Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017)
DOI: 10.15584/nsawg.2017.4.18 **ISSN 1898-5084**

dr hab. Zygmunt Mazur[1]
Katedra Inżynierii Oprogramowania
Wydział Informatyki i Zarządzania Politechniki Wrocławskiej

dr Janusz Pec[2]
Główny Urząd Statystyczny

Analiza ryzyka II poziomu w 3-poziomowym hierarchicznym modelu zarządzania bezpieczeństwem informacji uwzględniająca specyfiki statystyki publicznej

Wprowadzenie

Statystyka publiczna zajmuje się zbieraniem danych statystycznych, ich gromadzeniem, przechowywaniem i analizowaniem, a także ogłaszaniem, udostępnianiem i rozpowszechnianiem wyników badań statystycznych. Jest niezwykle ważnym elementem w systemie informacyjnym społeczeństwa demokratycznego. Obejmuje badania statystyczne, prace metodologiczne, klasyfikacyjne i nomenklaturowe, opracowania i publikacje, rejestry i bazy danych. Udostępnia organom władzy państwowej, administracji publicznej (rządowej i samorządowej), podmiotom gospodarczym i obywatelom dane statystyczne umożliwiające ocenę zjawisk ekonomicznych, demograficznych i społecznych. W Polsce centralnym organem statystyki publicznej jest Główny Urząd Statystyczny (GUS).

Do zarządzania danymi pozyskanymi przez służby statystyki publicznej od sprawozdawców oraz pozostałą informacją charakteryzującą funkcjonowanie organizacji będzie wykorzystywany Kompleksowy System Zarządzania Bezpieczeństwem Informacji (KSZBI). System ten powinien być częścią modelu informacyjnego statystyki publicznej rozumianego jako zbiór zidentyfikowanych procesów[3] organizacji (nie tylko biznesowych), łącznie z mapą powiązań między

[1] Adres korespondencyjny: Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław; e-mail: zygmunt.mazur@pwr.edu.pl, tel. 71 320 4223.

[2] Adres korespondencyjny: GUS, 00-925 Warszawa; e-mail: j.pec@stat.gov.pl, tel.22 608 38 92.

[3] Przez proces rozumiemy zbiór wzajemnie ze sobą powiązanych działań (czynności), następujących jedno po drugim, które przekształcają dane wejściowe w dane wyjściowe.

nimi (topologią). Należy przy tym zauważyć, iż tworzenie (a w zasadzie analiza) mapy procesów może uwidocznić procesy wcześniej niezidentyfikowane [Białas, 2008; Molski, Łacheta, 2006].

Podstawy prawne i zasady postępowania z danymi statystycznymi dotyczące bezpieczeństwa, zbierania, przechowywania, archiwizowania i niszczenia, kontroli i publikowania, muszą być precyzyjnie określone.

W artykule zostanie przeprowadzona analiza ryzyka w hierarchicznym modelu zarządzania bezpieczeństwem informacji, uwzględniająca specyfiki statystyki publicznej. Celem pracy jest rozpoznanie, na ile propozycja analizy zbioru specyfik organizacji statystyki publicznej umożliwi wykonanie w miarę wiarygodnej analizy ryzyka w przypadku braku modelu informacyjnego w korporacji.

Do ochrony ważnych informacji firmowych można wykorzystać opracowaną przez *European Network Security Institute* (ENSI) metodykę TISM (*Total Information Security Management*), udostępnianą na Licencji Bezpłatnej Dokumentacji GNU i umożliwiającą zbudowanie trójpoziomowego hierarchicznego modelu zarządzania bezpieczeństwem informacji [Byczkowski, 2000]. W modelu powinny być uwzględnione co najmniej minimalne wymagania zgodne z obowiązującymi uregulowaniami prawnymi, potrzeby danej instytucji, jej zasoby i specyfika funkcjonowania.

Podstawowe trzy poziomy zarządzania bezpieczeństwem informacji w metodyce TISM to:

– poziom I – Polityka Bezpieczeństwa Informacji (PBI) – obejmująca określenie wymagań bezpieczeństwa dla instytucji i zasady zarządzania nim,
– poziom II – Grupa informacji – zawierająca uszczegółowienie wymagań dla grup informacji chronionych,
– poziom III – System przetwarzania – dotyczy spełniania wymagań bezpieczeństwa przez systemy do przetwarzania informacji chronionych, wypełniania założeń dokumentów z poziomu I i II – określa cel i zakres systemu, schemat i kryteria bezpieczeństwa systemu, zasady zarządzania nim, zasady reagowania w sytuacjach kryzysowych i przeprowadzania audytów bezpieczeństwa.

