Nina Siemieniuk[1], Agnieszka Zalewska-Bochenko[2]

Bezpieczeństwo systemów informatycznych w instytucjach bankowych

1. Wstęp

Bankowość jest jednym z sektorów najbardziej zaawansowanych w użytkowaniu i wdrażaniu nowych technologii. Dzięki rozwojowi Internetu, technologii mobilnych i globalnych systemów informatycznych nastąpił wzrost znaczenia bankowości niezależnej od stref czasowych, położenia geograficznego i kanałów dostępu. Wprowadzanie innowacji w tym zakresie niesie ze sobą jednak szereg zagrożeń. W działalności banków największe znaczenie ma informacja, dlatego też do prawidłowego funkcjonowania instytucji bankowych niezbędne są bezpieczne systemy informatyczne. Jakiekolwiek zakłócenia w pracy systemów komputerowych bezpośrednio oznaczają utratę dochodów. Utrzymanie bezpieczeństwa systemu informatycznego stało się więc dla instytucji bankowych koniecznością.

W niniejszym artykule ze względu na złożoność podjętej problematyki niektóre z zagadnień dotyczących systemów informatycznych w instytucjach bankowych zostały jedynie zasygnalizowane.

2. System informatyczny – wprowadzenie

System informatyczny to program (lub zbiór programów i funkcji) zarządzający zasobami oraz umożliwiający wykorzystanie tych zasobów przez użytkowników[3].

[1] Uniwersytet w Białymstoku, Wydział Ekonomii i Zarządzania.
[2] Uniwersytet w Białymstoku, Wydział Ekonomii i Zarządzania.
[3] *Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki*, Warszawa 2002, s. 2, https://www.knf.gov.pl/Images/rekomendacja_d_tcm75-8552.pdf [dostęp 12.04.2016].

Aby system informatyczny w instytucjach bankowych mógł realizować właściwie swoje zadania, powinien być[4]:

- integralny, czyli zapewniać połączenia pomiędzy wszystkimi poprzez stosowanie wspólnych zbiorów danych, przeprowadzanie operacji eksportu/importu danych na poziomie transakcji, a nie baz danych oraz dbałość o zaplecze operacyjne na potrzeby bieżącego zarządzania;
- przepustowy, czyli zmierzać do zapewnienia jego nadążności;
- modułowy, czyli umożliwiać dołączanie nowych elementów systemu w przyszłości;
- elastyczny (definiowanie menu na poziomie użytkownika, tworzenie indeksów dostępów niepowtarzalnych numerów klienta, konta);
- bezpieczny (nadawanie haseł blokujących, korzystanie z niektórych funkcji systemu, system uprawnień dostępu, limity kwotowe dla pracowników, prowadzenie dziennika wejść do systemu);
- przyjazny dla użytkownika, czyli umożliwiać dostęp do informacji w dowolnym przekroju.

Do najczęstszych przyczyny niewłaściwego zabezpieczenia systemów informatycznych banku zaliczamy[5]:

- niewystarczającą świadomość zagrożeń;
- brak wiedzy specjalistycznej, a w szczególności z zakresu zarządzania zabezpieczeniem systemów o poufnym charakterze;
- wysokie koszty budowy zabezpieczeń, często trudnych do uzasadnienia;
- niechęć pracowników do przestrzegania dodatkowych, złożonych, utrudniających codzienną pracę procedur;
- niewystarczającą współpracę zainteresowanych komórek banku;
- błędy (niezamierzone) pracowników banku.

Banki są zobowiązane do budowania specjalnych systemów kontroli dostępu do bankowych systemów informatycznych w sposób, który zapewni ochronę danych i haseł umożliwiających ich przetwarzanie – zarówno przez klientów banku, jak i ich pracowników. Konieczne jest przy tym stałe monitorowanie

[4] http://docplayer.pl/2924076-Cechy-i-zadania-systemu-informatycznego-banku-informatyka-bankowa-wsb-w-poznaniu-dr-grzegorz-kotlinski.html [dostęp 12.04.2016].

