ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 798 STUDIA INFORMATICA NR 34 2014

Ireneusz Miciuła
Krzysztof Miciuła
Uniwersytet Szczeciński

ZNACZENIE PRZETWARZANIA W CHMURZE DLA BEZPIECZEŃSTWA DZIAŁALNOŚCI E-BIZNESOWEJ

Streszczenie

Artykuł prezentuje analizę występujących zagrożeń dla bezpieczeństwa danych przedsiębiorstw wykorzystujących w działalności narzędzia informatyczne, co w erze globalnego społeczeństwa informacyjnego wydaje się nieuniknione. Przedstawiono znaczenie i wpływ korzystania z usług na zasadzie przetwarzania w chmurze na bezpieczeństwo danych i procesów w działalności e-biznesowej.

Słowa kluczowe: chmura obliczeniowa, bezpieczeństwo w sieci, e-biznes

Wprowadzenie

Era e-gospodarki, tak jak większość innowacji, niesie ze sobą postęp ułatwiający życie ludziom i przedsiębiorstwom. W przypadku internetu jest to łatwy dostęp do dużego zbioru informacji oraz szybki i bezpośredni kontakt z różnymi instytucjami życia gospodarczego i społecznego. W rezultacie to także możliwość prowadzenia części lub całości działalności gospodarczej w internecie. Obecnie globalna gospodarka rozwija się w wirtualnej przestrzeni, gdzie nie zachodzi bezpośredni kontakt pomiędzy stronami transakcji. E-gospodarka oparta jest na rozwiązaniach teleinformatycznych i aplikacjach internetowych. W przestrzeni wirtualnej prowadzi się działalność ekonomiczną, zawierane są transakcje finansowe, nawiązuje się kontakty między podmiotami biznesu (producentami, dystrybutorami i odbiorcami produktów oraz usług). Za pomocą internetu zachodzą procesy biznesowe, dzięki którym następuje:

– redukcja kosztów związanych z komunikacją (wewnątrz i na zewnątrz firmy),
– prezentacja oferty handlowej,

– obsługa zamówień,
– sprostanie wymaganiom klientów,
– kreacja wizerunku firmy,
– obniżenie kosztów obsługi,
– wejście na nowe (globalne) rynki.

Jednym z innowacyjnych trendów w branży informatycznej jest tak zwane przetwarzanie w chmurze (ang. *cloud computing*), co wpływa na sposób prowadzenia biznesu, pracy działów w przedsiębiorstwach oraz zasady współpracy pomiędzy głównymi podmiotami rynkowymi. Przetwarzanie w chmurze polega na przeniesieniu świadczenia usług IT (sprzęt, oprogramowanie, dane, moce obliczeniowe) na serwer i umożliwia stały dostęp przez sprzęty posiadane przez klienta. Dzięki temu bezpieczeństwo nie zależy od stacji klienckiej, a szybkość procesów wynika z mocy obliczeniowej serwera. Jednak mimo wielu zalet i szans taka organizacja życia gospodarczego i społecznego w przestrzeni wirtualnej niesie także zagrożenia. Dlatego celem artykułu jest analiza występujących zagrożeń w zakresie bezpieczeństwa zasobów w gospodarce elektronicznej oraz zwrócenie uwagi na innowacyjne zjawisko, jakim jest przetwarzanie w chmurze.

1. Bezpieczeństwo w internecie

Gospodarka elektroniczna wpływa na każdą dziedzinę życia społeczno-ekonomicznego i modernizuje tradycyjną działalność przez stosowanie rozwiązań branży informatycznej we wszystkich gałęziach gospodarki. Wraz z rozwojem technologicznym świata następuje stale wzrastające znaczenie e-biznesu – szacuje się, że już prawie 8 trylionów dolarów rocznie przepływa za pośrednictwem handlu elektronicznego (e-commerce) (Mckinsey & Company, 2013). Wiele aktywności zarówno biznesowych, jak i społecznych byłaby niemożliwa bez korzystania z teleinformatyki. Potwierdza to istnienie bezpośredniego związku pomiędzy internetem a aktywnością gospodarczą. Dzięki temu widoczne są kierunki zmian w gospodarce wynikające z zastosowania narzędzi informatycznych.