Analiza ryzyka – podejście zasobowe i procesowe

Analizę ryzyka II poziomu można wykonać albo w oparciu o analizę zasobów organizacji, albo o analizę wszystkich procesów związanych z funkcjonowaniem organizacji w aspekcie jej bezpieczeństwa. Przy podejściu zasobowym do analizy ryzyka[4], z reguły rozważane są wszystkie aktywa, natomiast przy podejściu procesowym rozważane są tylko te aktywa, które są wykorzystywane przez dane

[4] Przez pojęcie „ryzyko" rozumiemy prawdopodobieństwo zajścia zdarzenia, które może negatywnie wpływać na realizację założonych celów (utrudniać lub wręcz uniemożliwiać realizację celów). Analiza ryzyka to proces obejmujący identyfikację ryzyka, jego ocenę oraz ocenę mechanizmów kontroli.

procesy. Przewaga podejścia procesowego wynika z faktu większej elastyczności i precyzji sposobu wykonania analizy, bowiem natura bezpieczeństwa jest głęboko umocowana w szczegółach, a przedstawione podejście uwzględnia je w większym stopniu niż zasobowe.

Przy podejściu procesowym zasoby i aktywa nieuwzględniane przez procesy, nie odgrywają żadnej roli i nie mają wpływu na wynik analizy ryzyka. Z punktu widzenia procesowości – nie istnieją. Pewne zasoby są niewykorzystywane, nieprzydatne lub nieistotne dla prawidłowego funkcjonowania danej organizacji/korporacji. Podejście zasobowe może też tworzyć luki (dziury) w bezpieczeństwie (tzw. problem durszlaka), gdyż w procesie analizy ryzyka dany zasób jest analizowany tylko raz w relacji do jego podatności i możliwych zagrożeń wykorzystujących te podatności. W przypadku analizy procesowej jest uwzględniany tyle razy, ile procesów dany zasób wykorzystywało.

Problemem przy podejściu procesowym jest monitorowanie zmienności procesów i reagowania na te zmiany.

W przypadku opisanego i ustalonego zbioru procesów i ich mapy powiązań, zjawisko zmienności procesów (ich zanikania, modyfikowania, ewentualnie powstawania nowych procesów) można w pewnej mierze monitorować za pomocą odpowiednich narzędzi, np. wykorzystując znane od dawna karty kontrolne Shewharta [Shewhart, 1931]. W przypadku niepełnych danych o procesach (problem durszlaka) nie wiadomo, ile jest brakujących danych (dziur) i jakiego są rodzaju (ponieważ nie znana jest mapa procesów). Nie wiadomo także, jaka jest tendencja i kierunek ich zmian (rozrostu) – przy dużej liczbie procesów elementarnych złożoność zadania znacznie rośnie. Osobnym zagadnieniem, wykraczającym poza ramy tej pracy, jest zdefiniowanie (wyodrębnienie) procesów elementarnych i zbudowanie algorytmu wyodrębniania z procesu złożonego procesów elementarnych.

Przy braku modelu informacyjnego pewnym substytutem w procesie analizy ryzyka na II poziomie może być próba rozważenia specyficznych właściwości funkcjonowania organizacji (tzw. specyfik), wyróżniających w pewnym zakresie daną organizację od innych. Pełny ich zestaw powinien ją jednoznacznie identyfikować.

ANALIZA WYBRANYCH SPECYFIK STATYSTYKI PUBLICZNEJ

W celu zilustrowania omawianego zagadnienia podamy przykładowe specyfiki statystyki publicznej oraz ich składowe. Lista ta oczywiście nie jest kompletna, gdyż nie uwzględnia specyfik poszczególnych Jednostek Organizacyjnych Systemu Statystyki Publicznej (JOSSP) w obszarze ich specjalizacji w odniesieniu do wszystkich grup informacji na II poziomie.

Przykładowa lista specyfik obejmuje 15 obszarów:

1. Spisy powszechne.
2. Statystka małych obszarów (SMO).

3. Wdrażanie wyników prac Komisji Metodologicznej GUS – organu opiniodawczo-doradczego i monitorującego jakość systemów, badań statystycznych i standardów metadanych.
4. Raportowanie do Eurostatu (Europejskiego Urzędu Statystycznego).
5. Współpraca transgraniczna.
6. Poziom i jakość współpracy metodologicznej z Polskim Towarzystwem Statystycznym (PTS) – prowadzenie niezależnych badań statystycznych przez organy PTS takie jak Biuro Badań i Analiz Statystycznych (BBiAS) oraz Sekcję Klasyfikacji i Analizy Danych (SKAD), dzięki czemu jest możliwość uzyskiwania rozbieżnych wyników i stosowania odmiennych metod analiz.
7. Portal geostatystyczny.
8. Specjalizacja Urzędów Statystycznych (US).
9. Utrzymywanie długich porównywalnych szeregów czasowych danych.
10. Gwarantowanie tajemnicy statystycznej podmiotom gospodarczym.
11. Bazy dziedzinowe.
12. Badanie obciążeń sprawozdawców.
13. Określanie standardów metadanych statystycznych.
14. Bank Danych Lokalnych (BDL), jako platforma współpracy z samorządami.
15. Informacje sygnalne.