[5] http://docplayer.pl/13356535-Bezpieczenstwo-systemu-informatycznego-banku-informatyka-bankowa-wsb-w-poznaniu-dr-grzegorz-kotlinski.html [dostęp 18.04.2016].

funkcjonowania systemów informatycznych[6]. Dlatego też system informatyczny banku wymaga[7]:

- uniezależnienia obsługi klienta od lokalizacji rachunku, ujednolicenia reguł postępowania w skali całego systemu bankowego (i banku);
- powstania centralnej bazy danych zawierającej definicje produktów, baz operacyjnych, komplet informacji o rachunkach i klientach, sięgać do nich powinien zarówno bank, jak i klienci;
- utrzymywania wysokiej niezawodności sieci, duplikacji urządzeń centrali, częściowej autonomizacji oddziałów;
- wirtualizacji działalności przedsięwzięć internetowych.

Dodatkowo banki muszą przestrzegać przepisów nakładających na nie obowiązek zapisywania wszystkich zdarzeń zachodzących w ich systemach w sposób, który umożliwi ich kontrolę nawet po kilku latach[8].

3. Zagrożenia dla działania systemu informatycznego

Coraz więcej klientów polskich banków korzysta z produktów i usług bankowych, do których dostęp zapewniają kanały zdalne. Na koniec 2014 r.[9]:

- 27,19 mln klientów indywidualnych i MŚP miało podpisaną umowę umożliwiającą korzystanie z bankowości internetowej;
- średnia wartość transakcji miesięcznych zlecanych przez klientów wynosiła 5579 PLN, a średnia wartość miesięczna MŚP 75 748 PLN;
- wielkość wolumenu przelewów zlecanych przez klientów indywidualnych i MŚP wyniosła 164,97 PLN;
- w obrocie było 36,07 mln kart płatniczych, z czego 29,75 mln kart debetowych, 6,04 mln kart kredytowych i 282 tys. kart obciążeniowych.

Dynamicznemu rozwojowi bankowości elektronicznej towarzyszy niestety również rozwój technik przestępczych. Naturalną konsekwencją tego są więc coraz silniejsze więzi sektora bankowego ze środowiskiem informatycznym,

---

[6] M. Jaślan, *Meandry bezpieczeństwa danych. Zabezpieczenia danych. Monitoring i bezpieczeństwo*, „Bank" 2008, nr 3, s. 47.

[7] http://docplayer.pl/2924076-Cechy-i-zadania-systemu-informatycznego-banku-informatyka-bankowa-wsb-w-poznaniu-dr-grzegorz-kotlinski.html [dostęp 12.04.2016].

[8] M. Jaślan, op.cit., s. 47.

[9] P.M. Balcerzak, *Bank i klient: potrzebujemy cybertarczy sektora bankowego*, „Bank" 2015, nr 5, s. 40.

które pozwalają na skuteczne pokonywanie bariery czasu i przestrzeni, ale których jedną z podstawowych reguł jest odpowiedni poziom ochrony danych[10]. Globalny charakter sieci sprawia bowiem, że wymiana informacji jest pozbawiona kontroli nad drogą przesyłania. Sieć Internetu, do której jest podłączony zarówno system informatyczny banku, jak i klient, jest narażona na ataki „sieciowych włamywaczy"[11].

Zagrożenia systemów informatycznych w instytucjach bankowych można podzielić na kilka podstawowych kategorii. Wszystkie zostały zgrupowane i przedstawione w tabeli 1.

Tabela 1. Zagrożenia dla systemów informatycznych w instytucjach bankowych

Zagrożenie	Charakterystyka zagrożenia
Wirusy	Program napisany w jednym z języków programowania. Przyłącza się do normalnych programów i dokumentów bez zgody lub wiedzy użytkownika. Ma zdolność do tworzenia własnych kopii.
Robaki	Program komputerowy, który rozprzestrzenia się samodzielnie, niezależnie od działania człowieka. Nie infekuje jednak innych plików. Głównym jego celem jest powielanie się w Internecie i spowolnienie łączy.
Konie trojańskie	Mogą przybierać formę innego nieszkodliwego i powszechnie używanego programu. Aplikacja ta uszkadza system lub przeprowadza inne destrukcyjne czynności. Nie rozprzestrzeniają się samodzielnie[12].
Szkodliwe kody	
Adware	Programy, które wyświetlają materiały reklamowe niezależnie od czynności wykonywanych przez użytkownika.
Binder	Program łączący szkodliwe pliki z rozszerzeniem .jpg z plikiem .exe. W ten sposób są dołączane do zdjęć konie trojańskie.
Bomba logiczna	Program niszczący dane, uruchamiający się w odpowiednim czasie lub okresowo w systemie komputerowym, określający warunki, w jakich mają być podejmowane niedozwolone działania.

