*Dariusz Garczyński**

TECHNOLOGICZNE ASPEKTY RYZYKA OPERACYJNEGO W BANKACH

Wprowadzenie

W ostatnich latach zauważyć można bardzo intensywny rozwój nowoczesnych technologii informatyczno-telekomunikacyjnych, który bezpośrednio lub pośrednio wpływa na sposób prowadzenia działalności przez banki. Stanowi on dla nich nie tylko okazję do wprowadzania nowych produktów i usług za pomocą innowacyjnych kanałów komunikacji elektronicznej, ale jest też poważnym zagrożeniem, powodującym wzrost ryzyka bankowego. Bez wątpienia bowiem technologie informatyczne z jednej strony otwierają przed bankami nowe możliwości, z drugiej strony pojawiają się nowe zagrożenia związane przede wszystkim z bezpieczeństwem bankowych systemów informatycznych i próbami jego naruszania.

Prezentowany artykuł charakteryzuje podstawowe obecnie technologie komunikacji elektronicznej z punktu widzenia ich zastosowania w bankowości, wskazując na ich wpływ na poziom ryzyka bankowego oraz jedno z najczęściej stosowanych obecnie narzędzi uzyskiwania nieautoryzowanego dostępu do zasobów systemu informatycznego, jakim jest inżynieria socjalna (*social engineering*). Ze względu na ograniczone ramy artykułu kwestie związane z zapobieganiem zagrożeniom ze strony tych technologii zostaną tylko zasygnalizowane, stanowiąc inspirację do dalszych publikacji.

1. Ryzyko informatyczne a ryzyko operacyjne

Systemy informatyczne wspomagają obecnie pracę niemal wszystkich obszarów działalności bankowej. Najbardziej widocznym przejawem ich funkcjonowania

* Uniwersytet Ekonomiczny we Wrocławiu, Wydział Zarządzania, Informatyki i Finansów.

w sektorze bankowym jest bez wątpienia powstanie i rozwój bankowości elektronicznej. Proces ten dostrzegły instytucje nadzoru finansowego, w tym przede wszystkim Bazylejski Komitet Nadzoru Bankowego, który już w 1998 r. doprowadził do powstania zespołu pod nazwą Electronic Banking Group (EBG), odpowiedzialnego za opracowywanie zaleceń i rekomendacji w zakresie praktyk nadzorczych w obszarze bankowości elektronicznej. EBG jednoznacznie stwierdza, że bankowość elektroniczna modyfikuje niektóre rodzaje ryzyka bankowego, a w szczególności wpływa na wzrost zagrożenia ryzykiem operacyjnym.

Do podstawowych cech bankowości elektronicznej, które powodują konieczność nowego spojrzenia na zarządzanie ryzykiem bankowym, Komitet Bazylejski zalicza:

- bezprecedensową szybkość zmian w zakresie innowacji technologicznych i obsługi klienta,
- wszechobecny, globalny charakter otwartych sieci elektronicznych,
- integrację aplikacji bankowości elektronicznej z pozostałymi systemami komputerowymi,
- rosnące uzależnienie banków od stron trzecich dostarczających niezbędnej technologii informatycznej.

Jak wspomniano wcześniej, systemy informatyczne znajdują zastosowanie w każdym obszarze działalności bankowej, wspomagają praktycznie każdą czynność i proces bankowy. Ryzyko informatyczne, związane z możliwością wystąpienia negatywnego zjawiska powodującego określone straty w systemie informatycznym, stanowi więc element ryzyka operacyjnego, rozumianego jako ryzyko bezpośrednich i pośrednich strat wynikających z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub z przyczyn zewnętrznych[1].

W opublikowanym w 2013 r. raporcie *Digital Trends 2013*[2], firma Deloitte wymienia osiem głównych trendów mających największy wpływ na gospodarkę elektroniczną na świecie. Wśród nich kluczowymi, z punktu widzenia ryzyka informatycznego, dla sektora bankowego są:

- rozwój technologii mobilnych,
- powstanie i rozwój mediów społecznościowych,
- coraz powszechniejsze wykorzystanie chmur obliczeniowych.

[1] KNF, Rekomendacja M, załącznik do Uchwały KNF z dn. 8.01.2013, Dz. Urz. KNF 2013, poz. 6.