Wymienione specyfiki dotyczą prawie wszystkich grup informacji i mają wpływ na wysokopoziomową analizę ryzyka[5] na II poziomie dla statystyki publicznej.

Przedstawimy teraz szczegółowo przykładowy opis dla dwóch pierwszych spośród piętnastu zidentyfikowanych specyfik: w tabeli 1 – dla spisów powszechnych, w tabeli 2 – dla statystyki małych obszarów.

Ocenę realizacji zagrożenia i jego skutku wykonuje silnik analizy ryzyka, który może być oparty na metodzie jakościowej. W przypadku różnych ograniczeń czasowych, organizacyjnych, finansowych opracowanie wskaźników ilościowych może być zadaniem trudnym do wykonania, natomiast będzie ono wręcz niezbędne na poziomie III (gdzie konieczne jest opracowanie wskaźników przynajmniej jakościowo-ilościowych, jeżeli ze względów metodologicznych i innych nie jest możliwe opracowanie wszystkich potrzebnych wskaźników ilościowych – wraz ze wzrostem liczby wskaźników ilościowych wzrasta poziom obiektywizmu i wiarygodności).

W rzeczywistości postać wzorów wykorzystywanych do obliczeń ryzyka na II poziomie w wysokopoziomowej analizie ryzyka nie jest aż tak istotna – o jej jakości nie decydują przyjęte wzory, ale jak najpełniejsza identyfikacja specyfiki pracy organizacji oraz standardowe działania jakie wykonuje większość organizacji w aspekcie ochrony informacji w powiązaniu z siatką zależności między grupami informacji na II poziomie – przepływ danych między nimi i wynikające z tego ryzyka.

[5] Wysokopoziomowa analiza ryzyka polega na wyróżnieniu obszarów wymagających dalszej szczegółowej analizy ryzyka oraz tych, w których wystarczy ochrona podstawowa.

Tabela 1. Opis specyfiki: Spisy powszechne

Przykładowe podatności	Przykładowe możliwe zagrożenia	Przykładowa ocena realizacji zagrożenia i jego skutku	Przykładowe wytyczne spływające z poziomu II do poziomu III w formie propozycji środków zapobiegawczych
1	*2*	*3*	*4*
1. Słaba metodologia spisów. 2. Słaba infrastruktura techniczno-organizacyjna. 3. Niewystarczające rozpoznanie firm wspomagających spisy przy przetargach. 4. Podatność na naciski społeczno-polityczne. 5. Duża stresogenność – dotrzymanie reżimów czasowych. 6. Brak szkoleń i pilotażów przed-spisowych. 7. Niska jakość raportów i publikacji po-spisowych. 8. Brak zastosowania metodyki projektowej.	1. Możliwość przekłamań. 2. Wyciek danych jednostkowych. 3. Mała precyzja zebranych danych. 4. Przekroczenie czasowe. 5. Atak mediów. 6. Brak profesjonalizmu kadry zarządzającej wskutek braku szkoleń lub ich niskiej jakości. 7. Niewłaściwa (celowa lub wynikająca z braku umiejętności) interpretacja danych przez użytkownika.	1. Duże prawdopodobieństwo wycieku danych jednostkowych (np. wykorzystanie podatności 1, 2, 5 skutkuje realizacją zagrożenia 2). 2. Niezgodności w danych demograficznych w raportach po-spisowych z rzeczywistością wywołujące frustrację miejscowej ludności (przykład z ostatniego spisu powszechnego ludności w 2011r.– sprawy etniczne związane z ludnością kaszubską) – wykorzystanie podatności 4. Może to być zdarzenie incydentalne – oszacowanie prawdopodobieństwa trudne ze względu na niestabilność dynamiki zachowań społecznych. Podatność ta może być wykorzystana przez zagrożenie 5 lub 7. 3. Średnie prawdopodobieństwo otrzymania spójności logicznej i wiarygodności danych zebranych metodą ankietyzacji bezpośredniej, np. wykorzystanie podatności 1, 2, 3, 5, 6.	– Na poziomie Operacyjnej Bazy Mikrodanych (OBM) (III poziom) sprawdzić algorytm anonimizacji danych – dobór odpowiednich generatorów liczb pseudolosowych (ze względu na skutek 1 z kolumny 3). – W systemie ankietyzacji poprawić ergonomiczność formularza handheldu i układu logicznego pytań (CAPI – *Computer Assisted Personal Interviewing*) – odpowiedź na realizację zagrożenia 3 i jego skutek 3. – Uzgodnić z przedstawicielami Zrzeszenia Kaszubsko-Pomorskiego treść pytań w formularzu spisowym (w systemie informatycznym realizującym ten formularz) obsługującym przynależność narodową lub etniczną – odpowiedź na realizację zagrożenia 2 i jego skutek 2.

Źródło: opracowanie własne.

