ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 874 STUDIA INFORMATICA NR 37 2015
DOI: 10.18276/si.2015.37-07

Ireneusz Miciuła*
Krzysztof Miciuła
Uniwersytet Szczeciński

KORZYSTANIE Z USŁUG E-ADMINISTRACJI A SPOSOBY ZAPEWNIENIA BEZPIECZEŃSTWA DLA INFORMACJI WRAŻLIWYCH W PAŃSTWACH UNII EUROPEJSKIEJ

Streszczenie

Artykuł prezentuje ilościową analizę korzystania z usług e-administracji w Polsce na tle państw członkowskich UE oraz czynniki wpływające na hamowanie jego rozwoju. Do elementów ograniczających rozwój społeczeństwa informacyjnego i e-usług organizacji publicznych niewątpliwie należy bezpieczeństwo informacji wrażliwych. Dlatego w artykule przedstawiono sposoby zabezpieczania informacji wrażliwych w ramach polityk prowadzonych przez państwa UE oraz kierunki rozwoju e-administracji.

Słowa kluczowe: społeczeństwo informacyjne, informacja wrażliwa, bezpieczeństwo informacji

* irekmic@wneiz.pl.

Wprowadzenie

Niemal każda innowacja niesie za sobą postęp, ułatwiający życie ludziom i funkcjonowanie przedsiębiorstwom. W przypadku Internetu jest to łatwy dostęp do zbioru danych i informacji oraz szybki i bezpośredni kontakt z różnymi instytucjami gospodarczymi i społecznymi. W rezultacie to także możliwość prowadzenia części lub całości działalności gospodarczej w Internecie. Jednak mimo wielu zalet i szans taka organizacja życia gospodarczego i społecznego w przestrzeni wirtualnej posiada także zagrożenia. Jedną z nich są próby wykorzystania niepożądanego dostępu do informacji wrażliwych. Celem ataków są najczęściej strony internetowe instytucji publicznych lub prywatnych przedsiębiorstw. Łamanie systemów bezpieczeństwa następuje przez wykorzystanie wielu narzędzi, m.in. programów szpiegujących (np. trojan, wirus), oraz metod podszywania się pod uprawnioną osobę lub instytucję w celu wyłudzenia poufnych informacji, takich jak hasła lub szczegóły dotyczące karty kredytowej (tzw. *phishing*). Wśród internautów coraz popularniejsze jest zjawisko samoodsłaniania się w Internecie (prnews.pl/aktualnosci/socjotechnika-w-sluzbie-kradziezy-danych.html, 20.02.2015). Polega ono na udostępnianiu poufnych informacji, bardziej lub mniej świadomie, czy to przez odpowiedzi na fałszywe e-maile, np. wzywające do zapłaty, czy też wpisywanie danych na fałszywych stronach internetowych. Dlatego każda instytucja i organizacja powinna prowadzić politykę bezpieczeństwa, pozwalającą na redukcję ryzyka utraty wrażliwych informacji. Takie działania wymiernie przekładają się na większą stabilność prowadzenia organizacji i zaufanie klientów. Rewolucja związana z wprowadzeniem nowoczesnych technologii informatycznych daje się porównać z rewolucją przemysłową w sferze środków produkcji. Gospodarka elektroniczna wpływa na każdą dziedzinę życia społeczno-gospodarczego i modernizuje tradycyjną działalność przez stosowanie ICT we wszystkich gałęziach gospodarki. Rewolucja internetowa sprawiła, że ochrona prywatności jest tematem niezwykle aktualnym. Szczególnie niebezpieczne wydają się zagrożenia związane z kradzieżą poufnych danych i tożsamości. Takie działanie stwarza zagrożenie dla prywatności, a nawet osobistego bezpieczeństwa. Ma to szczególne znaczenie z uwagi na niezamierzone skutki coraz częstszego odsłaniania się ludzi w sieci, jak i szybkiego wzrostu poziomu zaawansowania metod łamania zabezpieczeń. Dla większego bezpieczeństwa przed tymi zagrożeniami następuje upowszechnianie metod autoryzacji biometrycznej. Dzisiejsza rzeczywistość to czasy komunikacji internetowej, które