[10] E. Węsierska, *Dywersyfikacja metod ochrony systemów elektronicznych jako warunek funkcjonowania przedsiębiorstwa bankowego*, w: *Zastosowania rozwiązań informatycznych w instytucjach finansowych*, red. A. Gospodarowicz, „Prace Naukowe", nr 1035, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław 2004, s. 130–143.

[11] Por. D. Lynch, L. Lyndquist, *Digital Money: the new era of Internet commerce*, J. Wiley&Sons Inc., New York, 1996, s. 172–177.

[12] *Bankowość internetowa. Bezpieczeństwo transakcji bankowych w Internecie*, Związek Banków Polskich, http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=9 [dostęp 21.04.2016].

Zagrożenie	Charakterystyka zagrożenia
Dialer	Program, który bez wiedzy użytkownika przekierowuje zwykłe połączenie na numer o podwyższonej płatności.
Fałszywe alarmy	Przesyłane e-mailem instrukcje usunięcia ważnych plików systemowych, bez których system operacyjny nie może działać poprawnie.
Spam	Niechciana, niezamówiona reklama, spływająca głównie poprzez pocztę elektroniczną, generująca niepotrzebny ruch w sieci.
Ataki na zasoby sieciowe	
Hakerstwo	Próba uzyskania dostępu do systemu komputerowego z pominięciem uwierzytelniania. Ataki są przeprowadzane poprzez niechronione, otwarte porty, czyli kanały komunikacji komputera z Internetem[13].
Spyware, crimeware	Programy szpiegowskie, które bez zgody właściciela zbierają i wysyłają informacje o jego komputerze. Są to wszelkiego rodzaju konie trojańskie czy też aplikacje rejestrujące znaki wpisywane z klawiatury (tzw. keyloggery), które następnie są wysyłane do agresora.
Eksploit	Rodzaj ataku, program lub część kodu, wykorzystujące błąd lub lukę w aplikacji bądź systemie operacyjnym. W rezultacie przeprowadzenia takiego ataku agresor może zdobyć pełne uprawnienia do atakowanego komputera.
Atak słownikowy i back door	Atak polegający na próbie zalogowania się do systemu z wykorzystaniem dużej listy słów znajdujących się w określonym pliku jako kolejno próbowanych haseł. Back door, czy inaczej „tylne drzwi", to programy bazujące na zainstalowaniu odpowiedniego oprogramowania, pozwalającego na dostanie się do systemu w inny sposób niż logowanie.
Skanowanie portów	Wysyłanie do atakowanego systemu żądania udostępnienia usług na wielu portach w celu znalezienia uruchomionych usług oraz aktywnych portów.
Phishing	Polega na tworzeniu fałszywych wiadomości e-mail i stron WWW, wyglądających identycznie jak serwisy internetowe banków. Te atrapy mają za zadanie nakłonić klientów do podania numeru karty kredytowej, hasła logowania, informacji o koncie bankowym[14].
Pharming	Wykorzystywanie oprogramowania wymuszającego na przeglądarce internetowej przekierowanie wysyłanych danych do serwera atakującego zamiast do serwera banku.
Sniffing	Podsłuchiwanie przesyłanych przez sieć pakietów. Sniffer przechwytuje dane przesyłane niekodowanym kanałem.

[13] Por. D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej* w: *Bankowość elektroniczna*, red. A. Gospodarowicz, PWE, Warszawa 2005, s. 66.

[14] J. Grobicki, *Wirtualne, czyli realne straty*, „Bank" 2005, nr 7–8, s. 63.