Tabela 2. Opis specyfiki: Statystyka małych obszarów

Przykładowe podatności	Przykładowe możliwe zagrożenia	Przykładowa ocena realizacji zagrożenia i jego skutku	Przykładowe wytyczne spływające z poziomu II do poziomu III w formie propozycji środków zapobiegawczych
1	*2*	*3*	*4*
1. Zły dobór jednostek obserwacji (rejonu statystycznego). 2. Złe przypisanie charakterystyki do jednostki (miejska, miejsko-wiejska, wiejsko-miejska, wiejska). 3. Nieoptymalny wybór metod podziału jednostek statystycznych, np. w analizie skupień konkretny algorytm jest uwarunkowany źródłem danych i oczekiwaną postacią wyników –zamiast np. klasycznej hierarchicznej metody wyboru rozmytej analizy skupień. 4. Nieprecyzyjne dane topograficzne z Głównego Urzędu Geodezji i Kartografii (GUGiK), np. Baza Danych Obiektów Ogólnogeograficznych (BDOO) dla wymogów statystyki regionalnej za mało dokładna.	1. Niewłaściwa interpretacja zjawisk społeczno-gospodarczych w danym regionie. 2. Statystyka opisowa regionu nie odzwierciedla rzeczywistych parametrów statystycznych (np. średnie, kwartyle, odchylenia standardowe, mediany itp.). 3. Negatywny pływ na wynik grupowania. 4. Nieuwzględnienie niektórych ważnych obiektów topograficznych.	1. Mylny komunikat dla władz regionalnych –samorządowych i administracji terenowej. Wykorzystanie podatności 1i 2[6]. 2. Nieprecyzyjne lub nieprawdziwe informacje publikowane na stronach internetowych urzędów, co skutkuje utratą wizerunku, np. wykorzystanie podatności 2 i 3[7]. 3. Brak odnotowania zmian w strukturze pokrycia terenu – może skutkować błędnymi decyzjami środowiskowymi podjętymi przez władze terenowe – konflikty z lokalnymi środowiskami mieszkańców, ekologami itp. Wykorzystanie podatności 4[8].	– Przygotować lub uaktualnić w US teleinformatyczny system komunikacji elektronicznej (telekonferencja) do wspomagania lokalnego rzecznika prasowego w przypadku konieczności sprostowań w miejscowych mediach publicznych – odpowiedź na zagrożenie 1 i skutek 1. – W systemach obsługujących portale US algorytmy korekcji i monitorowania danych powinny pracować online – ciągła aktualizacja danych poprzez odpowiednią dla danego systemu konfigurację parametrów jego pracy – odpowiedź na realizację zagrożenie 2 i skutek 2. – Zwrócenie uwagi na zapytania o mikrodane z OBM w Portalu Geostatystycznym – zabezpieczenie aktualności danych – odpowiedź na zagrożenie 4 i skutek 3.

Źródło: opracowanie własne.

[6] Zdarzenie raczej incydentalne – prawdopodobieństwo wystąpienia niewielkie, ale skutek może być poważny.

[7] Prawdopodobieństwo wystąpienia raczej niewielkie, skutek wizerunkowy – duży.

[8] Realizacja zagrożenia raczej incydentalna, ale w razie wystąpienia skutki mogą być poważne.

PRZYKŁAD IMPLEMENTACJI ANALIZY RYZYKA UWZGLĘDNIAJĄCEJ SPECYFIKI STATYSTYKI PUBLICZNEJ

Zaproponowany opis specyfiki statystyki publicznej w aspekcie bezpieczeństwa informacji można wykorzystać w analizie ryzyka II poziomu.

Przyjmujemy następujące oznaczenia i założenia dla dalszych rozważań:

1. n – liczba obszarów (specyfik), n =15
2. sp_i – i-ta specyfika (i =1, …, n)
3. $il(sp_i)$ – liczba wytycznych dla i-tej specyfiki spływających z poziomu II na poziom III (i = 1, …, n),
4. $ZW = \{il(sp_i): i = 1, ..., n\}$ – zbiór liczb wytycznych dla wszystkich specyfik,

   $|ZW| = \sum_{i=1}^{i=n} il(sp_i)$ – liczba wszystkich wytycznych.

   Przyjmując następujące wartości zmiennych $il(sp_i)$, dla n=15:
   ZW = {18, 12, 5, 3, 7, 7, 11, 9, 4, 5,10, 3, 9, 13, 4},
   otrzymujemy $|ZW| = 120$.
5. $wsp(sp_i)$ – skuteczność wsparcia obszaru i-tej specyfiki – wsparcia technicznego i organizacyjnego (finansowego, kadrowego) oferowanego przez kadrę zarządzającą statystyką publiczną w celu redukcji słabości rozwiązań stosowanych w tym obszarze.
   $wsp(sp_i) \neq 0$, gdyż wspomniane rozwiązania funkcjonują (lepiej lub gorzej) w każdym z 15 obszarów.
   Przyjmijmy, że $wsp(sp_i) \in \{1, 2, 3\}$, gdzie:
   1– skuteczność niska,
   2 – skuteczność zadawalającą,
   3 – skuteczność odpowiednia do zauważonych słabości rozwiązań.
   Załóżmy, że określono następujący zbiór wartości skuteczności wsparcia dla zidentyfikowanych 15 obszarów:
   $\{wsp(sp_i), i = 1, …, 15\} = \{3, 2, 1, 3, 2, 2, 2, 1, 2, 2, 1, 1, 2, 2, 3\}$.
6. $kor(sp_i)$ – współczynnik korygujący dla i-tej specyfiki, odzwierciedlający słabość rozwiązań (techniczno-organizacyjnych) zastosowanych w danym obszarze specyfiki w stosunku do ogółu, określamy jako