Źródłem największego zagrożenia jest szkodliwe oprogramowanie (ang. *malicious software*, *malware*), które powoduje sprzeczne (złośliwe lub przestępcze) z intencją użytkownika komputera działania. W Polsce zagrożenie tego typu oprogramowaniem odpowiada za prawie dwie trzecie (64%), a na świecie ponad połowę (54%) wszystkich niebezpieczeństw dotyczących zasobów w sieci. Drugą pozycję wśród zagrożeń zajmują oszustwa internetowe, które według danych

z 2011 roku w Polsce występują średnio dwa razy częściej niż na świecie. Trzecie miejsce wśród najczęstszych przestępstw zajmuje tak zwany phishing (tabela 1).

Tabela 1

Najczęstsze zagrożenia w internecie w Polsce i na świecie w 2011 roku

Zagrożenie	Polska (%)	Świat (%)
Szkodliwe oprogramowanie	64	54
Oszustwa internetowe	20	11
Phishing	10	10

Źródło: (Norton Cybercrime Report, 2011).

Łamanie systemów bezpieczeństwa następuje przez wykorzystanie wielu metod, między innymi programów szpiegujących (na przykład trojan, wirus) oraz metod podszywania się pod uprawnioną osobę lub instytucję w celu wyłudzenia poufnych informacji, takich jak hasła (tak zwany phishing). Wśród internautów coraz powszechniejsze jest zjawisko „samoodsłaniania" się w internecie. Polega ono na udostępnianiu poufnych informacji, bardziej lub mniej świadomie, czy to przez odpowiedzi na fałszywe e-maile, czy też wpisywanie danych na fałszywych stronach internetowych.

Według statystyk w świecie wirtualnym przestępstw jest dwukrotnie więcej niż w świecie rzeczywistym (Eurostat, 2013). Przyczyn tego, że zostajemy ofiarami przestępstw internetowych, należy szukać w większej swobodzie działania cyberprzestępców oraz w brakach wiedzy dotyczącej bezpieczeństwa. W roku 2011 z powodu przestępczości internetowej, między innymi ataków internetowych, łączne straty wyniosły w Polsce 13 miliardów USD. Straty na świecie szacuje się na 388 miliardów USD. Bezpośrednie koszty, czyli środki skradzione przez przestępców lub poświęcone na rozwiązanie problemów, wyniosły w Polsce 2,9 miliarda USD, gdy na świecie kwota ta wyniosła 114 miliardów USD (tabela 2).

Tabela 2

Cyberprzestępczość w Polsce i na świecie w 2011 roku

	Polska	Świat
Koszty netto	13 mld zł	388 mld zł
Koszty bezpośrednie	2,9 mld zł	114 mld zł
Internauci – ofiary cyberprzestępców w 2011	71%	65%

Źródło: (Norton Cybercrime Report, 2011).

Z tego powodu każde przedsiębiorstwo powinno prowadzić politykę bezpieczeństwa, dzięki której uniknie ryzyka związanego z utratą danych. Działania na rzecz bezpieczeństwa wymiernie przekładają się na większą stabilność prowadzenia biznesu i zaufanie klientów.

Rewolucja internetowa sprawiła, że bezpieczeństwo w sieci jest aktualnym tematem i dochodową branżą. W tabeli 3 przedstawiono najczęściej spotykane zagrożenia według danych podanych przez Fundację „Bezpieczniej w Sieci". Wynika z nich, że najczęściej z niebezpiecznymi lub podejrzanymi sytuacjami spotykamy się, korzystając z portali społecznościowych, czyli nowego trendu w e-gospodarce. Również wysoki odsetek zagrożeń związany jest z utratą danych z komputera z różnych przyczyn (41%). Jedną z nich jest infekcja komputera przez złośliwe oprogramowanie, na które internauci często natykają się w serwisach społecznościowych (32%). Wysoki odsetek zagrożeń reprezentują także tak zwane oszukańcze maile wyłudzające dane (31%). Dzięki coraz lepszym urządzeniom i programom zabezpieczającym (na przykład zabezpieczenia biometryczne, autoryzacja i uwierzytelnianie przy logowaniu do konta bankowego czy do bazy danych w firmie) cyberprzestępcy mają coraz trudniejsze zadanie. Potwierdza to fakt, że najrzadziej z niebezpiecznymi lub podejrzanymi sytuacjami spotykamy się przy korzystaniu z konta bankowego (4%).