Zagrożenie	Charakterystyka zagrożenia
Spoofing	Podszywanie się pod inny komputer w sieci. W efekcie „legalny" użytkownik zostaje rozłączony, a włamywacz kontynuuje połączenie z pełnymi prawami dostępu np. do jego konta w banku.
Denial of service	Odmowa wykonania usługi. Atak ten bazuje na takim wykorzystaniu zasobów komputera, że nie jest on w stanie zagwarantować poprawniej realizacji usług, jakie oferuje.
Rootkit	Sposoby i metody, jakie stosują programy typu spyware, wirusy lub trojany do chowania się przed wszelkimi skanerami. Rootkitami mogą być także różne zestawy narzędzi lub programów, których zadaniem jest zamaskowanie jakiejkolwiek próby włamania i uzyskania uprawnień administratora.
Socjotechnika	Napastnik stosuje odpowiednie połączenie informacji o systemie i technik manipulacyjnych, aby wzbudzić zaufanie ofiary. Celem ataków socjotechnicznych jest uzyskanie dostępu fizycznego, uzyskanie danych uwierzytelniających do dostępu zdalnego, zdobycie informacji lub naruszenie innych mechanizmów kontroli bezpieczeństwa. Ataki socjotechniczne można przeprowadzić za pomocą różnych mediów komunikacyjnych: telefonu, poczty tradycyjnej i elektronicznej, stron WWW, komunikatorów, IRC, list wysyłkowych, forów dyskusyjnych. Przykładami ataków dokonywanych przez media mogą być: spotkanie, zwiedzanie firmy, przeprowadzenie rozmowy telefonicznej w charakterze pracownika lub sprzedawcy, fałszywa strona WWW gromadząca informacje logowania, ankieta listowna. Odpowiedzią na rosnącą liczbę incydentów w cyberprzestrzeni w obszarze finansowym jest propozycja budowy cybertarczy sektora bankowego. Niestety, liczba ataków na użytkowników bankowości elektronicznej stale rośnie. Odzwierciedleniem tej negatywnej tendencji jest liczba publikacji Rady Bankowości Elektronicznej na stronie internetowej Związku Banków Polskich o nowych incydentach nakierowanych na klientów korzystających z bankowości elektronicznej. W 2012 r. takie komunikaty były dwa, w 2013 r. trzy, a w 2014 r. było już ich dziesięć[15].

Źródło: M. Kopczewski, E. Czapik-Kowalewska, *Zagrożenia sieciowe a bezpieczeństwo informacyjne*, http://mit.weii.tu.koszalin.pl/MIT6/Modele%20inzynierii%20teleinformatyki%206_08%20Kopczewski%20Czapik%20Kowalewska.pdf [dostęp 21.04.2016].

Oczywiście nie zawsze tego rodzaju ataki muszą zakończyć się katastrofą, bo bywa bardzo często tak, że są one na wczesnym etapie identyfikowane i udaremniane przez ekspertów od zarządzania bezpieczeństwem systemów informatycznych.

[15] P.M. Balcerzak, op.cit., s. 40.

4. Bezpieczeństwo systemu informatycznego

Bezpieczeństwo w znaczeniu informatycznym to pewien stan, który charakteryzuje się określonym poziomem najważniejszych dla danego przypadku atrybutów. Do najistotniejszych atrybutów bezpieczeństwa w instytucjach bankowych zaliczamy[16]:

- poufność – gwarantującą, że dostęp do danych przechowywanych i przetwarzanych w systemie mają tylko osoby do tego uprawnione;
- integralność – gwarantującą, że dane przesyłane w czasie transakcji elektronicznej nie są przez nikogo modyfikowane;
- autentyczność – pozwalającą stwierdzić, czy osoba podpisująca się pod transakcją jest rzeczywiście osobą, za którą się podaje;
- niezaprzeczalność – niepozwalającą wyprzeć się faktu nadania lub odbioru komunikatu drogą elektroniczną;
- dostępność – gwarantującą stały dostęp do systemu bankowości elektronicznej;
- niezawodność – gwarantującą, że system działa w sposób, jakiego się od niego oczekuje.

