INCYDENTY ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI W ADMINISTRACJI PUBLICZNEJ W POLSCE

DOMINIKA LISIAK-FELICKA, MACIEJ SZMIT

Streszczenie

Liczba incydentów związanych z bezpieczeństwem informacji w administracji publicznej z roku na rok wzrasta. Według „Raportu o stanie bezpieczeństwa cyberprzestrzeni RP" w roku 2014 Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL) zarejestrował ponad trzydziestoprocentowy wzrost liczby zgłoszonych incydentów bezpieczeństwa.

W artykule przedstawiono analizę porównawczą danych o incydentach związanych z bezpieczeństwem informacji w Polsce (w oparciu o raporty zespołów CERT, raport NIK o cyberbezpieczeństwie Polski oraz badania własne autorów) oraz wybranych krajach Unii Europejskiej.

Słowa kluczowe: bezpieczeństwo informacji, systemy zarządzania bezpieczeństwem informacji, incydenty związane z bezpieczeństwem informacji

Wprowadzenie

Incydent związany z bezpieczeństwem informacji został zdefiniowany w normie ISO/IEC 27000:2014 (2.36) jako pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [8]. Takie incydenty zdarzają się we wszystkich organizacjach, również w jednostkach administracji publicznej. Istnieje kilka aktów prawnych, które zwracają szczególną uwagę na wymóg odpowiedniego zarządzania bezpieczeństwem informacji, w tym zarządzania incydentami związanymi z bezpieczeństwem informacji. Jednym z nich jest 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 (rozporządzenie KRI) [15]. Zgodnie z § 20 tego rozporządzenia, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie określonych działań wymienionych w rozporządzeniu. W zakresie incydentów związanych z bezpieczeństwem informacji powinny być podjęte działania m.in. poprzez bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Pojęcie incydentów związanych z bezpieczeństwem informacji pojawia się również w obowiązującej od 2013 r. „Polityce ochrony cyberprzestrzeni RP" [13], opracowanej przez Ministerstwo Administracji i Cyfryzacji oraz Agencję bezpieczeństwa Wewnętrznego. Ocena skuteczności „Polityki" będzie dokonywana na podstawie mierników bezpośrednio związanych ze zgłaszaniem

i obsługą incydentów (m.in. liczba zamkniętych incydentów w stosunku do ogólnej liczby sklasyfikowanych, liczba odpowiedzi na zgłoszenia, skrócenie czasu obsługi incydentu, średni czas odpowiedzi na niego).

1. Cel i metoda badawcza

Badanie ankietowe miało przede wszystkim cel poznawczy. Respondenci byli pytani o to, czy w przeszłości zdarzały się incydenty związane z bezpieczeństwem informacji, czy były one rejestrowane, ile incydentów zostało zarejestrowanych w roku 2012, 2013 i 2014, czy były one zgłaszane np. do CERT.GOV, prokuratury, itp., jak wygląda zarządzanie incydentami w badanych jednostkach oraz czy urzędy mogły liczyć na wsparcie w zakresie zarządzania incydentami związanymi z bezpieczeństwem informacji ze strony innych organów administracji publicznej. Zakres pytań w kwestionariuszu ankiety był szerszy, w niniejszym artykule prezentujemy tylko część wyników badań dotyczącą incydentów związanych z bezpieczeństwem informacji.

W ramach prac badawczych przeprowadzono analizę raportów CERT.GOV.PL oraz NIK, badanie ankietowe z wykorzystaniem kwestionariusza ankiety umieszczonego w Internecie oraz analizę raportów CERT z wybranych krajów Unii Europejskiej.

Badanie ankietowe przeprowadzono na próbie losowej 100 urzędów gmin (w tym gmin miejskich, gmin miejsko-wiejskich i gmin wiejskich).