pomimo nieocenionych zalet i nowych możliwości niosą również za sobą wiele zagrożeń. Dlatego nie sposób pominąć pojęcia ochrony informacji wrażliwych, czyli prawnie chronionych, a więc istotnych z punktu widzenia interesów majątkowych, oraz tych, które nie wchodzą do zakresu informacji, a stanowią element wiedzy ogólnej (www.iniejawna.pl/pomoce/ela.html, 11.03.2015). Celem artykułu jest analiza korzystania z usług e-administracji w Polsce na tle państw członkowskich UE oraz ukazanie perspektyw rozwoju. Do elementów ograniczających dalszy rozwój społeczeństwa informacyjnego i e-usług organizacji publicznych niewątpliwie należy bezpieczeństwo informacji wrażliwych. Dlatego w dalszej części pracy przedstawiono sposoby zabezpieczania informacji wrażliwych w ramach polityk prowadzonych przez państwa UE.

1. Korzystanie z usług e-administracji i perspektywy rozwoju

Powstanie systemu ekonomicznego opartego na gospodarce elektronicznej jest nie tylko problemem technicznym, ale zagadnieniem dotyczącym organizacji, zarządzania czy stworzenia odpowiedniego środowiska gospodarczego. Nie jest to kwestia mody związanej z pojawieniem się nowych technik i wykorzystywaniem technologii teleinformatycznych, lecz raczej kwestia zrozumienia, że są to narzędzia, które pojawiły się wskutek przeobrażeń w funkcjonowaniu gospodarki. Pojawienie się Internetu oraz globalizacja gospodarki tworzą szansę dla poszerzenia aktywności na rynku. Powoduje to wyrównanie szans w dostępie do informacji, zdobywaniu zamówień i konkurowaniu. Wiedza i technologia występują jako podstawowe czynniki dynamizujące rozwój społeczno-gospodarczy. Kluczowe znaczenie dla rozwoju zyskał kapitał intelektualny, stając się głównym czynnikiem sukcesu i wpływając na transformację otoczenia i coraz silniejszą konkurencję. Wdrożenie technologii informatycznych i posiadanie wykwalifikowanej kadry intensyfikuje aktywność organizacji, wpływając na zdolność do działania w wirtualnej przestrzeni, będącej elementem elektronicznej gospodarki (Dudek, 2011, s. 4). Jednocześnie nowe technologie to także czynnik destabilizujący otoczenie organizacji i konieczność przystosowania się do zmian.

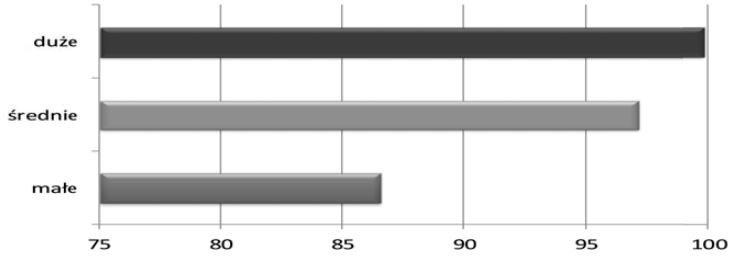
W dobie społeczeństwa informacyjnego, w której informacja jest traktowana jako szczególne dobro niematerialne, niejednokrotnie cenniejsze od dóbr materialnych, e-gospodarka udostępnia niezastąpione narzędzia wspomagające procesy funkcjonowania organizacji. W gospodarce elektronicznej istotną rolę

odgrywają kompetencje związane z wykorzystaniem różnych narzędzi informatycznych. Bez nich niemożliwe jest dziś efektywne kierowanie firmami, funkcjonowanie sprawnej administracji publicznej oraz prowadzenie współpracy na arenie międzynarodowej. Dynamiczny rozwój społeczeństwa informacyjnego oraz rosnące zapotrzebowanie na coraz lepszą jakość usług i produktów ICT stały się przyczyną powszechnego rozwoju gospodarki elektronicznej w różnych dziedzinach życia. Jednym z istotnych aspektów jest korzystanie z e-administracji, wspierającej UE, co uwidacznia się w jej celach, aby na koniec 2015 roku połowa obywateli UE i ok. 80% przedsiębiorstw korzystało z tej formy gospodarki elektronicznej. Obecnie określa się, że 42% obywateli UE korzysta z usług administracji elektronicznej. W najbardziej zaawansowanych pod tym względem krajach odsetek obywateli korzystających z e-administracji wynosi ponad 60%, a należą do nich Dania, Wielka Brytania, Szwecja i Finlandia. Dodatkowo z badań ankietowych obywateli UE wynika, że 80% obywateli twierdzi, że usługi publiczne on-line pozwalają zaoszczędzić czas, 76% docenia ich wygodę i elastyczność, a 62% uważa, że dzięki nim wydaje mniej pieniędzy. Jednocześnie należy zwrócić uwagę, iż dalszą ekspansję hamują m.in. obawy o zachowanie prywatności obywateli. Kontrowersje wywołują plany digitalizacji prywatnych zapisków lekarskich o pacjentach i powstawanie różnorodnych kolejnych baz danych (prawo.rp.pl/artykul/1035898.html, 5.04.2015). Dlatego dla dalszego rozwoju e-gospodarki, a w tym e-administracji, niezbędne są strategie zabezpieczania i w ten sposób przeciwdziałanie wyciekowi informacji wrażliwych.