[2] www.deloitte.com/assets/Dcom-Poland/Local%20Assets/Documents/Raporty,%20badania, %20rankingi/Digital_Trends_1.pdf, dostęp 20.03.2015.

2. Technologie mobilne

Pod pojęciem technologii mobilnych rozumie się zazwyczaj kombinację technologii samej sieci bezprzewodowej oraz technologii urządzeń mobilnych (wraz z instrumentami identyfikacyjnymi)[3]. Pierwsza generacja bezprzewodowych sieci komunikacyjnych opierała się na technologii analogowej (AMPS – Advanced Mobile Phone System) i jako taka nie nadawała się do transmisji cyfrowej. Przełomem w rozwoju technologii sieci bezprzewodowych stała się druga generacja – 2G, umożliwiała bowiem jednoczesną transmisję głosu i danych. Obecnie stosowane technologie UMTS i HSPA (trzeciej generacji) pozwalają na przesyłanie danych z dużą prędkością, co umożliwia stosowanie rozbudowanych aplikacji mobilnych, operujących na dużych zbiorach danych. Ostatnio zaprezentowano sieć czwartej generacji – LTE (Long Term Evolution), której podstawową cechą jest prawie czterokrotne zwiększenie przepustowości sieci komórkowych.

Możliwości samych urządzeń mobilnych rosły równolegle do rozwoju technologii sieci bezprzewodowych – od prostych telefonów z niewielkim monochromatycznym wyświetlaczem znakowym do zaawansowanych technologicznie urządzeń, będących w istocie komputerami. Także narzędzie identyfikacji właściciela urządzenia mobilnego – tzw. karta SIM (Subscriber Identity Module), ewoluowało od instrumentu typowo identyfikacyjnego po wszechstronny układ, spełniający funkcje nie tylko identyfikacyjne, ale też zarządzające połączeniami (np. roamingiem) lub zabezpieczający transakcje mobilne.

Bankowość mobilna jest najnowszym kanałem bankowości elektronicznej, zapewniającym wygodny sposób dokonywania operacji bankowych za pomocą telefonu komórkowego lub innego urządzenia przenośnego. Zainteresowanie banków tym sposobem komunikacji z klientem wiąże się z rosnącą dostępnością i coraz większymi możliwościami samych urządzeń oraz rozwojem infrastruktury telekomunikacyjnej na całym świecie. Konkurencja wśród dostawców usług telekomunikacyjnych i rozwój technologii powodują stałe obniżanie kosztów transmisji danych, co dodatkowo stymuluje wzrost rynku komunikacji mobilnej. Ważnym czynnikiem wzrostu jest także „mobilny" styl życia, czyli moda na nowoczesne gadżety telefonii komórkowej lub inne urządzenia przenośne typu PDA czy tablet.

[3] *The Internet Encyclopedia*, Vol. 2, red. H. Bigdoli, J. Wiley & Sons, 2004, s. 618–619.

Usługi bankowości mobilnej oferowane są klientom już od początku XXI w., ale ich akceptacja postępuje stosunkowo wolno z następujących powodów[4]:

- koszt dostępu do sieci Internet (pomimo faktu, że koszty transferu danych są coraz niższe) sprawia wciąż, że klienci niechętnie wykorzystują aplikacje mobilne),
- nieintuicyjny interfejs użytkownika (istotną kwestią w projektowaniu interfejsu urządzeń mobilnych jest jego prostota i adaptowalność do wymagań użytkownika, ważne także z tego powodu, że warunki pracy z urządzeniem mobilnym zazwyczaj różnią się od warunków pracy z urządzeniem stacjonarnym – ruch uliczny, warunki atmosferyczne, itp.),
- brak wiedzy o możliwościach bankowości mobilnej (wielu klientów banku nie ma świadomości istnienia takiego kanału dostępu lub nie zna korzyści płynących z jego wykorzystania),
- ograniczenia funkcjonalności urządzeń mobilnych (technologie mobilne są wciąż ograniczone jakością lub niedostatecznym rozwojem samych urządzeń mobilnych czy infrastrukturą, w której muszą pracować; ograniczenia to np. słaba jakość baterii, wielkość i rozdzielczość ekranu, pojemność pamięci, niepewna jakość połączenia sieciowego),
- dostępność sieci bezprzewodowych (co prawda w wielu miejscach istnieją punkty dostępowe do Internetu, ale wciąż są „białe plamy" w pokryciu sieci, z drugiej strony jakość i szybkość połączenia może być niezadowalająca przy stosowaniu aplikacji bankowych),
- bezpieczeństwo (zaawansowane technologie mobilne, podobnie jak technologie informatyczne, narażone są na wiele zagrożeń związanych z atakami wirusów lub hakerów, możliwością przechwycenia czy modyfikacji transmitowanych danych, kradzieżą haseł itp.),
- sprawy organizacyjne (aby oferować usługi bankowości mobilnej konieczna staje się zazwyczaj modyfikacja struktury organizacyjnej oraz procesów biznesowych w banku),
- mały wybór (nie wszystkie banki oferują tego typu dostęp),
- przeładowanie technologią i informacją (zbyt duża liczba zaawansowanych technologicznie urządzeń, które współczesny konsument posiada i użytkuje, powoduje obniżenie zdolności percepcji informacji, które napływają w zbyt dużej ilości ze zbyt dużej liczby kanałów).