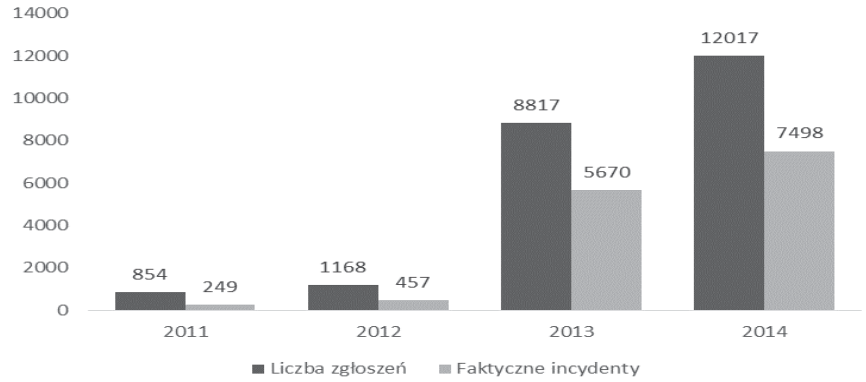
2. Wyniki badania

Informacji o liczbach incydentów związanych z bezpieczeństwem informacji w administracji publicznej dostarczają Raporty Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL).

2.1. Raporty Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL)

CERT.GOV.PL został powołany w celu zapewniania i rozwijania zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Głównym zadaniem cert.gov.pl jest koordynatorem procesu obsługi incydentów komputerowych w Cyberprzestrzeni RP (CRP).

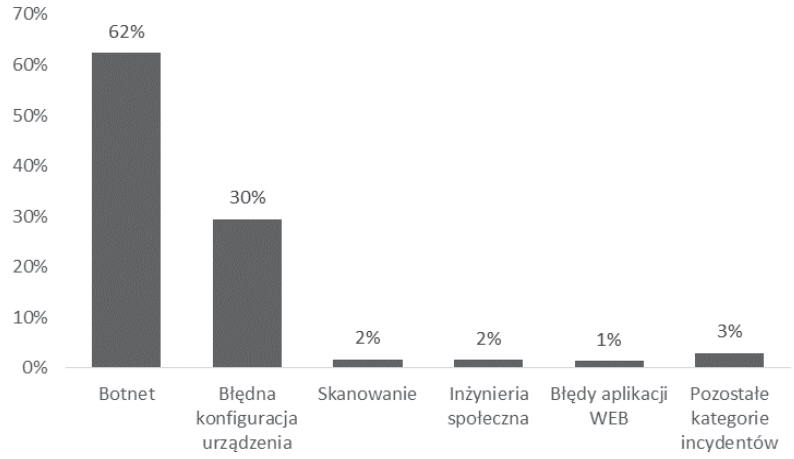
Liczba incydentów związanych z bezpieczeństwem informacji w administracji publicznej z roku na rok wzrasta. Według „Raportu o stanie bezpieczeństwa cyberprzestrzeni RP" w roku 2014 Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL) zarejestrował 12017 zgłoszeń, z których 7498 zostało zakwalifikowanych jako faktyczne incydenty. Dla porównania, w roku 2013 zarejestrowanych było 8817 zgłoszeń, z których 5670 uznano za rzeczywiste incydenty. Na rysunku 1 przedstawiono liczby zgłoszeń oraz faktycznych incydentów zarejestrowanych przez cert.gov.pl w latach 2011–2014 [16], [17], [18], [19].



Rysunek 1. Liczba zgłoszeń oraz faktycznych incydentów zarejestrowanych przez CERT.GOV.PL

Źródło: opracowanie własne na podstawie CERT.GOV.PL.

W 2014 roku najczęściej zgłaszanymi incydentami były botnety – 62% spośród wszystkich zgłoszonych incydentów. Następną grupę stanowiły zdarzenia związane z błędną konfiguracją urządzenia, a na trzecim miejscu – incydenty polegające na skanowaniu sieci. Na rysunku 2 wymieniono 5 kategorii incydentów, które były najczęściej zgłaszane do CERT.GOV.PL. Zgłoszenia dla pozostałych kategorii stanowiły 3% liczby wszystkich zgłoszeń.



Rysunek 2. Udział procentowy poszczególnych kategorii incydentów w zgłoszeniach zarejestrowanych przez CERT.GOV.PL

Źródło: opracowanie własne na podstawie CERT.GOV.PL.

Najwięcej zgłoszeń dotyczyło sieci botnet (4681 incydentów). Najczęściej występujące typy botnetów, które zostały wykryte w infrastrukturze administracji publicznej i zgłoszone do CERT.GOV.PL to Downadup, Conficker, B68_DNS, Zeus. W kolejnej kategorii (błędna konfiguracja urządzenia – tutaj uwzględniono również dane o podatnościach oraz błędach konfiguracji aplikacji, bądź urządzeń sieciowych) duży wpływ na statystyki miały dane o podatnościach serwerów DNS, NTP, a także protokołu SNMP (łącznie 2213 zgłoszeń). CERT.GOV.PL zarejestrował 132 zgłoszenia dotyczące skanowania sieci, 119 ataków inżynierii społecznej oraz 101 zgłoszeń wynikających z błędów aplikacji internetowych (webowych).