$$kor(sp_i) = \frac{il(sp_i)}{\sum_{i=1}^{i=n} il(sp_i)}$$

   W rozważanym przykładzie $kor(sp_i) = \frac{il(sp_i)}{120}$, dla i =1, …, 15, otrzymujemy następujący zbiór wartości (po zaokrągleniu do dwóch miejsc po przecinku)
   $\{kor(sp_i), i = 1, …, 15\} = \{0.15, 0.10, 0.04, 0.02, 0.05, 0.05, 0.09, 0.07, 0.03, 0.04, 0.08, 0.02, 0.07, 0.11, 0.03\}$.
7. $p(sp_i)$ – prawdopodobieństwo wykorzystania słabości stosowanych rozwiązań w rozważanym obszarze i-tej specyfiki,

$p(sp_i) \in [0, 1]$, dla $i = 1, \ldots, n$.
Wartości $p(sp_i)$ można oszacować metodą delficką (lub jej zmodyfikowaną wersją) z dokładnością do dwóch miejsc po przecinku (lub równoważnie procentowo).
Otrzymany zbiór wartości w rozważanych 15 obszarach:
$\{p(sp_i),\ i = 1, \ldots, 15\} = \{0.22, 0.35, 0.32, 0.33, 0.27, 0.11, 0.44, 0.37, 0.55, 0.07, 0.34, 0.22, 0.31, 0.47, 0.21\}$.

8. $m(sp_i)$ – miara dla i-tej specyfiki wyrażona jako wartość w ustalonej skali. Im wyższa wartość $m(sp_i)$, tym większa słabość stosowanych w danym obszarze specyfiki rozwiązań, a więc pośrednio zwiększa to wartość ryzyka. Na II poziomie nie rozważamy atrybutów dostępności, integralności, poufności dla obszaru specyfiki, gdyż w poszczególnych obszarach specyfiki może być wiele systemów informacyjnych i różnych typów informacji. Różne regulacje prawne dotyczące ich ochrony (różne dane chronione) uniemożliwiają praktycznie wyliczanie średnich wielkości. Można to zrobić na III poziomie po wykonaniu dokładnej klasyfikacji poszczególnych jednostkowych informacji – danych opisujący całościowo konkretny system użytkowy.

Propozycje interpretacji miar dla poszczególnych specyfik

W odniesieniu do zdefiniowanej listy 15-tu specyfik przedstawimy propozycję interpretacji poszczególnych wartości miar.

Kontynuując przykład, zakładamy, że wartości miar dla danej specyfiki zostały uśrednione, a wybór dokonany przez grupę ekspertów zaznaczamy symbolem „✓”.

1. Spisy powszechne – $m(sp_1) \in \{0, 1, 2\}$, gdzie:
- 0 – spis przeprowadzony, wyniki wiarygodne, ✓
- 1 – spis przeprowadzony, wyniki mało wiarygodne,
- 2 – brak przeprowadzonego spisu w założonym terminie.

2. Statystyka małych obszarów – $m(sp_2) \in \{1, 2, 3\}$, gdzie:
- 1 – etap rozwoju i wdrażania, ✓
- 2 – etap zamknięcia – metody nie są dalej rozwijane,
- 3 – faza testów.

3. Wdrażanie wyników prac Komisji Metodologicznej – $m(sp_3) \in \{0, 1, 2\}$, gdzie:
- 0 – wdrażanie sukcesywne,
- 1 – wdrażanie z opóźnieniami, ✓
- 2 – brak wdrożenia.

4. Raportowanie do Eurostatu – $m(sp_4) \in \{1, 2, 3\}$, gdzie:
- 1 – przekazywanie makroagregatów,
- 2 – przekazywanie mikrodanych zanonimizowanych,
- 3 – przekazywanie danych jednostkowych. ✓

5. Współpraca transgraniczna – $m(sp_5) \in \{0, 1, 2\}$, gdzie:
0 – brak współpracy,
1 – współpraca okazjonalna,
2 – stała współpraca. ✓

6. Poziom i jakość współpracy z PTS (niezależne badania, np. BBIAS, SKAD) – $m(sp_6) \in \{0, 1, 2\}$, gdzie:
0 – wyniki zgodne,
1 – wyniki częściowo zgodne, ✓
2 – wyniki rozbieżne.