Problematyka bezpieczeństwa zasobów informacji w instytucjach bankowych jest niezwykle szeroka i ma charakter interdyscyplinarny[17]. Zagrożenia, jakie niesie ze sobą świadczenie usług bankowych na odległość, wywołują brak zaufania klientów do elektronicznej bankowości oraz obawy o bezpieczeństwo środków, co stanowi jedną z głównych barier rozwoju zdalnych usług bankowych. Tymczasem zabezpieczenia stosowane przez banki w Polsce należą do jednych z najbardziej zaawansowanych. Można wyróżnić kilka kategorii środków ochrony[18], których klasyfikację przedstawiono w tabeli 2.

---

16 Por. A. Grandys, *E-bankowość – bankowość gospodarki cyfrowej*, cz. 2, „Monitor Rachunkowości i Finansów" 2001, t. 6, s. 49–50; D. Kosiur, *Understanding Electronic commerce*, Microsoft Press, Redmond 1997, s. 66.

17 A. Michalski, *Wykorzystanie technologii systemów informatycznych w procesach decyzyjnych*, Politechnika Śląska, Gliwice 2002, s. 134.

18 Por. S. Wojciechowska-Filipek, *Metody kontroli dostępu w bankowości elektronicznej*, s. 559–560, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/115.pdf [dostęp 03.04.2016].

Tabela 2. Środki bezpieczeństwa stosowane w instytucjach bankowych

Środki fizyczne	• urządzenia przeciwwłamaniowe, • sejfy, alarmy, • urządzenia ochrony przeciwpożarowej, • rozwiązania architektoniczne, pomieszczenia odpowiednio przystosowane do pracy komputerów, urządzenia klimatyzacyjne
Środki techniczne	• urządzenia podtrzymujące zasilanie, • karty magnetyczne i mikroprocesorowe, • urządzenia do identyfikacji osób, tzw. urządzenia biometryczne, • urządzenia wykorzystywane do tworzenia kopii zapasowych wraz z metodami ich stosowania, • zapory ogniowe – firewall i serwery Proxy, • sprzętowe blokady dostępu do klawiatur, napędów dysków, • dublowanie okablowania
Środki programowe	• dzienniki systemowe, • programy śledzące, czyli mechanizmy umożliwiające monitoring pracy użytkowników systemu w czasie rzeczywistym, • mechanizmy rozliczania, czyli rozwiązania pozwalające na identyfikację wykonawców określonych operacji w systemie, • programy antywirusowe, programy wykrywające słabe hasła istniejące w systemie, kody korekcyjne
Środki kontroli dostępu	• hasła, numery identyfikacyjne, karty magnetyczne, • metody biometryczne
Środki kryptograficzne	• algorytm DES oraz jego modyfikacje, algorytm IDEA, algorytm RSA

Źródło: opracowanie własne na podstawie: *Technologie informatyczne w bankowości*, red. A. Gospodarowicz, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2002, s. 193–203; por. D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, w: *Bankowość elektroniczna*, red. A. Gospodarowicz, PWE, Warszawa 2005, s. 63–78; M. Kopczewski, E. Czapik-Kowalewska, *Zagrożenia sieciowe a bezpieczeństwo informacyjne*, http://mit.weii.tu.koszalin.pl/MIT6/Modele%20inzynierii%20teleinformatyki%206_08%20Kopczewski%20Czapik%20Kowalewska.pdf [dostęp 21.04.2016].

Aby zapewnić odpowiedni poziom bezpieczeństwa systemów bankowych, są używane liczne narzędzia informatyczne, wśród których można wyróżnić: analizatory wersji oprogramowania i pakietów naprawczych, skanery zabezpieczeń, analizatory bezpieczeństwa haseł użytkowników, pułapki i przynęty, narzędzia do wykrywania nadużyć i włamań czy też ochronę przed błędami oprogramowania[19].