2.2. Raporty Najwyższej Izby Kontroli

Danych o sposobach zarządzania bezpieczeństwem informacji, w tym zarządzania incydentami dostarczają również raporty Najwyższej Izby Kontroli.

W 2014 roku NIK przeprowadził kontrolę „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" [14] w 25 jednostkach: 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.

Podczas kontroli NIK wykazał liczne nieprawidłowości i ogólnie negatywnie ocenił działania władz miast w zakresie zarządzania bezpieczeństwem informacji. Według danych z raportu pokontrolnego spośród 24 badanych jednostek w 21 stwierdzono nieprawidłowości w tym obszarze. Urzędy nie posiadały całościowej Polityki Bezpieczeństwa Informacji, niewłaściwie zarządzały uprawnieniami użytkowników, nie przeprowadzały corocznych audytów wewnętrznych bezpieczeństwa informacji i nie posiadały stosowanych umów na zakup lub serwis sprzętu/oprogramowania zawierających zapisy gwarantujące zapewnienie poufności przetwarzanych w nich danych. Zdaniem NIK nie realizowały zadań wynikających z §20 rozporządzenia KRI.

W zakresie zarządzania incydentami, o którym mówi §20 ust. 2 pkt 13 rozporządzenia KRI, spośród 24 urzędów, w 23 opracowano i wdrożono procedury opisujące zasady postępowania w przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji, jednak w 17 urzędach procedury te odnosiły się tylko do incydentów związanych z przetwarzaniem danych osobowych.

Inną kontrolę dotyczącą „Realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni" przeprowadzono w latach 2008–2014. Kontrolowane były następujące jednostki: Ministerstwo Administracji i Cyfryzacji, Ministerstwo Spraw Wewnętrznych, Agencję Bezpieczeństwa Wewnętrznego – Zespół CERT.GOV.PL, Ministerstwo Obrony Narodowej, Urząd Komunikacji Elektronicznej, Rządowe Centrum Bezpieczeństwa, Policję, Naukową i Akademicką Sieć Komputerową – Zespół CERT Polska [1]. Kontrolerzy NIK wykazali m.in. brak prowadzenia spójnych i systemowych działań związanych z ochroną cyberprzestrzeni RP oraz liczne problemy w realizacji zadań wynikających z potrzeby zapewnienia bezpieczeństwa cyberprzestrzeni, zapisanych między innymi w „Polityce Ochrony Cyberprzestrzeni RP". Wśród tych problemów wymieniono: „brak świadomości nowych zagrożeń u decydentów politycznych i kierownictwa administracji rządowej oraz brak zainteresowania kwestiami bezpieczeństwa IT ze strony najważniejszych osób w państwie, działania bez przygotowania i spójnej wizji systemowej, brak

ośrodka decyzyjnego i koordynacyjnego, rozproszenie kompetencji i brak współpracy instytucji państwowych, brak kompleksowych regulacji prawnych, niewykorzystywanie istniejących przepisów, przyjęcie podejścia polegającego na biernym oczekiwaniu na dyrektywę NIS, brak CERT'u narodowego oraz braki i wady Polityki Ochrony Cyberprzestrzeni RP" [1]. W odniesieniu do tematyki niniejszego artykułu kontrola wykazała w niektórych jednostkach brak:

- zdefiniowanych zasad i wymagań bezpieczeństwa informacji,
- kontroli systemów teleinformatycznych,
- kompleksowego systemu reagowania na incydenty komputerowe,
- ewidencjonowania incydentów,
- zespołu CERT,
- świadomości obowiązków w zakresie ochrony cyberprzestrzeni.

Wymienione informacje o kontrolach NIK potwierdzają, że jednostki administracji publicznej mają problemy w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa informacji i zarządzania incydentami związanymi z bezpieczeństwem informacji.

2.3. Wyniki badań własnych

Spośród 100 urzędów gmin, zaledwie w 14 incydenty miały miejsce, natomiast w 12 jednostkach były rejestrowane. Dane o incydentach, które zdarzały się w badanych urzędach gmin przedstawiono w tabeli 1. Należy podkreślić, że nie wszystkie urzędy gmin chciały udostępnić dane o liczbach zarejestrowanych incydentów.