7. Portale statystyki publicznej – $m(sp_7) \in \{0, 1, 2\}$, gdzie:
0 – nieodwiedzane,
1 – rzadko odwiedzane, przypadkowo, okazjonalnie,
2– odwiedzane w zależności od potrzeb edukacyjnych, informacyjnych i sprawozdawczych użytkowników. ✓

8. Specjalizacja US – wartość $m(sp_8) \in \{0, 1\}$, gdzie:
0 – brak dalszego rozwoju specjalizacji, ✓
1– rozwijanie specjalizacji w relacji do programu badań statystycznych.

9. Utrzymywanie długich porównywalnych szeregów czasowych – $m(sp_9) \in \{0, 1, 2\}$, gdzie:
0 – brak,
1 – częściowe utrzymywanie (niektóre szeregi w niektórych komórkach organizacyjnych, np. US), ✓
2 – pełne utrzymywanie (wszystkie w ramach danej specjalizacji) przez wszystkie komórki organizacyjne statystyki publicznej.

10. Gwarantowanie tajemnicy statystycznej podmiotom gospodarczym – $m(sp_{10}) \in \{0, 1\}$, gdzie:
0 – zapewniona gwarancja, ✓
1 – brak gwarancji.

11. Bazy dziedzinowe/wiedzy – $m(sp_{11}) \in [0\%, 100\%]$ – wartość procentowa określająca użyteczność dla użytkowników (częstość odwiedzin w miesiącu), – przyjmujemy 33% w skali roku. ✓

12. Badanie obciążeń sprawozdawców – $m(sp_{12}) \in \{1, 2, 3\}$, gdzie:
1 – małe,
2 – średnie, ✓
3 – duże.

Uwaga: przypadki 2 i 3 sugerują możliwość popełniania błędów w sprawozdaniach.

13. Jakość standardów metadanych statystycznych – $m(sp_{13}) \in \{1, 2, 3\}$, gdzie:
1 – wysoka,
2 – średnia, ✓
3 – mała.

Uwaga: dotyczy zwłaszcza bezpieczeństwa semantycznego/ontologicznego (nie ujawnia się żadnych dodatkowych informacji o danych).

14. BDL jako forma współpracy z samorządami – $m(sp_{14}) \in \{0, 1, 2\}$, gdzie:
0 – nie istnieje,
1 – niski poziom współpracy,
2 – poziom satysfakcjonujący. ✓
15. Informacje sygnalne – $m(sp_{15}) \in \{0, 1\}$, gdzie:
0 – opublikowane w terminie, ✓
1 – opublikowane z opóźnieniem.

Analiza ryzyka II poziomu

Prawidłowo wykonana analiza ryzyka – jakościowa, ilościowa czy mieszana powinna uwzględniać specyfikę danej organizacji/korporacji. Jest to dokument podstawowy – źle wykonana analiza ryzyka przekreśla w znaczącym stopniu dokumenty pochodne – polityki, a te z kolei procedury, regulaminy, instrukcje.

Dokumentacji PBI II poziomu powinna uwzględniać następujące główne zagadnienia (pomijając wstęp, podsumowanie, metryczkę itp.):

1. Uzasadnienie wyboru metodyki analizy ryzyka dla danej polityki – zalety i wady wyboru.
2. Opis środowiska działania – kontekst (uwzględnienie specyfiki statystyki publicznej odnoszące się do tej grupy informacji).
3. Opis implementacji zabezpieczeń odnośnie zagrożeń zidentyfikowanych wcześniej w analizie ryzyka i odnoszących się do najważniejszych składowych ryzyka wysokopoziomowego – w tym celu można posłużyć się listą składowych ryzyka określoną w wykonanej uprzednio analizie ryzyka na rzecz PBI II poziomu.
4. Opis zasad zarządzania bezpieczeństwem informacji na II poziomie w aspektach:

– sprzętowym – opis sprzętu komputerowego – wersje firmware, podział na marki firmowe, przewidywana żywotność, itp.,
– oprogramowania – opis używanych programów (zwłaszcza monitorujących bezpieczeństwo), wersji, PKI, stosowanej kryptografii itp.,
– organizacyjnym: kwalifikacje personelu i system rekrutacji oraz struktura organizacyjna Centrum Informatyki Statystycznej (CIS),
– logistycznym – serwisowanie oprogramowania, sprzętu, klimatyzacji, zabezpieczenie zasilania, ogólne zasady ochrony fizycznej i alarmowej, ośrodki zapasowe,
– współpracy z partnerami wewnętrznymi i zewnętrznymi (jednostki administracji państwowej, organizacje społeczne i zawodowe, firmy wspomagające realizację zadań statystyki publicznej oraz partnerzy zagraniczni np. Eurostat),
– zgodności ze standardami normalizacyjnymi,
– zgodności z regulacjami prawnymi (krajowymi i unijnymi),
– architektury korporacyjnej i jej modyfikacji (w tym architektury sieci),
– zasad pracy systemowej analitycznej i projektowej – zasady bezpiecznego projektowania stosowane w CIS,