Instytucje bankowe widziane przez pryzmat bezpieczeństwa są w pewnym sensie specyficzne, z jednej strony bank udostępnia swoje zasoby informatyczne,

[19] T. Bilski, *Nowe narzędzia do ochrony systemów informatycznych w bankowości*, w: *Zastosowania rozwiązań informatycznych w bankowości*, red. A. Gospodarowicz, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2000, s. 394–407.

z drugiej strony klient też musi skorzystać z połączenia internetowego, które może nieść ze sobą pewne niebezpieczeństwa. Takie otwarcie systemów na zewnątrz oczywiście stwarza możliwość ataku hakerów, którzy mogą próbować włamać się do sieci. Jednym z zabezpieczeń przed tym jest ściana ogniowa. Technologia ta zabezpiecza przed niedozwolonymi sposobami komunikacji z serwerem, co w praktyce oznacza niedopuszczenie przepływu danych na innych portach niż dozwolone. Z wielu opracowań można dowiedzieć się o różnych rodzajach zabezpieczeń stosowanych w bankowości internetowej. W większości przeważają jednak cztery główne[20]:

- szyfrowanie transmisji danych;
- proste uwierzytelnianie, np. login, hasło;
- silne uwierzytelnianie, np. token;
- podpis elektroniczny[21].

Pierwsza metoda jest ściśle związana z kryptografią, a jej stosowanie ma na celu uniemożliwienie dostępu osobom nieupoważnionym do poufnych danych przesyłanych drogą elektroniczną. Druga i trzecia metoda, jak sama nazwa wskazuje, służy identyfikacji stron transakcji i ma na celu uniemożliwienie zaistnienia sytuacji, w których jedna osoba podszywa się pod inną osobę. Z kolei czwarta metoda ma związek z zasadą niezaprzeczalności. Jednocześnie podpis elektroniczny pełni funkcję uwierzytelniania strony transakcji[22].

Budując bezpieczny system informatyczny, należy pamiętać o[23]:

- wydzieleniu sieci komputerowych o zróżnicowanych stopniach „zmilitaryzowania";
- stosowaniu urządzeń filtrujących ruch sieciowy (firewall);
- zdefiniowaniu zasad bezpieczeństwa i uprawnień zarówno w stosunku do poszczególnych modułów systemu, jak i do poszczególnych ról użytkowników;
- zdefiniowaniu zasad fizycznego dostępu do serwerów i innych kluczowych elementów systemu;

---

[20] Por. P. Wroński, *Bankowość elektroniczna dla firm*, CeDeWu, Warszawa 2004, s. 57; A. Jurkowski, *Bankowość elektroniczna*, „Materiały i Studia" 2001, nr 125, Narodowy Bank Polski, s. 18–23.

[21] Szerzej zob. M.M. Skarbek, *Podpis elektroniczny*, „Bank" 2002, nr 9, s. 57–59; I. Paprotna, *Gwarancja bankowa w formie elektronicznej*, „Bank" 2003, nr 4, s. 56–59; K. Gaińska, *Znaczenie podpisu elektronicznego dla funkcjonowania podmiotów gospodarczych*, w: *Technologie informacyjne w finansach i rachunkowości*, red. N. Siemieniuk, J. Sikorski, Uniwersytet w Białymstoku, Białystok 2003, s. 274–287; P. Hołownia, *Zrozumieć także klienta*, „Bank" 2007, nr 1, s. 22; E. Włodarczyk, *Certyfikat nie do złamania*, „Bank" 2007, nr 5, s. 49.

[22] A. Jurkowski, op.cit., s. 18–23.

[23] M. Jaślan, op.cit., s. 47.

- odpowiedniej organizacji monitorowania pracy systemu ze szczególnym uwzględnieniem procedur zapobiegania i wykrywania włamań;
- logowaniu wszystkich dostępów do danych systemu;
- wprowadzeniu procedur monitoringu operacji oraz możliwości przeprowadzenia dodatkowej weryfikacji.

Instytucje bankowe, zgodnie ze strategią lizbońską[24], stale opracowują i wdrażają różnorodne techniki zabezpieczeń, aby przekonać klientów o dużym bezpieczeństwie przy samoobsługowym korzystaniu z usług i produktów bankowych. Do najnowszych zalicza się rozwiązania biometryczne[25]. Biometria umożliwia identyfikację klienta banku na podstawie cech ludzkich. Rozróżnia się cechy fizyczne, do których należą m.in. obraz tęczówki czy linie papilarne (np. palca), oraz cechy behawioralne, do których należy np. głos[26].

Biometria jest sprawdzona pod względem technologii, rośnie jej popularność, a dzięki niej banki umożliwiają swoim klientom przejście na nowy, wyższy poziom obsługi i gwarantują bezpieczeństwo. Polska była pierwszym krajem Unii Europejskiej, w którym biometria została przyjęta do rozwiązań bankowych – służy do weryfikacji tożsamości klientów i pracowników oraz do uwierzytelnienia transakcji i operacji[27].