Tabela 1. Incydenty związane z bezpieczeństwem informacji w badanych urzędach gmin

Gminy	Liczba urzędów, które rejestrowały incydenty	Liczba incydentów w 2012 r.	Liczba incydentów w 2013 r.	Liczba incydentów w 2014 r.
Miejskie	8	14	10	14
Miejsko-wiejskie	2	brak danych	1	8
Wiejskie	2	0	1	4
Razem	12	14	12	26

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Żaden z 12 urzędów gmin nie zgłaszał powyższych incydentów do CERT.GOV.PL czy prokuratury. Nie wszystkie urzędy podały informacje o sposobie zarządzania incydentami związanymi z bezpieczeństwem informacji. Poniżej zaprezentowano przykładowe odpowiedzi urzędów na to pytanie:

- „Pracownik przez wewnętrzny system zgłasza żądanie usługi lub incydent – zespół IT podejmuje działanie stosowne do zgłoszenia.
- Prowadzony jest rejestr incydentów. Powiadomiony jest o incydencie ADO, ABI, ASI. Zależnie od wagi incydentu są podejmowane kroki do jego wyjaśnienia.
- Zgłoszony incydent jest rozpatrywany i oceniany, czy jest niebezpieczny. Pracownik, który zawinił jest pouczany.
- Opracowano procedury by wyeliminować incydenty.
- Wykrycie, Badanie, Reakcja, Zalecenia, Monitoring.

- Instruktaż, weryfikacja procesów praktycznych, pouczenie.
- Monitoring systemu zabezpieczeń.
- Informacja o incydencie jest przekazywana przez pracownika bezpośredniemu przełożonemu i Administratorowi Bezpieczeństwa Informacji. Jest on zobowiązany przeprowadzić postępowanie wyjaśniające i o jego wynikach poinformować Administratora Danych.
- Sporządzenie notatki służbowej i przedstawienie jej kierownictwu wraz z zaleceniami.
- Zgodnie z Instrukcją zarządzania systemem informatycznym.
- 1. Zgłaszanie incydentów, 2. Zabezpieczenie danych, 3. Wyjaśnianie incydentu, 4. Działania naprawcze.
- Analiza wystąpienia błędu, skutki dla organizacji, zabezpieczenie ewentualnych dowodów, przeszkolenie pracownika, podjęcie działań naprawczych".

Urzędy, w których miały miejsce incydenty deklarują, że nie mogą liczyć na wsparcie ze strony innych organów administracji państwowej w zakresie zarządzania incydentami.

W poprzednich badaniach [9], [10], [11], [12] zebrano informacje o incydentach związanych z bezpieczeństwem informacji w urzędach marszałkowskich i urzędach wojewódzkich. Spośród 13 uzyskanych odpowiedzi z urzędów marszałkowskich w 7 urzędach pojawiały się i były rejestrowane incydenty związane z bezpieczeństwem informacji. W przypadku urzędów wojewódzkich z 11 odpowiedzi, incydenty miały miejsce i były rejestrowane w 5 jednostkach. Liczby incydentów w badanych urzędach kształtowały się od 0 do 15 w roku.

2.4. Incydenty związane z bezpieczeństwem informacji w wybranych krajach Unii Europejskiej

Dla porównania dokonano analizy incydentów bezpieczeństwa informacji w wybranych krajach Unii Europejskiej (Niemcy, Szwecja, Estonia, Hiszpania, Rumunia). Wyniki zestawiono w tabeli 2.

We wszystkich krajach można zauważyć wzrost zgłoszeń w 2014 roku w stosunku do ubiegłego roku. Niestety z uwagi na różny sposób opracowywania raportów przez narodowe zespoły CERT, nie można dokonać porównania wszystkich wskaźników.