[4] M. Shah, S. Clarke, *E-Banking Management: Issues, Solutions and Strategies*, ISR, Hershey, New York 2009, s. 33–36.

3. Przetwarzanie w chmurze jako nowy model dostarczania usług IT

Przetwarzanie w chmurze (*cloud computing*) lub chmura obliczeniowa to nazwy modelu przetwarzania opartego na idei usług IT dostarczanych na żądanie klienta. Jest to stosunkowo nowy model przetwarzania. Chmura obliczeniowa z punktu widzenia użytkownika stanowi wygodny sposób prowadzenia działalności, bez konieczności zakupu własnego sprzętu komputerowego, oprogramowania systemowego i aplikacji biznesowych. Według amerykańskiego instytutu NIST (National Institute of Standards and Technology), chmurę obliczeniową można scharakteryzować poprzez pięć cech[5]:

- samodzielne korzystanie z usługi dostarczonej na żądanie (*on-demand self-service*),
- swobodny dostęp poprzez sieć (*broad network access*),
- agregacja zasobów niezależnie od lokalizacji (*resource pooling*),
- natychmiastowa elastyczność (*rapid elasticity*),
- płatność tylko za wykorzystane zasoby (*measured service*).

Istnieje kilka modeli chmury obliczeniowej:

- Infrastructure as a Service (IaaS) – klient otrzymuje infrastrukturę informatyczną (sprzęt, odpowiednio przygotowane pomieszczenia, oprogramowanie) wraz z serwisowaniem,
- Platform as a Service (PaaS) – klient otrzymuje funkcjonalność IaaS oraz platformę aplikacyjną,
- Software as a Service (SaaS) – najbardziej rozbudowany model chmury, gdzie klient otrzymuje funkcjonalność PaaS wraz z potrzebnymi mu aplikacjami.

Mogą one występować jako:

- chmury prywatne – wykorzystywane przez jednego klienta,
- chmury publiczne – udostępniane wielu klientom,
- chmury hybrydowe – łączą cechy chmur prywatnych i publicznych,
- chmury wspólnotowe –udostępniane klientom spełniającym te same standardy (np. bezpieczeństwa).

Ze względu na stosunkowo krótki okres wykorzystywania chmur obliczeniowych w praktyce, trudno jest jednoznacznie określić, czy stanowią one tylko nowinkę technologiczną, czy też wpiszą się na stałe do kanonu modeli przetwarzania. Do niewątpliwych zalet tego rodzaju wykorzystywania zasobów IT zalicza się przede wszystkim dużą elastyczność i koszt, na ogół niższy niż w tradycyjnych rozwiązaniach. Wadami chmur obliczeniowych, ważnymi z punktu widzenia informatyki bankowej, są brak

[5] G. Petri, *Shedding Light on Cloud Computing*, CA Technologies, 2010, s. 4.

kontroli nad danymi przekazywanymi do chmury oraz brak szczegółowych uregulowań prawnych, szczególnie dla chmur istniejących w innych krajach niż kraj klienta.