Tabela 3

Zagrożenia w internecie

Najczęściej spotykane zagrożenia w internecie w Polsce	Odsetek badanych, którzy zadeklarowali zetknięcie się z danym typem zagrożenia (w %)
Niechciane treści w serwisach społecznościowych	63
Utrata danych z komputera (z różnych przyczyn)	41
Otrzymanie złośliwej aplikacji w serwisie społecznościowym	32
Oszukańcze maile wyłudzające informacje	31
Podszywanie się, kradzież tożsamości	9
Włamanie do komputera bez kradzieży danych	9
Ujawnienie hasła do konta e-mail	8
Włamanie do komputera i kradzież danych	4
Próba włamania do konta bankowego	4
Włamanie do konta bankowego i kradzież pieniędzy	3

Źródło: (Fundacja „Bezpieczniej w Sieci", 2012).

Zagrożenia determinują rozwój rozwiązań technicznych, mających za zadanie jej ochronę. Firmy, ustalając politykę bezpieczeństwa, zasadniczo robią to, aby ograniczyć trzy typy ryzyk:

– zniszczenie lub uszkodzenie danych z powodu ataku lub z innej przyczyny,
– ujawnienie poufnych danych w wyniku włamania,
– niedostępność usług teleinformatycznych z powodu ataku z zewnątrz.

Powyżej wymienione ryzyka odpowiadają głównym elementom definicji bezpieczeństwa teleinformatycznego, to jest poufności oraz dostępności danych i systemów. W trakcie procesu ochrony zasobów przedsiębiorstwa bardzo ważne są wewnętrzne procedury bezpieczeństwa. Najczęściej stosowanymi metodami w wewnętrznej procedurze są tworzenie kopii zapasowej danych oraz procesy autoryzacji i uwierzytelniania. Dzięki nim można zarządzać dostępem (uprawnieniami) do danych w firmach. Do najczęściej używanych metod zabezpieczenia zasobów przed zagrożeniami 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 zestawie.

Dzięki ulepszaniu zabezpieczeń w najnowszych pakietach bezpieczeństwa oprócz podstawowych programów, jak program antywirusowy, filtr antyspamowy czy zapora internetowa, firmy dostarczają dodatkowe usługi mające zagwarantować nam bezpieczeństwo, na przykład przy połączeniach z bankowością elektroniczną oraz sklepami internetowymi. Program sprawdza, czy użytkownik chce uzyskać dostęp do prawdziwej strony systemu bankowości internetowej lub systemu płatności przez sprawdzenie certyfikatów używanych do nawiązania połączenia szyfrowanego. To zapobiega uzyskaniu dostępu do fałszywej strony internetowej.

Najczęstszymi ofiarami ataków są przedsiębiorstwa, które nie przykładają uwagi, co się dzieje z ich przetwarzanymi danymi. Trudniej jest wykraść dane od przedsiębiorstw, które mają świadomość wagi posiadanych informacji i pilnie strzegą miejsc, w których się one znajdują. Należy dokonać klasyfikacji i ustalenia mechanizmów monitorowania poszczególnych grup danych. Dla bezpieczeństwa warto wdrożyć mechanizm podziału uprawnień, wskazać osoby uprzywilejowane, na przykład administratorów. Oprócz podstawowych narzędzi ochrony zaleca się wykorzystanie między innymi rejestracji specyficznego ruchu czy

kryptografii. Rejestracja specyficznego ruchu jest wykorzystywana na potrzeby ewentualnego śledztwa, co pozwala na oszacowanie wielkości strat i skali danych skradzionych z firmy. Mając informacje o ataku, można podjąć kroki zaradcze i udoskonalić zabezpieczenia oraz wprowadzić odpowiednie procedury w firmie. Dla ochrony przy przesyłaniu danych przez sieć wykorzystuje się kryptografię, czyli szyfrowanie.