W Polsce wydatki na technologie informacyjne w 2014 roku stanowiły 2,2% PKB, a średnio w UE-25 wnoszą 3,2% (najwięcej – ponad 4% – w Szwecji i Wielkiej Brytanii). Warunkiem koniecznym, choć niewystarczającym, budowy społeczeństwa informacyjnego, a tym samym również osiągnięcia celów spójności, jest upowszechnienie dostępu do Internetu. W przedsiębiorstwach poziom ten jest zadowalający i podstawowe wskaźniki nie odbiegają od średnich UE. Należy też podkreślić szybkie tempo nadrabiania zaległości w tym zakresie w gospodarstwach domowych. Natomiast poprawy wymaga poziom zaawansowania rozwoju e-usług publicznych w Polsce, który wynosi 35% (wśród krajów UE-25 – 68%). Poziom pełnej interaktywności usług publicznych on-line kształtuje się na poziomie 19% (w UE – 42%). Najwyższym wskaźnikiem rozwoju e-usług publicznych dla obywateli charakteryzują się takie usługi, jak: poszukiwanie pracy (74%), podatek dochodowy od osób fizycznych (50%), rejestracja na wyż-

sze uczelnie (36%), a najniższym służba zdrowia (2%) i rejestracja zgłoszeń na policję (2%).

Dużego znaczenia w gospodarce nabiera sektor usług, który systematycznie się rozwija. W 2014 roku jego udział w tworzeniu wartości dodanej brutto wyniósł 64,5%, wobec przeciętnej 69,7% w UE. Jednocześnie dynamicznie rośnie zatrudnienie w usługach. Na ten stan rzeczy duży wpływ ma gospodarka elektroniczna, która tworzy wiele miejsc pracy w usługach. W 2014 roku obejmowało ono 59,8% pracujących ogółem (CapGemini, 2014). Ocenia się, że w usługach istnieje możliwość tworzenia znacznych ilości miejsc pracy. Jednocześnie mając na uwadze nadal niskie koszty pracy w naszym kraju, jak również znaczne zasoby młodych wykształconych kadr, Polska może być miejscem lokowania przez inwestorów zagranicznych swoich ośrodków usługowych, obsługujących firmy i całe koncerny. Przykładem takich usług mogą być już istniejące centra usługowe z zakresu księgowości, informatyki itp. Członkostwo Polski w UE daje również szanse na zwiększenie eksportu polskich usług do krajów UE. Istotne znaczenie będzie mieć upowszechnianie dostępu do usług elektronicznych. Działania inwestycyjne powinny objąć zarówno usługi i bazy informatyczne administracji centralnej i terytorialnej, jak i rozwój komercyjnych sieci i usług elektronicznych.



Wykres 1. Przedsiębiorstwa korzystające z e-administracji w 2013 roku
Źródło: GUS, październik 2014.

Korzystanie z e-administracji zapewnia przedsiębiorcom oszczędność czasu poprzez możliwość wypełniania i odsyłania dokumentów drogą on-line. Pozwala też na bieżące śledzenie zmian w przepisach i aktach prawnych umieszczanych na stronach instytucji publicznych. Z e-administracji w 2014 roku korzystało 91% przedsiębiorstw, przy czym tę formę kontaktu z administracją publiczną stosowały prawie wszystkie firmy duże (99,7%) oraz 97% przedsiębiorstw średnich

i 86,4% przedsiębiorstw małych. Przedsiębiorstwa korzystają z e-administracji w celach pozyskania informacji, pobierania i przesyłania wypełnionych formularzy oraz dla uzyskania dokumentów przetargowych, w tym specyfikacji w elektronicznym systemie zamówień publicznych (egospodarka.pl, 15.01.2015).