4. Media społecznościowe

Pojęcie media społecznościowe (*social media*) w potocznym rozumieniu używane jest na określenie wszystkich sposobów publikacji treści w sieci Internet, przez wszystkich użytkowników, nie tylko przez profesjonalnych twórców zawartości stron internetowych. Rozwój mediów społecznościowych, jaki można zaobserwować w ostatnich latach, umożliwiły dwie koncepcje związane z technologiami informatycznymi – Web 2.0 i User Created Content (treści tworzone przez użytkownika)[6]. Koncepcja Web 2.0 powstała jako rezultat kryzysu związanego z pęknięciem tzw. bańki internetowej w 2001 r., czyli załamaniem się rynku spółek branży IT i pokrewnych. Sam termin „Web 2.0" użyty został po raz pierwszy w 2004 r. dla opisania nowego podejścia do tworzenia narzędzi oraz treści zamieszczanych w sieci Internet[7].

Podstawową cechą tego podejścia było rozumienie ogólnoświatowej sieci Internet jako platformy tworzenia i publikowania treści nie przez pojedynczych autorów, ale przez wszystkich użytkowników. Przykładowo, serwis Encyclopedia Britannica Online[8], jako tworzony przez grupę specjalistów, zalicza się do ery Web 1.0, natomiast serwis Wikipedia[9], tworzony przez wszystkich użytkowników Internetu (po spełnieniu pewnych warunków) jest elementem Web 2.0. Choć termin Web 2.0 (oraz Web 1.0) nie odnosi się do jakiejś konkretnej wersji WWW (jak to ma miejsce w wypadku kolejnych wersji oprogramowania komputerowego), to charakterystyczne jest wykorzystywanie pewnych narzędzi zapewniających określoną funkcjonalność, takich jak wtyczki Flash (umożliwiające dodawanie animacji, interakcji i strumieni audio/video do stron internetowych), kanały RSS (pozwalające automatycznie przesłać subskrybowane wiadomości z określonych stron WWW) lub skryptów Java (zapewniające interaktywność ze stronami WWW poprzez reakcję na zdarzenia lub możliwość budowania elementów nawigacyjnych). Druga z koncepcji, które legły u podstaw rozwoju mediów społecznościowych, to User Created Content, czyli treści tworzone

[6] A. Kaplan, M. Haenlein, *Users of the world, unite! The challenges and opportunities of Social Media*, "Business Horizons" 2010, No. 53(1), s.60.

[7] T. O'Reilly, *What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software,* oreilly.com, dostęp 20.03.2015.

[8] www.britannica.com, dostęp 20.03.2015.

[9] www.wikipedia.com, dostęp 20.03.2015.

przez użytkownika. Koncepcja ta może być rozumiana jako różnorakie formy dostępnych publicznie treści medialnych, tworzonych przez użytkowników końcowych.

W 2007 r. OECD sformułowała trzy kryteria[10], które musi spełniać treść, aby mogła być uważana jako UCC. Po pierwsze, musi być zamieszczona w Internecie w miejscu publicznie dostępnym, lub, jeśli jest zawężona do pewnego kręgu odbiorców, nie może pochodzić ze źródeł prywatnych (typu poczta elektroniczna lub komunikatory). Po drugie, musi nosić cechy kreacji autorskiej, to znaczy w całości lub znaczącej części być efektem oryginalnej pracy poszczególnych użytkowników, co wyklucza na przykład zamieszczanie kopii istniejącego artykułu na własnym blogu bez jakichkolwiek modyfikacji lub komentarzy. Po trzecie, powinna być efektem pozaprofesjonalnej działalności twórcy, nienastawionego na efekty komercyjne.

Najbardziej znanym i największym portalem społecznościowym jest Facebook (www.facebook.pl). W styczniu 2014 r. liczba użytkowników portalu na całym świecie wynosiła ponad miliard osób, a co miesiąc wgrywanych jest ponad 1 mld zdjęć oraz 10 mln filmów, których obecnie jest ok. 265 mld. Tak duża popularność portalu sprawia, że stanowi on dobre medium do komunikacji pomiędzy instytucjami finansowymi a klientami (także potencjalnymi). Pod koniec 2013 r. Facebook ogłosił sukces w implementacji swoich rozwiązań w Commonwealth Banku[11] w Australii. Użytkownicy społecznościowego medium, będący jednocześnie klientami tego banku, mogą z poziomu Facebooka dokonywać przelewów na rachunki zarówno firm, jak i znajomych. Transakcje są zabezpieczane przez wewnętrzne systemy bankowe.