Aktualnie e-biznes czekają wyzwania dotyczące różnorodnych zagrożeń. Przedsiębiorstwa dostarczają programy sieciowe do oddalonych oddziałów i biur oraz pracowników zdalnych. Wymaga to zapewnienia odpowiedniej ochrony dla wszystkich obsługiwanych środowisk i lokalizacji. Rozwiązaniem jest stosowanie zintegrowanych rozwiązań dla zabezpieczenia zasobów firmy. Pakiety bezpieczeństwa chronią przed wieloma zagrożeniami, od ataków wirusów po kradzież informacji i inne niezidentyfikowane niebezpieczeństwa.

2. Chmura obliczeniowa i jej znaczenie dla bezpieczeństwa

Chmura obliczeniowa (ang. *cloud computing*) to model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę. Funkcjonalność ta jest tu rozumiana jako usługa oferowana przez dane oprogramowanie oraz konieczną infrastrukturę. Oznacza to eliminację konieczności zakupu licencji czy konieczności instalowania oprogramowania i administracji nim. Dzięki chmurze przedsiębiorstwa mogą mieć przez cały czas dostęp do swoich danych bez ponoszenia kosztów utrzymania własnych serwerowni. Pojęcie chmury nie jest jednoznaczne, w szerokim znaczeniu przetwarzane w chmurze jest wszystko, co jest na zewnątrz zapory sieciowej, włączając w to konwencjonalny outsourcing. Rozróżniamy następujące rodzaje chmury:

a) prywatne (ang. *private cloud*), będące częścią organizacji, aczkolwiek jednocześnie autonomicznym dostawcą usługi;
b) publiczne (ang. *public cloud*), będące zewnętrznym, ogólnie dostępnym dostawcą (na przykład Amazon.com, Google, Microsoft itd.);
c) hybrydowe (ang. *hybrid cloud*), będące połączeniem filozofii chmury prywatnej i publicznej – pewna część aplikacji i infrastruktury danego klienta pracuje w chmurze prywatnej, a część jest umiejscowiona w przestrzeni chmury publicznej.

Wirtualna chmura usług nie wymaga świadomości szczegółów jej działania przez klienta, gdyż jest to zbędne przy korzystaniu z niej. Dla bezpieczeństwa

danych firmy mogą wykorzystywać chmurę do przechowywania i udostępniania danych, tak zwaną wirtualizację zasobów. Dzięki chmurze przedsiębiorstwa mogą mieć przez cały czas dostęp do swoich danych bez ponoszenia kosztów utrzymania własnych serwerowni. Chmura dostarcza trzy typy usług:

1. SaaS (*Software as a Service*) – model chmury, w której dostawca udostępnia niezbędną infrastrukturę sprzętowo-sieciową oraz aplikację użytkową z miejscem, gdzie można umieszczać swoje dane.
2. PaaS (*Platform as a Service*) – dostawca udostępnia kompletne środowisko programistyczne dla danych i aplikacji klienta. Dostarcza całościową platformę do projektowania i wdrażania własnych aplikacji.
3. IaaS (*Infrastructure as a Service*) – dostawca dostarcza klientom kompletną infrastrukturę informatyczną używaną do wdrażania własnych projektów i aplikacji oraz system składowania danych. Udostępnia także infrastrukturę sieci, która umożliwia klientom tworzenie prywatnych chmur.