W rankingu najlepiej przystosowanych krajów do ery nowych technologii Polska znalazła się na 32. miejscu na 65 badanych państw (Economist Intelligence Unit, 2013). Do mocnych stron polskiej branży ICT zaliczamy:

- kapitał intelektualny (pracownicy – informatycy, szczególnie programiści), który bardzo intensywnie rozwija się także na rynkach zagranicznych,
- kompleksowe rozwiązania (połączenie sprzętu, oprogramowania, a także usług i wsparcia kompetencyjnego. Dają one wyraźny efekt biznesowy – albo poprzez ograniczenie kosztów, albo poprzez wzrost zysków),
- usługi outsourcingowe po niższych cenach niż w państwach zachodnich UE,
- złożone innowacyjne usługi informatyczne, takie jak rozwiązania w chmurze,
- bardzo dynamicznie rozwijający się sektor producentów gier,
- świetne rozwiązania klasy biznesowej – bardzo dużo produkuje się w Polsce rozwiązań mobilnych wspierających sprzedaż.

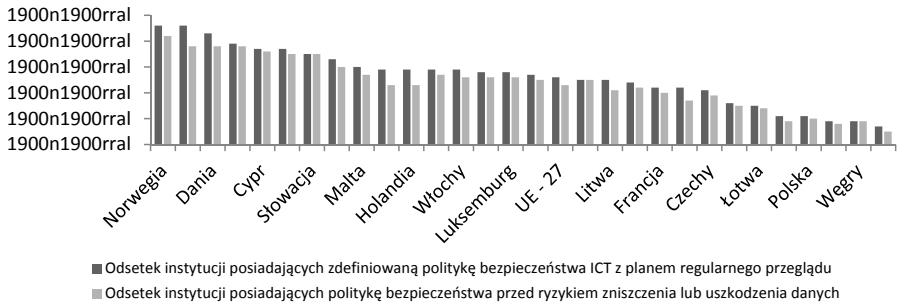
W XXI wieku Polska staje przed ogromem wyzwań natury społecznej i technologicznej. Od sprostania im zależy powodzenie strategicznego rozwoju naszego kraju, zapewnienie materialnego dobrobytu polskich rodzin, umocnienie ich samodzielności ekonomicznej oraz poczucia bezpieczeństwa. Kluczowym zadaniem dla Polski jest włączenie się w proces budowy ery informacyjnej poprzez wykorzystanie nowoczesnych technik teleinformatycznych, stwarzanie warunków do bezpośredniego dostępu do informacji, kształtowanie świadomości społeczeństwa oraz rozwijanie jego potencjału intelektualnego i gospodarczego. W celu dostosowania polskich rozwiązań i standardów ekonomiczno-społecznych do kształtującego się nowoczesnego społeczeństwa informacyjnego należy:

- zwiększyć zakres usług dostępnych w e-administracji do poziomu średniej państw UE-27,
- dostosować gospodarkę narodową do wymagań globalnej gospodarki elektronicznej poprzez wprowadzenie odpowiednich regulacji prawnych, ułatwiających i obniżających koszty dostępu do technologii informacyjnej,

- przygotować społeczeństwo polskie do wyzwań nowego rynku pracy i nowych metod pracy, czyli wspierać rozwój kapitału ludzkiego,
- promować procesy związane z rozwojem wartości kapitału intelektualnego,
- stworzyć przejrzyste zasady działania administracji publicznej na miarę otwartego społeczeństwa informacyjnego za pomocą narzędzi teleinformatycznych,
- stworzyć warunki dla trwałego i zrównoważonego rozwoju regionalnego z uwzględnieniem nowoczesnych technik teleinformatycznych przez dalsze inwestycje w infrastrukturę informacyjną, którą cechuje szybka zmienność technologiczna,
- zadbać o rozwój nowoczesnych gałęzi przemysłu i wzrost ich innowacyjności w celu poprawy konkurencyjności polskiej gospodarki,
- szerzej korzystać z programów UE w celu pozyskiwania środków finansowych na projekty informatyczne (w roku 2013 w sektorze MSP odsetek był niewielki i wynosił odpowiednio 4% i 13%),
- zapewnić wsparcie dla gospodarki elektronicznej przez zaplecze naukowe w celu lepszego wykorzystania szans, jakie oferuje model społeczeństwa informacyjnego.