Jednym z pierwszych banków na świecie, wykorzystujących Facebook do realizacji płatności elektronicznych, był także bank Alior Sync (obecnie pod marką T-mobile usługi bankowe). Specjalne, powiązane z portalem, konto pozwala na łatwy i szybki przelew środków na rachunek odbiorcy. Zrealizowanie pierwszego przelewu wymaga zalogowania się do bankowości internetowej banku – kolejne można już zlecać bezpośrednio z portalu. Aby móc przelewać środki do swoich znajomych na portalu, należy otworzyć specjalny rachunek powiązany z portalem oraz zainstalować dedykowaną aplikację. Transakcja kończy się autoryzacją kodem SMS, co gwarantuje pełne bezpieczeństwo. Ze względów bezpieczeństwa wprowadzono limit maksymalnej wielkości kwoty jednorazowego przelewu. Odbiorca płatności nie musi być klientem banku, jednak aby przelew mógł być zrealizowany, także powinien zainstalować na Facebooku odpowiednią aplikację, podać swoje imię i nazwisko oraz numer rachunku bankowego, na który będą trafiać przekazywane środki.

---

[10] *Participative web and user-created content: Web 2.0, wikis, and social networking*, Paris 2007, Organisation for Economic Co-operation and Development, s. 18.

[11] www.facebook.com/commonwealthbank, dostęp 20.03.2015.

5. Inżynieria społeczna jako zagrożenie bezpieczeństwa informatycznych systemów bankowych

Pojęcie inżynierii socjalnej (socjotechniki, inżynierii społecznej) nie doczekało się jeszcze jednej, ogólnie obowiązującej definicji. T. Trejderowski[12] definiuje socjotechnikę jako „ogół metod, działań i środków praktycznych zmierzających do uzyskania pożądanego zachowania jednostek czy też grup ludzkich; innymi słowy, zmierzających do wywołania pożądanych przemian w postawach i zachowaniach społecznych". Podobnie pojmuje socjotechnikę A. Podgórecki[13], wskazując na jej praktyczny aspekt – „socjotechnika jako »nauka praktyczna«dostarcza wiedzy, której zastosowanie, używając odpowiednich instrumentów i środków, pozwala na skłonienie jednostek bądź grupy osób do zachowań oczekiwanych przez sprawców oddziaływań".

Niekwestionowany autorytet w dziedzinie cyberprzestępstw – K. Mitnick[14] uwzględnia w swojej definicji socjotechniki ważne z punktu widzenia technologii informatycznych aspekty – „Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji".

R. Cialdini[15] podaje siedem najważniejszych reguł socjotechniki. Są to:

- reguła wzajemności, polega na potrzebie odwzajemnienia doznanego dobra. Podobnie doznanie z czyjejś strony krzywdy wywołuje dokładnie taką samą reakcję,
- reguła sympatii opiera się na miłych skojarzeniach lub ciepłych uczuciach wywoływanych przez manipulatora. W tym wypadku uczucie przyjaźni wykorzystywane jest jako narzędzie służące do wywierania wpływu na innych,
- reguła niedostępności, której podstawą są sztucznie wykreowane, bezpowrotnie przemijające okazje. Mówi ona, że ograniczoność dóbr, jak i czasu ich dostępności dla zainteresowanego, powoduje automatyczny i sztuczny wzrost ich wartości,
- reguła społecznego dowodu słuszności – wykorzystuje ona tendencję do powielania zachowań masowych,
- reguła konsekwencji, wykorzystująca ludzką cechę konsekwentnego podążania za obranym celem,

---

[12] T. Trejderowski, *Socjotechnika: podstawy manipulacji w praktyce*, Eneteia, Warszawa 2009, s. 33.
[13] A. Podgórecki, *Zasady socjotechniki*, Wiedza Powszechna, Warszawa 1966, s. 9.
[14] K. Mitnick, *Sztuka podstępu*, Helion 2003, s. 360.
[15] R. Cialdini, *Wywieranie wpływu na ludzi, Teoria i praktyka*, Wydawnictwo Gdańskie Psychologiczne, Gdańsk 2013.

- reguła autorytetu opiera się na naszej głęboko zakorzenionej potrzebie ulegania osobom społecznie ważnym i uznanym,
- reguła wartości, zwana również regułą maksymalizacji własnego zysku, polega na utożsamianiu rzeczy (pojęć) drogich z rzeczami (pojęciami) dobrej jakości.