Dzięki używaniu usług w modelu chmurowym przedsiębiorstwa nie muszą inwestować w sprzęt i oprogramowanie, co wpływa na obniżenie kosztów działalności. Usługa zdejmuje z działu IT problem przywracania danych i odtwarzania systemów. Teraz utrata danych na skutek awarii, kradzieży, zagubienia czy skasowania nie stanowi problemu. Przedsiębiorstwa udostępniające chmury powinny w różny sposób chronić dane, które przechowują. Jeśli miejsce przechowywania i dostępu do serwerów jest zabezpieczone fizycznie, trzeba też spojrzeć na bezpieczeństwo informatyczne w aspekcie szyfrowania danych. Dane wędrujące przez publiczne łącza internetu między serwerami a pracownikami przedsiębiorstw powinny być szyfrowane, aby były zabezpieczone przed odczytaniem w serwerowni lub w otoczeniu przedsiębiorstwa. Przedsiębiorcy i użytkownicy dzięki wykorzystaniu chmury nie muszą ponosić kosztów związanych z licencją czy obsługą serwerowni i stacji roboczych. Otrzymują dostęp do różnych programów i rozwiązań na serwerach dostawcy. Chmura stanowi bezpieczniejsze miejsce gromadzenia danych niż lokalna infrastruktura w przedsiębiorstwie. Wynika to z efektu skali i wykorzystywanych rozwiązań technologicznych. Dzięki prawidłowo zbudowanej infrastrukturze chmury każdy plik skopiowany jest na kilka niezależnych dysków zlokalizowanych w odrębnych centrach danych. Taka architektura zmniejsza ryzyko utraty danych.

Ważnym podejściem w tej technologii jest zagwarantowanie bezpieczeństwa przez dostawcę usługi. Dlatego firma świadoma zagrożeń dotyczących bezpieczeństwa danych powinna upewnić się, jakie standardy w tej dziedzinie zapewnia

dostawca chmury. Najczęstszym modelem wirtualizacji serwerów prywatnych jest jedna z konfiguracji VPS. Tradycyjny model VPS to dzielenie serwera na kilka mniejszych serwerów wirtualnych udostępnianych klientom w formie usługi serwera VPS. Dostawcy stosują różnego rodzaju techniki i technologie mające zapewnić niezawodność. Infrastruktura chmury zakłada rozdzielenie mocy obliczeniowej dotyczącej pamięci masowej. Moc obliczeniowa jest dzielona przez setki fizycznych urządzeń połączonych w klaster. Dane klientów są umieszczone na współdzielonej, centralnej macierzy dyskowej. Umożliwia to dostęp do wszystkich serwerów jednocześnie. W przypadku awarii serwera w klastrze jego miejsce zajmuje inny, sprawny, który zapewni dalszą pracę uruchomionych na nim serwerów wirtualnych. Technologia przetwarzania w chmurze zapewnia wysoką elastyczność i skalowalność całego rozwiązania. Klastry można rozbudować o kolejne serwery, a macierze pamięci masowej o kolejne dyski twarde. W ten sposób dostawcy mogę tworzyć prywatne chmury, które rosną wraz z potrzebami klientów. Chmura daje klientom możliwość zmiany konfiguracji serwera VPS oraz płacenie tylko za zużyte zasoby. W każdej chwili klient może zamówić dodatkowe zasoby procesora, pamięci operacyjnej lub przestrzeni dyskowej. Jest to istotne w momencie rozwoju działalności przez przedsiębiorstwo. Dla zwiększenia bezpieczeństwa każdy serwer powinien być wyposażony w minimum 2 źródła zasilania, zduplikowane łącza do sieci oraz mechanizmy przełączania i routingu. Połączenia między poszczególnymi częściami chmury realizowane są w ramach wirtualnej sieci prywatnej odizolowanej od sieci innych klientów.