2. Sposoby zabezpieczenia informacji wrażliwych w państwach UE

Zagrożenia naszej prywatności determinują rozwój rozwiązań technicznych mających za zadanie jej ochronę. Według Komisji Europejskiej w grudniu 2013 roku 27% instytucji w UE-27 miało zdefiniowaną politykę bezpieczeństwa ICT z planem regularnego przeglądu. Na wykresie 2 przedstawiono odsetek instytucji w poszczególnych państwach, które posiadają zdefiniowaną politykę bezpieczeństwa dotyczącą ataków internetowych z planem regularnego przeglądu. Największy odsetek instytucji z określoną polityką bezpieczeństwa odnotowano w Szwecji i Norwegii – po 46% oraz Danii – 43%. Najniższy odsetek instytucji, poniżej 10%, jest w Rumunii, Bułgarii i na Węgrzech. Sytuacja w Polsce nie jest lepsza, gdyż z odsetkiem 11% zajmujemy w rankingu wraz z Estonią czwarte miejsce od końca. Największy odsetek organizacji posiadających zdefiniowaną politykę bezpieczeństwa dotyczącą ryzyka zniszczenia i uszkodzenia danych notowany jest w Norwegii (42%). W przypadku Polski był on 4 razy niższy (10%), co dało nam piąte miejsce od końca.



Wykres 2. Odsetek instytucji w państwach UE, które posiadają formalnie zdefiniowaną politykę bezpieczeństwa ICT

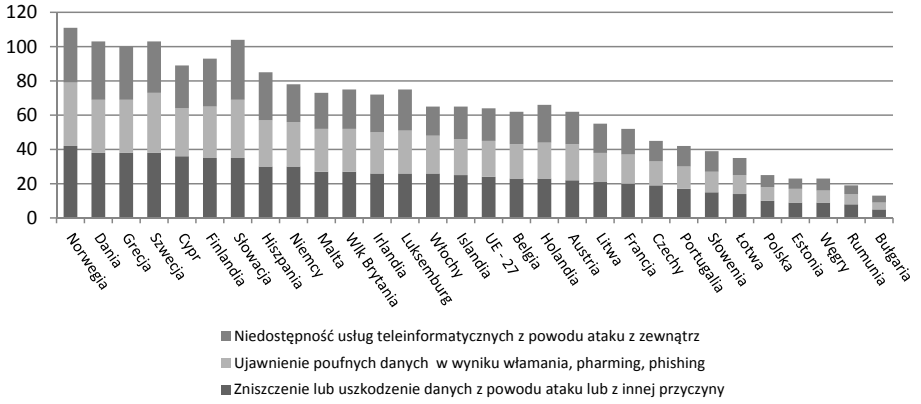
Źródło: Eurostat, grudzień 2014.

Zgodnie z raportem Eurostatu instytucje w krajach UE przyjmują różne podejścia mające na celu podniesienie świadomości swoich pracowników na temat polityki bezpieczeństwa teleinformatycznego i zagrożeń, którym ma ona zapobiegać. Warto tu przybliżyć 3 podejścia podejmowane przez organizacje:

1. Dobrowolne szkolenia lub ogólnie dostępne informacje.
2. Kształtowanie świadomości swoich obowiązków w odniesieniu do bezpieczeństwa ICT na mocy np. umowy o pracę.
3. Obowiązkowe szkolenia lub prezentacje mające na celu podnoszenie świadomości na temat polityki bezpieczeństwa teleinformatycznego i odpowiedniego rodzaju ryzyka.

