of preparation to the risk analysis process. Next, the method of risk estimation is presented and its usability for privacy protection is discussed.

Keywords: GDPR, information security, IT risk management, personal data protection.