Od jakości centrum przetwarzania danych dostawców chmur obliczeniowych zależy stabilność usług. Dostawcy tego typu usług powinni dysponować wysokim standardem zarówno ochrony fizycznej, przeciwpożarowej, jak i stabilności zasilania oraz łączności i ochrony powierzonych danych. Zadaniom tym dedykowana jest cała infrastruktura i oprogramowanie, które wspierają stabilność usług chmury obliczeniowej. Właśnie w tym obszarze następują największe korzyści dla klientów usług opartych na e-chmurach. Ochronę przed utratą danych zapewniają kopie zapasowe przechowywane na minimum dwóch serwerach oraz możliwość tworzenia „backup" plików używanych przez klienta w czasie rzeczywistym. Wówczas dane są chronione podwójnie i istnieje możliwość ich odzyskania w razie ich ewentualnej utraty czy awarii. W celu zapewnienia poufności przechowywanych danych podstawowymi metodami są uwierzytelnianie i autoryzacja oraz stosowanie kryptografii. Transmisja między komputerem a serwerem jest zaszyfrowana, przykładowo protokołem SSL, a dane na dyskach szyfrowane

są za pomocą algorytmu AES-256. Obecnie chmury wykorzystuje się w rozwiązaniach służących do zabezpieczania komputera przed szkodliwym oprogramowaniem (wirusami, robakami itp.). Antywirusy wykorzystywane w chmurze porównują sumy kontrolne skanowanych plików z danymi w bazie internetowej. Jest to tak zwana kolektywna inteligencja, czyli rozproszona sieciowa baza danych.

Korzystanie z usług w chmurze ma przede wszystkim zalety finansowe (obniżanie kosztów) i nieocenione zwiększenie poziomu bezpieczeństwa danych przez przeniesienie części odpowiedzialności na usługodawców. Natomiast nie należy zapominać o własnej polityce bezpieczeństwa – przedsiębiorcy korzystający z chmury muszą też sami wpływać na zwiększenie ochrony danych. Powinni używać aktualnego programu antywirusowego, ustawiać odpowiednie hasła, zabezpieczać komunikację oraz szyfrować dane, co wpłynie na ochronę danych gromadzonych w chmurze dostawcy usługi. Z badania przeprowadzonego na zlecenie Komisji Europejskiej wśród firm, które korzystają z chmury obliczeniowej, wynika, że oszczędności z tym związane wyniosły średnio 15% kosztów IT. Dynamiczny rozwój społeczeństwa informacyjnego oraz rosnące zapotrzebowanie na coraz lepszą jakość usług i produktów stały się przyczyną powszechnego rozwoju gospodarki elektronicznej w różnych dziedzinach życia. W warunkach rosnącej otwartości gospodarki i procesów globalizacyjnych gospodarka podlega coraz silniejszym wpływom otoczenia zewnętrznego. W celu szybkiego wdrożenia modelu chmury obliczeniowej w Unii Europejskiej w 2012 Komisja Europejska zaproponowała między innymi przyjęcie nowych ram prawnych dla ochrony danych oraz opracowanie jednolitych standardów regulujących ich przetwarzanie, co ma zwiększyć bezpieczeństwo świadczenia tej usługi.

Podsumowanie

Przedsiębiorstwa, które chcą funkcjonować i rozwijać swoją działalność w e-biznesie, są zmuszone kłaść coraz większy nacisk na politykę bezpieczeństwa danych, aby zapewnić poufność i ochronę danych swoim klientom. Podstawowe rodzaje zagrożeń bezpieczeństwa danych firmy wynikają z niedoskonałości technologii IT lub nieświadomego czynnika ludzkiego. Przedsiębiorca dla bezpieczeństwa powinien wdrożyć politykę bezpieczeństwa, która określa sposób korzystania z systemów informatycznych, zasobów i narzędzi IT w całym przedsiębiorstwie. Pozwoli to na zmniejszenie strat operacyjnych wynikających z łamania systemów bezpieczeństwa. Firmy zajmujące się tworzeniem systemów bezpie-

czeństwa powinny wdrażać urządzenia i programy wychwytujące, które będą skuteczne w zwalczaniu i ograniczaniu ataków cyberprzestępców. Czas działa na niekorzyść chronionych zasobów. Żywotność systemów bezpieczeństwa nie powinna być długa, a przerwa pomiędzy kolejnymi aktualizacjami systemów musi być na tyle krótka, aby osoby niepowołane nie miały czasu na znalezienie sposobów na ich złamanie. Natomiast użytkownicy nie powinni bezgranicznie liczyć jedynie na pewne rozwiązania (zabezpieczenia), na przykład filtr bezpieczeństwa, lecz przede wszystkim postępować w zgodzie z ogólnymi zasadami bezpieczeństwa, które zmieniają się wraz z otaczającą nas rzeczywistością.