– opis ogólnych zasad testowania i rozwoju systemów pod kątem bezpieczeństwa i ich jakości,
– opis modelu statystycznego zdarzeń związanych z bezpieczeństwem informatycznym,
– opis zasad ciągłości działania i przywracania stanu docelowego,
– opis ogólnych zasad refleksji powłamaniowej i analizy forensic,
– opis zasad pracy rzecznika prasowego CIS lub osoby reprezentującej interesy CIS w przypadku incydentów – ochrona wizerunku.

5. Opis ścieżki dojścia (w punktach) wymienionych w pkt. 4 od stanu wykazanego w audycie lub po analizie ryzyka do stanu pożądanego. Powinien on zawierać:
– inwentaryzację stanu bieżącego, procedury, polityki, instrukcje, stosowane dobre praktyki itp.,
– identyfikację parametrów docelowych przy istniejących ograniczeniach i harmonogram dojścia do celu.
6. Listę wytycznych dla polityk III poziomu i referencji do polityk II poziomu pozostałych grup informacji, które będą korzystać z jej zaleceń (lista referencyjna, do której będą się odwoływać pozostałe polityki).

Polityki III poziomu różnią się od poziomu II, chociaż mają też elementy wspólne. Są one bardziej związane ze szczegółami infrastruktury techniczno-organizacyjnej dla konkretnego rozwiązania obsługującego daną usługę biznesową lub wynikającą z potrzeby spełnienia obowiązujących wymagań prawnych.

Dla wcześniej przyjętych danych przykładowych oszacujmy jakość udzielonego wsparcia i jego wpływ na zmniejszenie ryzyka.

Przyjmijmy oznaczenia:

R_P – ryzyko początkowe (pierwotne, bez udzielonego wsparcia),

R_K – ryzyko końcowe (po udzieleniu wsparcia).

Z reguły zachodzą zależności: $0 \le R_P$, $R_K \le 1$ oraz $R_K \le R_P$, chyba, że wsparcie przyczyniło się do zwiększenia ryzyka, co jest mało prawdopodobne, ale możliwe w przypadku błędnych decyzji.

Obliczając oba ryzyka (po zaokrągleniu do dwóch miejsc po przecinku) otrzymujemy:

$$R_P = \sum_{i=1}^{i=15} p(sp_i) \times m(sp_i) \times kor(sp_i) =$$

$0.22\times0\times0.15 + 0.35\times1\times0.10 + 0.32\times1\times0.04 + 0.33\times3\times0.02 + 0.27\times2\times0.05 + 0.11\times1\times0.05 + 0.44\times2\times0.09 + 0.37\times0\times0.07 + 0.55\times1\times0.03 + 0.07\times0\times0.04 + 0.34\times0.33\times0.08 + 0.22\times2\times0.02 + 0.31\times2\times0.07 + 0.47\times2\times0.11 + 0.21\times0\times0.03 \approx \underline{\mathbf{0.36}}$

$$R_K = \sum_{1=1}^{i=15} (p(sp_i) \times m(sp_i) \times kor(sp_i))/wsp(sp_i) =$$

$(0.22\times0\times0.15)/3 + (0.35\times1\times0.10)/2 + (0.32\times1\times0.04)/1 + (0.33\times3\times0.02)/3 + (0.27\times2\times0.05)/2 + (0.11\times1\times0.05)/2 + (0.44\times2\times0.09)/2 + (0.37\times0\times0.07)/1 + (0.55\times1\times0.03)/2 + (0.07\times0\times0.04)/2 + (0.34\times0.33\times0.08)/1 + (0.22\times2\times0.02)/1 + (0.31\times2\times0.07)/2 + (0.47\times2\times0.11)/2 + (0.21\times0\times0.03)/3 \approx \underline{\mathbf{0.29}}$

W celu oszacowania jakości wsparcia obliczamy $R_P - R_K = 0.07$, czyli po udzieleniu wsparcia uzyskaliśmy 7% poprawę (zmniejszyliśmy ryzyko o 7%).