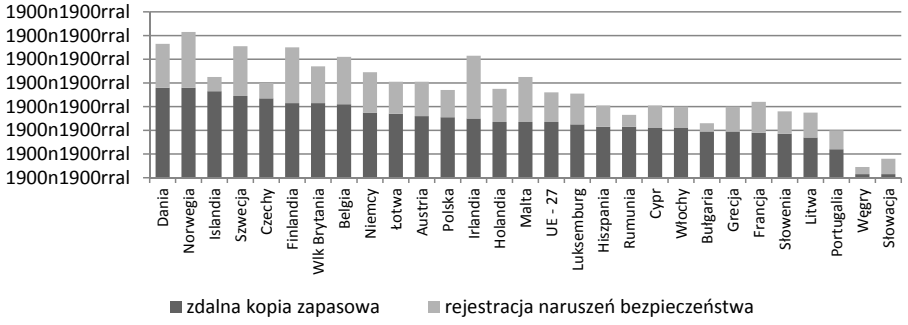
Podejścia te różnią się metodami podnoszenia świadomości pracowników na temat bezpieczeństwa teleinformatycznego i zagrożeń, którym mają przeciwdziałać. Zgodnie z raportem Eurostatu instytucje i ich pracownicy najczęściej korzystali z dobrowolnych szkoleń lub wykorzystywali ogólnie dostępne informacje. Liderem korzystania z tej formy pozyskiwania wiedzy są przedsiębiorcy z Cypru i Finlandii (odpowiednio 77 % i 74%). W Polsce odsetek ten wynosił 11%. Drugie podejście do budowania wiedzy o bezpieczeństwie teleinformatycznym oparte jest na świadomości własnej w odniesieniu do bezpieczeństwa ICT w trakcie swoich obowiązków pracowniczych w ramach umowy prawnej (np. umowy o pracę). Odsetek przedsiębiorstw propagujących takie podejście był najwyższy w Norwegii i Irlandii (odpowiednio 42% i 41%). W Polsce odsetek ten wynosił 9%. Z kolei Włochy były państwem, które miało najwyższy odsetek przedsiębiorstw realizujących trzecie podejście, czyli obowiązkowe szkolenia

lub prezentacje (39%). Kolejnymi państwami są Norwegia i Słowacja, z odsetkiem odpowiednio 37% i 33%. W Polsce odsetek ten wyniósł 8%, co świadczy o znikomym stosowaniu wymienionych form podnoszenia świadomości swoich pracowników na temat polityki bezpieczeństwa teleinformatycznego.



Wykres 3. Udział instytucji ze zdefiniowaną polityką bezpieczeństwa według typów ryzyka z podziałem na państwa członkowskie UE (w %)

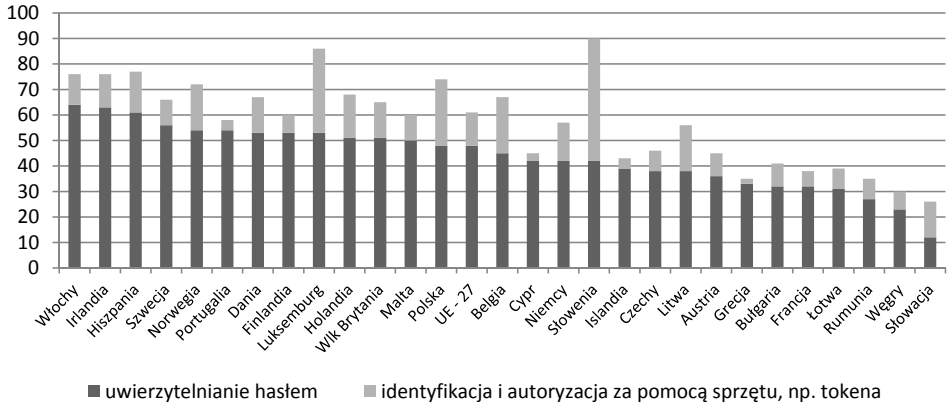
Źródło: Eurostat, grudzień 2014.



Wykres 4. Odsetek instytucji stosujący zdalną kopię zapasową i rejestrację zdarzeń dla analizy incydentów naruszających bezpieczeństwo ze względu na kraj (uporządkowany wg zmiennej „zdalna kopia zapasowa")

Źródło: Eurostat, grudzień 2014.

W czasie procesu ochrony zasobów instytucji niezmiernie ważne są wewnętrzne procedury bezpieczeństwa (Schetina, Green, Carlson, 2002). Najczęściej stosowanymi metodami w wewnętrznej procedurze są tworzenie zdalnej kopii zapasowej danych i silne uwierzytelnianie hasłami. Metodami służącymi zabezpieczeniu zasobów jest tworzenie kopii zapasowej poza siedzibą, czyli zdalnej kopii zapasowej, i rejestracja naruszeń bezpieczeństwa. Najwyższy odsetek instytucji korzystających z przygotowywania zdalnej kopii zapasowej odnotowano w Danii i Norwegii – 76%, a następnie w Islandii – 73% i Szwecji – 69%. Polska, z wynikiem 51%, znajduje się w środku rankingu.



Wykres 5. Odsetek instytucji publicznych i prywatnych stosujący metody identyfikacji i uwierzytelniania ze względu na kraj (uporządkowany wg zmiennej „uwierzytelnianie hasłem")

Źródło: Eurostat, grudzień 2014.