Tabela 2. Incydenty związane z bezpieczeństwem informacji w wybranych krajach UE

Kraj	Nazwa CERT	Czy posiada strategię cyberbezpieczeństwa [2]	Dane o incydentach
Niemcy	CERT-Bund	Tak, od 2011 roku	Raport z 2014 roku: - 80% wzrost liczby zgłoszeń incydentów związanych ze spamem, - 36% wzrost w liczbie wiadomości e-mail, których załączniki zawierały złośliwe oprogramowanie, - milion ataków maleware w ciągu jednego miesiąca, - około milion komputerów jest częścią sieci botnet, - ponad 32 tys. ataków z kategorii DDoS [4].
Szwecja	CERT-SE	Nie	Dane z raportu KPMG z 2014 roku: - w Szwecji nie istnieją przepisy wymagające obowiązkowego zgłaszania incydentów, - najniższy stopień zainfekowania przez złośliwe oprogramowanie (wynosi on 19,98%) podczas gdy średnia światowa to 30,42%, - wśród rodzajów złośliwego oprogramowania, które zostało wykryte podczas badania najliczniejszą grupę stanowiły obiekty typu Botnet (41%) oraz Trojan (36%). Najmniej licznie reprezentowaną grupą są wirusy (3%) [6].
Estonia	CERT EE	Tak, od 2008 roku, jako jedno z pierwszych państw, nowelizacja w 2014 roku	Dane z raportu z 2014: - 1151 incydentów zarejestrowanych w 2014 roku, w tym 22 typu DoS, - znaczący wzrost incydentów w instytucjach rządowych, w 2014 zarejestrowano 486 incydentów, 135 w 2013 r., - największą grupę stanowiły incydenty o priorytecie niskim i średnim, odpowiednio 34% i 31% wszystkich incydentów zgłaszanych przez instytucje rządowe [7].
Hiszpania	INTECO-CERT i CCN-CERT	Tak, od 2013 roku	Dane z 2014 roku z CNN-CERT: - zarejestrowano 12916 incydentów w roku 2014, (7263 w 2013 r.), - największą grupę stanowiły zgłoszenia o złośliwym oprogramowaniu – 10137, kolejna kategoria: włamanie – 2153 zgłoszeń, - najliczniej rejestrowane były ataki o priorytecie wysokim - 79% [5].
Rumunia	CERT-RO	Tak, od 2013 roku	Dane z 2014 roku z CERT-RO: - liczba alertów: 78769993, (43231149 w 2013 r.), - najczęściej występującą kategorią incydentów były te wykorzystujące słabości systemu/sieci (53,5%), następnie sieci botnet (45,3%), bezprawne uzyskanie informacji (0,6%), złośliwe oprogramowanie (0,4%) i cyberataki (0,2%) [3].

Źródło: opracowanie własne na podstawie danych CERT z wybranych krajów UE.

3. Podsumowanie

Po raz kolejny (tym razem w przypadku urzędów gmin) wykazano, że w większości urzędy administracji publicznej nie rejestrują incydentów związanych z bezpieczeństwem informacji. A te urzędy, które prowadzą dokumentację, wykazują w raportach bardzo małe liczby incydentów. W odniesieniu do wyników dla urzędów gmin, zaledwie 12 urzędów ze 100 dokonywało rejestracji zdarzeń, w sumie przez trzy lata w 12 urzędach wystąpiły 52 incydenty. Wynikać to może z kilku przyczyn:

- urzędy rejestrują tylko najpoważniejsze zdarzenia,
- urzędy nie chcą udostępnić informacji o rzeczywistej liczbie incydentów,
- urzędy administracji samorządowej (zwłaszcza te mniejsze) nie są narażone aż na tak wiele ataków co urzędy administracji rządowej.

Analiza danych z poszczególnych urzędów gmin nie wskazuje również tendencji wzrostowej, przy ogólnym wzroście liczby incydentów związanych z bezpieczeństwem informacji wykazywanym w raportach Rządowego Zespołu Reagowania na Incydenty Komputerowe.

Na podstawie udzielonych odpowiedzi można zauważyć, że większość urzędów nie zarządza incydentami we właściwy sposób. Niektóre badane jednostki obsługują tylko incydenty związane z bezpieczeństwem danych osobowych. Urzędy, które nie posiadają wdrożonego systemu zarządzania incydentami powinny jak najszybciej podjąć takie działania, by móc prawidłowo obsługiwać pojawiające się w przyszłości zdarzenia.

Pomimo, że liczba incydentów była stosunkowo niewielka, występowały problemy z prawidłowym reagowaniem i procesem zarządzania nimi.

Potwierdzają to raporty NIK, według których w wielu jednostkach nie ma wdrożonego kompleksowego systemu reagowania na incydenty komputerowe, nie ma zespołów CERT, a incydenty nie są rejestrowane. Jednym z postulatów NIK jest opracowanie procedur dotyczących zgłaszania incydentów nie tylko związanych z zagrożeniem danych osobowych, ale również innych danych przetwarzanych w urzędach. Taką sytuację potwierdzają również wyniki badań – w wielu badanych jednostkach obsługiwane są incydenty związane tylko z ochroną danych osobowych.