Przyjmując, że liczba komórek organizacyjnych w statystyce publicznej wynosi 21 (16 US, Centrala GUS, 4 dodatkowe jednostki wspierające – CIS, ZWS, CBiES, CBS) oraz, że dowolna kombinacja specyfik może dotyczyć każdego z 15 obszarów, można policzyć ryzyko maksymalne początkowe R_{MAX_P} i końcowe R_{MAX_K}, według wzorów:

$$R_{MAX_p} = \sum_{l=1}^{l=21} \sum_{j=1}^{j=\binom{15}{i}} \sum_{i=1}^{i=15} p(sp_{i,j,l}) \times m(sp_{i,j,l}) \times kor(sp_{i,j,l})$$

$$R_{MAX_K} = \sum_{l=1}^{l=21} \sum_{j=1}^{j=\binom{15}{i}} \sum_{i=1}^{i=15} \frac{p(sp_{i,j,l}) \times m(sp_{i,j,l})}{wsp(sp_{i,j,l})} \times kor(sp_{i,j,l})$$

gdzie:

l – numer komórki organizacyjnej,

$\binom{15}{i}$ – liczba kombinacji z 15 elementów po i elementów,

$p(sp_{i,j,l})$, $m(sp_{i,j,l})$, $kor(sp_{i,j,l})$, $wsp(sp_{i,j,l})$ – zdefiniowane wcześniej wartości dla i-tej specyfiki w j-tej kombinacji specyfik, do której ona należy, dla l-tej komórki organizacyjnej.

Można także policzyć wielkości $\frac{R_P}{R_{MAX_P}}$ i $\frac{R_K}{R_{MAX_K}}$ ilustrujące stosunek ryzyka początkowego (stan aktualny przed wdrożeniem zabezpieczeń) do maksymalnego możliwego ryzyka początkowego (analiza najgorszego przypadku) i podobnie dla ryzyka końcowego (po wdrożeniu zalecanych zabezpieczeń).

Zakończenie

Propozycja uwzględnienia specyfiki statystyki publicznej w analizie ryzyka II poziomu przedstawiona w niniejszej pracy i sposób jej implementacji stanowi jedno z możliwych rozwiązań tego problemu w praktyce. Idea tej metody może posłużyć innej organizacji, w tym korporacjom, być może w zmodyfikowanej wersji do wykorzystania w swoich działaniach doskonaląc ochronę ważnych informacji w tym technologicznych. Decyduje to często o utrzymaniu przewagi konkurencyjnej. Jak już wspomniano na początku pracy, innym i dokładniejszym sposobem jest oparcie analizy ryzyka o mapę powiązań wszystkich procesów funkcjonujących w organizacji, które wpływają na bezpieczeństwo informacji. Wydaje się jednak, że w przypadku braku takiej mapy prezentowane tutaj rozwiązanie jest prostym sposobem sprostania wyzwaniom, jakie stawia dobrze wykonana analiza ryzyka II poziomu. Będzie ona oczywiście tym dokładniejsza, im więcej specyfik zostanie zidentyfikowanych w organizacji.

BIBLIOGRAFIA

Białas A., 2008, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa,

Byczkowski M., Marciniak P., 2000, *Metodyka TISM – Total Information Security Ma-nagement*, European Network Security Institute, Warszawa.

Molski M. Łacheta M., 2006, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice.

Shewhart W.A., 1931, *Economic control of quality of manufactured product* [w]: I. Grattan--Guinness (ed.), Landmark Writings in Western Mathematics (2005), 1640-1940, Chapter 72, Elsevier, str. 926-935, http://doi.org/10.1016/B978-044450871-3/50153-4.

Streszczenie

W pracy przedstawiono propozycję uwzględnienia specyfiki statystyki publicznej, jako istotnego warunku dobrze wykonanej analizy ryzyka grup informacji (II poziom) przy założeniu 3-poziomowej struktury modelu bezpieczeństwa informacji w krajowej organizacji statystycznej o strukturze korporacyjnej hierarchiczno-sieciowej. Model trójpoziomowej struktury modelu zarządzania bezpieczeństwem informacji został zaproponowany w metodyce TISM. Analizę ryzyka II poziomu można wykonać albo w oparciu o analizę zasobów organizacji, albo o analizę wszystkich procesów związanych z funkcjonowaniem organizacji w aspekcie jej bezpieczeństwa. W przypadku braku mapy procesów w organizacji, w jakimś stopniu niedoskonałym substytutem rozwiązania takiej sytuacji może być analiza poszczególnych specyfik funkcjonowania danej organizacji, która grupuje pewne procesy w ramach właściwości każdej z nich. W pracy zilustrowano wykorzystanie specyfik statystyki publicznej w analizie ryzyka II poziomu.

Słowa kluczowe: analiza ryzyka, bezpieczeństwo informacji, specyfika organizacji

Analysis of level II risk in a 3-layer hierarchical model of information security management, taking into account characteristics of public statistics

Summary

We present a proposal for including characteristics of public statistics as a precondition of validity for any level II risk analysis based on a 3-layered model of information security in a national statistic organization with hierarchical-networking corporate structure. 3-layered model is proposed using the TISM methodology. The risk analysis can be based on corporate resources or all business processes within the organization related to its security. In case of lack of a mapping of relationships between processes, there is a possibility of an imperfect substitute in the form of an analysis of specifics of organisational functions, which groups some processes by their characteristics. An example is given to illustrate utilization of the characteristics of public statistics in level II risk analysis.

Keywords: risk analysis, information security, organization characteristics

JEL: C10, C20, D80, H12