Proces identyfikacji jest uzupełniany procedurami uwierzytelniania. Dzięki nim można zarządzać dostępem (uprawnieniami) do informacji wrażliwych w instytucjach publicznych i przedsiębiorstwach prywatnych. Najwyższy odsetek instytucji publicznych i prywatnych, które stosowały uwierzytelnianie hasłami jako wewnętrzną procedurę, odnotowano w następujących państwach: Włochy – 64%, Irlandia – 63% i Hiszpania – 61%. W Polsce wskaźnik ten wynosił 48%. Wynik dla Polski jest również średnią UE-27. Najwyższy odsetek instytucji publicznych i przedsiębiorstw prywatnych, które wykorzystują metodę identyfikacji i autoryzacji użytkownika za pomocą sprzętu (np. tokeny), zanotowano w Słowenii (48%), Luksemburgu (33%) i Polsce (26%). Są to zaskakujące

wyniki na tle państw UE, ale należy zwrócić uwagę, że wyniki tego badania dotyczą zarówno instytucji publicznych, jak i przedsiębiorstw prywatnych, np. banków, które szeroko stosują nowoczesne metody autoryzacji. Natomiast niewątpliwie wynik Polski w tym zestawieniu należy określić jako niespodziewanie pozytywny. Jedynie szkoda, że nie podano danych, które ukazują, jaki jest udział w tym wyniku instytucji publicznych.

Do najczęściej używanych praktycznych metod zabezpieczenia zasobów informatycznych przed zagrożeniami typu złośliwe ataki, wirusy i robaki z Internetu zaliczamy programy antywirusowe, oprogramowanie zabezpieczające przed programami szpiegującymi i zapory. W przypadku poczty internetowej wykorzystuje się filtr antyspamowy oraz oprogramowanie wykrywające niebezpieczne elementy w e-mailach. Obecnie dostępne są pakiety bezpieczeństwa posiadające programy dostarczające wszystkie te możliwości w jednym. Dzięki ulepszaniu zabezpieczeń w najnowszych pakietach bezpieczeństwa, oprócz podstawowych programów, mamy dodatkowe usługi mające zagwarantować nam bezpieczeństwo, na przykład przy połączeniach z bankowością elektroniczną oraz sklepami internetowymi. W raportach Eurostatu można odnaleźć ogólne zalecenia i procedury, które powinny stosować w celu dbania o bezpieczeństwo informacji wrażliwych zarówno instytucje publiczne odpowiedzialne za e-administrację, jak i przedsiębiorstwa prywatne. Zaliczamy do nich:

- instalowanie oprogramowania antywirusowego wraz z aktualizacjami,
- stosowanie programowej i sprzętowej zapory sieciowej (*firewall*),
- korzystanie z aktualizacji systemu i przeglądarek internetowych,
- przeprowadzanie regularnego skanowania systemu,
- szyfrowaną transmisję danych, np. przy płatnościach drogą elektroniczną,
- instalowanie programów prewencyjnych (do wykrywania i zapobiegania włamaniom),
- używanie oryginalnego systemu i aplikacji, które pochodzą z zaufanego źródła,
- stosowanie metod autoryzacji i uwierzytelniania,
- dokonywanie regularnych kopii zapasowych,
- prowadzenie szkoleń podnoszących świadomość pracowników na temat bezpieczeństwa w Internecie.