Tendencję wzrostową liczby incydentów można zauważyć nie tylko w Polsce, ale również w krajach Unii Europejskiej, między innymi w analizowanych w ramach niniejszego artykułu państwach: Niemcy, Hiszpania, Estonia, Rumunia i Szwecja. W krajach UE występują również problemy w zakresie zarządzania incydentami wynikające z braku wdrożenia np. strategii cyberbezpieczeństwa (np. Szwecja, Bułgaria, Chorwacja, Dania, Irlandia). Analizę porównawczą danych dla Unii Europejskiej utrudnia fakt, że nie wszystkie państwa posiadają obowiązek rejestrowania incydentów (np. Szwecja, Irlandia). Z drugiej strony nie ma jednakowych szablonów raportów i klasyfikacji incydentów, co utrudnia analizę porównawczą danych z państw, które takie raporty sporządzają.

W ramach dalszych prac badawczych przewidziane jest badanie dotyczące sposobów zarządzania bezpieczeństwem informacji w pozostałych jednostkach administracji publicznej.

Bibliografia

[1] Bieńkowski M., dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego NIK, Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni, Wstępne Wyniki Kontroli, Warszawa, 26.11.2014 r. Materiały konferencyjne Security Case Study 2014.
[2] http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf [2015-06-21].
[3] http://www.cert-ro.eu/files/doc/915_20150325000331012990800_X.pdf [2015-06-21].
[4] https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html [2015-06-21].
[5] https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf [2015-06-21].
[6] https://www.kpmg.com/SE/sv/kunskap-utbildning/nyheter-publikationer/Publikationer-2014/Documents/Study-report-UnknownThreats-in-Sweden.pdf [2015-06-21].
[7] https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf [2015-06-21].
[8] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary.
[9] Lisiak-Felicka D., Szmit M., *Information Security Management Systems In Marshal Offices In Poland*, „Information Systems In Management", vol. 3(2)/2014, pp. 134–144.
[10] Lisiak-Felicka D., Szmit M., *Selected Apects of Information Security Management in Voivodeship Office in Poland*, „Securitologia" 2(20)/2014 pp. 55–69.
[11] Lisiak-Felicka D., Szmit M., W*ybrane aspekty zarządzania bezpieczeństwem informacji w urzędach marszałkowskich*, Securitologia 2/2013, pp.39–53.
[12] Lisiak-Felicka D., Szmit M.: *Information security incidents management in marshal offices and voivodeship offices in Poland*, Studies & Proceedings of Polish Associacion for Knowledge Management, Volume 72, Bydgoszcz 2014, pp. 28–38,
[13] Ministerstwo Administracji i Cyfryzacji, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.
[14] NIK, Informacja o wynikach kontroli: 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, luty 2015, https://www.nik.gov.pl/kontrole/P/14/004/ [2015-06-16].
[15] 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. 2012 poz. 526.
[16] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 r.*, Warszawa 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [2015-06-16].
[17] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, Warszawa 2014,

http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html [2015-06-16].

[18] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, Warszawa 2013, http://www.cert.gov.pl/portal/cer/57/605/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2012_roku.html [2015-06-16].

[19] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, Warszawa 2012, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/549,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2011-roku.html [2015-06-16].

INFORMATION SECURITY INCIDENTS IN PUBLIC ADMINISTRATION IN POLAND

Summary

The number of information security incidents in public administration increases from year to year. According to the "Report of Polish cyberspace security status" in the year 2014, The Governmental Computer Security Incident Response Team (CERT.GOV.PL) registered over 30 percent increase in the number of notified information security incidents.

The article presents a comparative analysis of information security incidents in Poland (based on CERTs reports, Supreme Audit Office cyber security reports and research conducted by authors) and selected EU countries.

Keywords: information security, information security management systems, information security incidents

Dominika Lisiak-Felicka
Katedra Informatyki Ekonomicznej
Wydział Ekonomiczno-Socjologiczny
Uniwersytet Łódzki
e-mail: dominika.lisiak@gmail.com

Maciej Szmit
Orange Labs Poland
e-mail: maciej.szmit@gmail.com