5. Podsumowanie

Techniki stosowane przez cyberwłamywaczy są coraz bardziej wyrafinowane. Aby sprostać zagrożeniom oraz maksymalnie utrudnić dostęp osób niepowołanych do systemu bankowego, banki powinny stosować zabezpieczenia wielopoziomowe, które zawsze są najskuteczniejsze. Nie powinny opierać się wyłącznie na programie antywirusowym, ale korzystać kompleksowo również z systemów: przeciwdziałających włamaniom, monitorujących ruch w sieci wewnętrznej, wykrywających fraudy, przeciwdziałających wyciekom informacji, śledzących anomalie w systemach, analizujących zdarzenia istotne z punktu

[24] Szerzej zob. I. Gębska-Nędzi, *Gdyby nie one…*, „Bank" 2006, nr 9, s. 24–25.

[25] A. Janc, *Komputeryzacja usług bankowych i warunki jej wdrażania*, w: *Nowe usługi bankowe na tle wybranych problemów organizacji i zarządzania bankiem uniwersalnym*, red. A. Janc, Akademia Ekonomiczna w Poznaniu, Poznań 2001, s. 12–23.

[26] W. Grudzień, P. Gałuszyński, *Biometria w banku*, „Gazeta Bankowa", 2007, nr 8, s. 343; P. Pietkun, *Biobezpieczeństwo*, „Gazeta Bankowa" 2007, nr 50, s. 56–57.

[27] M. Kubiak, *Biometria technologią przyszłości*, „Człowiek i Dokumenty" 2012, nr 27.

widzenia bezpieczeństwa i kontrolujących logi systemowe oraz dzienniki zdarzeń systemów. Systemy zabezpieczeń to jednak nie wszystko. Banki powinny nieustannie analizować swoje systemy pod kątem podatności – czyli znanych i na bieżąco wykrywanych luk w oprogramowaniu – by zidentyfikowane likwidować, zanim staną się celem ataków hakerskich. Powinny też testować systemy równie skutecznie, jak robią to hakerzy, oraz jak najsprawniej reagować na incydenty, jeśli takowe już nastąpią.

Podsumowując: banki, prowadząc własny monitoring bezpieczeństwa systemów informatycznych, odnoszą wiele korzyści, do których m.in. należą: podniesienie poziomu bezpieczeństwa chronionych zasobów, możliwość podejmowania natychmiastowych kroków naprawczych w przypadku nieprawidłowości, natychmiastowe informowanie o naruszeniach bezpieczeństwa kierownictwa, koordynacja działań służb wewnętrznych w przypadku wystąpienia zagrożeń, podniesienie jakości usług realizowanych przez podmioty zewnętrzne, możliwość jednoczesnego rozliczania realizacji usług, krótkoterminowa analiza raportów, pozwalająca na klasyfikację i prezentację zdarzeń alarmowych.

Bibliografia

Balcerzak P.M., *Bank i klient: potrzebujemy cybertarczy sektora bankowego*, „Bank" 2015, nr 5, s. 40.

Bilski T., *Nowe narzędzia do ochrony systemów informatycznych w bankowości*, w: *Zastosowania rozwiązań informatycznych w bankowości*, red. A. Gospodarowicz, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2000, s. 394–407.

Gaińska K., *Znaczenie podpisu elektronicznego dla funkcjonowania podmiotów gospodarczych*, w: *Technologie informacyjne w finansach i rachunkowości*, red. N. Siemieniuk, J. Sikorski, Uniwersytet w Białymstoku, Białystok 2003, s. 274–287.

Gębska-Nędzi I., *Gdyby nie one…*, „Bank" 2006, nr 9, s. 24–25.

Grandys A., *E-bankowość – bankowość gospodarki cyfrowej*, cz. 2, „Monitor Rachunkowości i Finansów" 2001, t. 6, s. 49–50.

Grobicki J., *Wirtualne, czyli realne straty*, „Bank" 2005, nr 7–8, s. 63.