E-biznes stał się kluczowym elementem współczesnego świata. Dlatego można stwierdzić, że trendy napędzające rozwój cyfrowych sieci komunikacyjnych w znacznym stopniu zadecydują o rozwoju społecznym i ekonomicznym. Będąc na etapie procesu budowy ery informacyjnej poprzez wykorzystanie nowoczesnych technik ICT stwarzamy warunki do bezpośredniego dostępu do informacji oraz rozwijanie potencjału intelektualnego i gospodarczego na świecie. Światowa gospodarka jest w fazie globalizacji opartej na zaawansowanych technologiach, co dotyczy szczególnie handlu elektronicznego. Systemy informatyczne, dzięki którym te przemiany są możliwe, można zakwalifikować do grupy systemów strategicznych, przełomowych w osiąganiu przyszłych sukcesów gospodarczych. Ma to ogromne znaczenie w przełożeniu na e-biznes przedsiębiorstw. Przy skomplikowaniu działania e-biznesu w świecie wirtualnym i narażeniu na niebezpieczeństwa zarówno celowe, jak i niecelowe (natury sprzętu i oprogramowania), to największą zaletą usług w chmurze jest zapewnienie bezpieczeństwa i ciągłość działania. Kolejną fundamentalną zaletą tego typu usług jest możliwość dopasowywania przez klienta środowiska do aktualnych potrzeb biznesowych przez racjonalizowanie w ten sposób kosztów ponoszonych na IT. Te dwie podstawowe zalety i korzyści wynikające z korzystania usług przetwarzania w chmurze powodują, że jest to jeden z najważniejszych trendów w branży ICT w XXI wieku na świecie.

Bibliografia

CERT Polska (2012), *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, NASK, Warszawa.

„Chip" (2009), *Internet jest chmurą*, nr 3, s. 38.

Chmielarz W. (2007), *Systemy biznesu elektronicznego*, Difin, Warszawa.

„Computerworld" (2010), *Masowa wirtualizacja: czy to bezpieczne*, nr 5–6, s. 21–25.

Dwornik B. (2013), *Bezpieczeństwo w Internecie*, Interaktywnie.com (14.03.2014).

Eurostat (2013), *ICT Security in Enterprises 2011–2012*, http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/ (15.03.2014).

Fundacja „Bezpieczniej w Sieci" (2012), *Bezpieczny Internet,* http://www.bezpieczniejwsieci.org/ (25.04.2014).

GUS (2014), *Wyniki badań do raportu: Społeczeństwo informacyjne w Polsce w 2013 roku*, http://www.stat.gov.pl (21.03.2014).

Komisja Europejska (2012), Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Wykorzystanie potencjału chmury obliczeniowej w Europie* (COM (2012) 529 final), 27.09.2012.

McKinsey & Company (2013), *Internet Matters: Essays in Digital Transformation*, Mckinsey.com (13.03.2013).

Norton Cybercrime Report (2011), http://pl.norton.com/cybercrimereport/promo (10.04.2014).

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

Trojnar D. (2010), *Wirtualizacja jako przyszłość sieci teleinformatycznych. SECON 2010 – Materiały konferencyjne*, WAT, Warszawa.

THE IMPORTANCE CLOUD COMPUTING FOR SAFETY E-BUSINESS

Summary

The article presents an analysis of existing threats to the security of enterprise data, which using the ICT tools, what in the era of global information society seems inevitable. The paper presents the significance and impact of the use of services on the basis of cloud computing for data security and business processes in e-business.

Translated by Ireneusz Miciuła

Keywords: cloud computing, network security, e-business

Informacje o autorach:

Ireneusz Miciuła, dr inż., Krzysztof Miciuła, mgr, Uniwersytet Szczeciński, Wydział Nauk Ekonomicznych i Zarządzania, irekmic@wneiz.pl.