Zastosowanie reguł socjotechniki zazwyczaj przeprowadzane jest na osobie reprezentującej jedną z grup:

- nieświadomi wartości informacji – pracownicy administracji, ochrony, recepcji ale także klienci bankowości elektronicznej,
- posiadający specjalne przywileje – pomoc techniczna, administratorzy systemów komputerowych, operatorzy komputerów, administratorzy systemów telefonicznych,
- producenci sprzętu i oprogramowania,
- określone wydziały – księgowość, kadry.

Do typowych metod socjotechnicznych wykorzystywanych w manipulacji Mitnick zalicza:

- udawanie pracownika tej samej firmy,
- udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej,
- udawanie kogoś, kto ma władzę,
- udawanie nowego pracownika proszącego o pomoc,
- udawanie przedstawiciela producenta systemu operacyjnego zalecającego pilną aktualizację,
- oferowanie pomocy w razie wystąpienia jakiegoś problemu, sprawienie, by problem wystąpił i manipulacja ofiarą w taki sposób, aby sama zadzwoniła z prośbą o pomoc,
- wysłanie darmowego programu do aktualizacji lub zainstalowania,
- wysłanie wirusa lub konia trojańskiego w załączniku do poczty,
- użycie fałszywego okna dialogowego wyświetlającego prośbę o powtórne załogowanie się lub wprowadzenie hasła,
- przechwytywanie naciśniętych klawiszy za pomocą specjalnego oprogramowania,
- podrzucenie w okolicach stanowiska pracy ofiary dyskietki lub płyty CD-ROM zawierającej niebezpieczny kod,
- używanie wewnętrznej terminologii i żargonu w celu zbudowania zaufania,
- oferowanie nagrody za rejestrację, poprzez wprowadzenie nazwy użytkownika i hasła na stronie internetowej,
- podrzucenie dokumentu lub pliku w pomieszczeniu poczty wewnętrznej firmy, aby dotarł do miejsca przeznaczenia jako korespondencja wewnętrzna,
- zmiana ustawień nagłówka w faksie tak, aby wydawał się pochodzić z wewnątrz,
- prośba do recepcjonistki o odebranie i przesłanie faksu dalej,

- prośba o transfer pliku do lokalizacji, która wydaje się wewnętrzna,
- ustawienie skrzynki poczty głosowej w taki sposób, że w trakcie oddzwaniania napastnik jest identyfikowany jako osoba z wewnątrz,
- podawanie się za pracownika z innego oddziału i prośba o tymczasowe otwarcie konta e-mail.

Niektóre z podanych wyżej metod stosowane są wobec klientów bankowości elektronicznej w celu uzyskania haseł dostępu do rachunku. Proceder wyłudzania haseł do zasobów systemów informatycznych nazywany jest *phishingiem* (podobno nazwa ta pochodzi od *password fishing* – łowienie haseł). Jak pokazuje badanie[16] przeprowadzone w maju 2012 r. przez O+K Research na zlecenie Kaspersky Lab, rozpoznanie takiej wiadomości nie zawsze jest łatwe. Aż 50% respondentów przyznało, że nie potrafi rozpoznać wiadomości *phishingowej* lub spreparowanej strony internetowej. Z badania wynika, że cyberprzestępcy, którzy wykorzystują *phishing* jako narzędzie do kradzieży danych, są głównie zainteresowani uzyskaniem nieautoryzowanego dostępu do kont na portalach społecznościowych, kont w systemach bankowości online oraz systemach płatności, jak również sklepach internetowych. Wyniki badania stanowią bezpośredni dowód na to, że metoda wykorzystująca masowe wysyłki przynosi efekty: około połowa respondentów przyznała, że trafiła już na podejrzaną korespondencję na portalach społecznościowych i w poczcie e-mail, 47% użytkowników komputerów PC otrzymało wiadomość z podejrzanym odsyłaczem lub załącznikiem, a 29% respondentów dostało wiadomość wysłaną w imieniu banku, portalu społecznościowego lub innego portalu wyglądającego na wiarygodny. Ponadto, 26% użytkowników przyznało, że ich komputery zostały zainfekowane w wyniku otworzenia załącznika do wiadomości, a 13% respondentów podało osobiste oraz finansowe dane na podejrzanych stronach.