Podsumowanie

Aktualnie uczestniczymy w gospodarce informacyjnej, czyli poprzez używanie nowoczesnych technik ICT korzystamy z bezpośredniego dostępu do informacji. Światowa gospodarka jest w fazie globalizacji opartej na zaawansowanych technologiach, co wymusza coraz większe znaczenie i wartość kapitału intelektualnego. Dlatego oprócz odpowiedniego zabezpieczania danych i informacji, które zminimalizują ryzyko nieprawnego wykorzystania informacji wrażliwych, instytucje powinny określić poziomy ryzyka dla wszystkich krytycznych informacji. Organizacje powinny aktywnie opracowywać całościowy, strategiczny plan zabezpieczenia, włączając w to politykę bezpieczeństwa, opracowane procedury oraz wdrażane technologie, które integrują aplikacje i procesy przy jednoczesnym zachowaniu zgodności z wymogami bezpieczeństwa oraz odpowiednimi przepisami i regulacjami. Trzeba pamiętać, że techniczne zabezpieczenia nie zapewniają całkowitej ochrony. W wielu przypadkach największym zagrożeniem jest sam użytkownik. Wszyscy pracownicy powinni znać zasady polityki bezpieczeństwa oraz przejść odpowiednie szkolenia. Pozwoli to na przezwyciężenie niezwykle istotnych obaw o bezpieczeństwo informacji wrażliwych, co Komisja Europejska uznała za jeden z istotniejszych elementów ograniczających rozwój administracji elektronicznej. Natomiast z analizy danych zawartych w artykule widać, że zapotrzebowanie i chęć korzystania z usług e-administracji jest ogromny. Dlatego należy w pierwszej kolejności zadbać o odpowiednią organizację i zarządzanie systemem e-administracji, który będzie gwarantował bezpieczeństwo informacji wrażliwych, w wyniku czego uzyska zaufanie użytkowników. Istota tego zagadnienia została dostrzeżona przez Unię Europejską, która od 2010 roku przeznaczyła oddzielne fundusze na wspieranie rozwoju e-administracji w państwach członkowskich, w tym na zapewnienie bezpieczeństwa informacji wrażliwych.

Bibliografia

Batorski D. red. (2012), *Cyfrowa gospodarka. Kluczowe trendy rewolucji cyfrowej*, MGG Conferences, Warszawa.

Borowiecki R., Kwieciński M. red. (2003), *Monitorowanie otoczenia: przepływ i bezpieczeństwo informacji, w stronę inteligencji przedsiębiorstwa*, Zakamycze, Kraków.

CapGemini (2014), *Web-based survey on electronic public services*, Badania na zlecenie Komisji Europejskiej.

Combe C. (2006), *Introduction to e-business, management and strategy*, Amsterdam –Boston–Heidelberg–Londyn–Nowy Jork–Paryż–Oxford.

Dudek T. (2011), *Obszary zastosowania gospodarki elektronicznej*, Biblioteka Cyfrowa, Szczecin.

Dwornik B. (2013), *Bezpieczeństwo w Internecie*, Interaktywnie.com.

Economist Intelligence Unit (2013), *The 2013 e-readiness rankings*, The IBM Institute for Business Value.

Eurostat (2013), *ICT security in enterprises 2011–2012*, kwiecień 2013.

Grynkiewicz T., Poznański P. (2011), *Twoja firma w Internecie*, Oplograf, Opole.

GUS (2014), Wyniki badań do raportu: *Społeczeństwo informacyjne w Polsce w 2013 roku*, Warszawa, www.stat.gov.pl.

Jak działa e-administracja w Europie, prawo.rp.pl/artykul/1035898.html (5.04.2015).

Krzyżak E., *Organizacja ochrony informacji wrażliwych w świetle uregulowań obowiązujących przepisów prawa*, www.iniejawna.pl/pomoce/ela.html (11.03.2015).

Kulisiewicz T., Średniawa M. (2012), *Kierunki rozwoju technologii informacyjnych oraz ich zastosowań w sektorze MSP*, MGG Conferences, Warszawa.

Schetina E., Green K., Carlson J. (2002), *Bezpieczeństwo w sieci*, Helion, Gliwice.

Socjotechnika w służbie kradzieży danych, prnews.pl/aktualnosci/socjotechnika-w-sluzbie-kradziezy-danych.html (20.02.2015).

Stokłosa J. (2005), *Ochrona danych i zabezpieczenia w systemach teleinformatycznych*, Wydawnictwo Politechniki Poznańskiej, Poznań.

Tapscott D. (1997), *The digital economy: promise and peril in the age of networked intelligence*, McGraw-Hill, New York.

World Economic Forum (2013), *Global Information Technology Report*, http://reports.weforum.org/global-information-technology-report-2015/.

Wrycza S. (2010), *Informatyka ekonomiczna*. *Podręcznik akademicki*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

SERVICES E-GOVERNMENT, AND WAYS TO ENSURE SAFETY SENSITIVE INFORMATION IN THE EU COUNTRIES

Summary

The paper presents a quantitative analysis of the use of e-government services in Poland compared to EU Member States and inhibiting factors affecting the development prospects. The elements limiting the further development of the information society and e-services of public organizations is undoubtedly the security of sensitive information. Therefore, the article explains how to protect sensitive information in the context of policies pursued by the EU and the directions of the development of e-government.

Translated by Ireneusz Miciuła

Keywords: information society, sensitive information, security information