Grudzień W., Gałuszyński P., *Biometria w banku*, „Gazeta Bankowa" 2007, nr 8, s. 343.

Hołownia P., *Zrozumieć także klienta*, „Bank" 2007, nr 1, s. 22.

Janc A., *Komputeryzacja usług bankowych i warunki jej wdrażania*, w: *Nowe usługi bankowe na tle wybranych problemów organizacji i zarządzania bankiem uniwersalnym*, red. A. Janc, Akademia Ekonomiczna w Poznaniu, Poznań 2001, s. 12–23.

Jaślan M., *Meandry bezpieczeństwa danych. Zabezpieczenia danych. Monitoring i bezpieczeństwo*, „Bank" 2008, nr 3, s. 47.

Jurkowski A., *Bankowość elektroniczna*, „Materiały i Studia" 2001, nr 125, Narodowy Bank Polski, s. 18–23.

Kosiur D., *Understanding Electronic commerce*, Microsoft Press, Redmond 1997.

Kubiak M., *Biometria technologią przyszłości*, „Człowiek i Dokumenty" 2012, nr 27.

Lynch D., Lyndquist L., *Digital Money: the New era of Internet commerce*, J. Wiley & Sons Inc., New York 1996.

Michalski A., *Wykorzystanie technologii systemów informatycznych w procesach decyzyjnych*, Politechnika Śląska, Gliwice 2002.

Paprotna I., *Gwarancja bankowa w formie elektronicznej*, „Bank" 2003, nr 4, s. 56–59.

Pietkun P., *Biobezpieczeństwo*, „Gazeta Bankowa" 2007, nr 50, s. 56–57.

Skarbek M.M., *Podpis elektroniczny*, „Bank" 2002, nr 9, s. 57–59.

Technologie informatyczne w bankowości, red. A. Gospodarowicz, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2002.

Wawrzyniak D., *Bezpieczeństwo bankowości elektronicznej* w: *Bankowość elektroniczna*, red. A. Gospodarowicz, PWE, Warszawa 2005, s. 63–78.

Węsierska E., *Dywersyfikacja metod ochrony systemów elektronicznych jako warunek funkcjonowania przedsiębiorstwa bankowego*, w: *Zastosowania rozwiązań informatycznych w instytucjach finansowych*, red. A. Gospodarowicz, „Prace Naukowe", nr 1035, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław 2004, s. 130–143.

Włodarczyk E., *Certyfikat nie do złamania*, „Bank" 2007, nr 5, s. 49.

Wroński P., *Bankowość elektroniczna dla firm*, CeDeWu, Warszawa 2004.

Źródła sieciowe

Bankowość internetowa. Bezpieczeństwo transakcji bankowych w Internecie, Związek Banków Polskich, http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=9 [dostęp 21.04.2016].

http://docplayer.pl/13356535-Bezpieczenstwo-systemu-informatycznego-banku-informatyka-bankowa-wsb-w-poznaniu-dr-grzegorz-kotlinski.html [dostęp 18.04.2016].

http://docplayer.pl/2924076-Cechy-i-zadania-systemu-informatycznego-banku-informatyka-bankowa-wsb-w-poznaniu-dr-grzegorz-kotlinski.html [dostęp 12.04.2016].

Kopczewski M., Czapik-Kowalewska E., *Zagrożenia sieciowe a bezpieczeństwo informacyjne*, http://mit.weii.tu.koszalin.pl/MIT6/Modele%20inzynierii%20teleinformatyki%206_08%20Kopczewski%20Czapik%20Kowalewska.pdf [dostęp 21.04.2016].

Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, Warszawa 2002, https://www.knf.gov.pl/Images/rekomendacja_d_tcm75-8552.pdf [dostęp 12.04.2016].

Wojciechowska-Filipek S., *Metody kontroli dostępu w bankowości elektronicznej*, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/115.pdf [dostęp 03.04.2016].

* * *

Security Systems in Banking Institutions

Abstract

The aim of the publication is to analyze the security of information systems in banking institutions in Poland. The analysis was conducted based on the available literature. The results show that without continuous monitoring of security of information systems, the development of banking institutions, and hence of electronic services, is not possible.

Keywords: information systems, information system security, the threat of information systems