Podsumowanie

Technologie informatyczne stanowią coraz ważniejsze narzędzie wspomagające pracę banku. Oprócz niewątpliwych korzyści z ich stosowania należy zauważać zagrożenia, które niosą. Zaprezentowane w artykule możliwości nowych technologii IT w zakresie mobilności, chmur obliczeniowych i mediów społecznościowych, mogą stanowić dla banku narzędzia zapewniające przewagę konkurencyjną, ale mogą być

[16] www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf, dostęp 20.03.2015.

jednocześnie przyczyną poważnych kłopotów. Wydaje się, że omówione technologie przez najbliższe lata będą wdrażane i rozwijane przez banki, stąd konieczność poszerzonej analizy zagrożeń, które ze sobą niosą. Przekracza to jednakże ramy przedstawianego artykułu.

Bibliografia

Cialdini R., *Wywieranie wpływu na ludzi, Teoria i praktyka*, Wydawnictwo Gdańskie Psychologiczne, Gdańsk 2013.

Kaplan A., Haenlein M., *Users of the world, unite! The challenges and opportunities of Social Media*, "Business Horizons" 2010, No. 53(1), 2010.

KNF, Rekomendacja M, załącznik do Uchwały KNF z dn. 8.01.2013, Dz. Urz. KNF z 2013, poz. 6.

Mitnick K., *Sztuka podstępu*, Helion, Warszawa 2003.

O'Reilly T., *What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software*, oreilly.com, dostęp 20.03.2015.

Participative web and user-created content: Web 2.0, wikis, and social networking, OECD, Paris 2007.

Petri G., *Shedding Light on Cloud Computing*, CA Technologies, 2010.

Podgórecki A., *Zasady socjotechniki*, Wiedza Powszechna, Warszawa 1966.

Shah M., Clarke S., *E-Banking Management: Issues, Solutions and Strategies*, ISR, Hershey, New York 2009.

The Internet Encyclopedia, Vol. 2, red. H. Bigdoli H., J. Wiley & Sons, 2004.

Trejderowski T., *Socjotechnika: podstawy manipulacji w praktyce*, Eneteia, Warszawa 2009.

www.britannica.com, dostęp 20.03.2015.

www.deloitte.com/assets/Dcom-Poland/Local%20Assets/Documents/ Raporty,%20badania, %20rankingi/Digital_Trends_1.pdf, dostęp 20.03.2015.

www.facebook.com/commonwealthbank, dostęp 20.03.2015.

www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf, dostęp 20.03.2015.

www.wikipedia.com, dostęp 20.03.2015.

Technological Aspects of the Operational Risk in Banks

The development of IT technology enables implementation of new tools that allow a bank to build competitive advantage. However, new technologies also cause increase of the risk level that is associated with them, which is part of the operational risk in the bank. Key trends in the development of electronic society not only generate potential profits for the banks but are a source of new threats that need to be analyzed in order to avoid potentially serious problems in the banking sector.

Keywords: operational risk, IT risk, mobile technology, social media, social engineering

Les aspects technologiques du risque opérationnel dans les banques

Le développement des TIC favorise la mise en œuvre de nouveaux outils qui permettent à une banque de construire un avantage concurrentiel. Cependant, les nouvelles technologies entraînent également une augmentation du risque technologique, qui fait partie du risque opérationnel de la banque. Les tendances clés dans le développement d'une société électronique non seulement génèrent des profits potentiels pour les banques, mais aussi elles sont une source de nouvelles menaces qui devraient être analysées afin d'éviter des problèmes potentiellement graves dans le secteur bancaire.

Mots-clés: le risque opérationnel, le risque informatique, la technologie mobile, les médias sociaux, l'ingénierie sociale

Технологические аспекты операционного риска банка

Развитие новых информационных технологий позволяет вводить все новые и новые инструменты создания конкурентного преимущества банка. Тем не менее, это приводит к увеличению, связанного с ними, риска, являющегося частью операционного риска банка. Основные тенденции в развитии электронного общества не только проносят банкам потенциальные прибыли, но и являются источником новых угроз, которые должны быть

проанализированы для того, чтобы избежать потенциально серьезные проблемы в банковском секторе.

Ключевые слова: операционный риск, риск ИТ, мобильные технологии, социальные медиа, социальная инженерия