Zeszyty Naukowe PWSZ w Płocku
Nauki Ekonomiczne, t. XXIV, 2016.

Radosław Bandera
Państwowa Wyższa Szkoła Zawodowa w Płocku

Jacek Grzywacz
Państwowa Wyższa Szkoła Zawodowa w Płocku

ZAGROŻENIA BEZPIECZEŃSTWA W BANKOWOŚCI ELEKTRONICZNEJ

Streszczenie

W artykule w sposób kompleksowy omówiono zagadnienia związane z bezpieczeństwem systemów informatycznych wykorzystywanych przez banki, w tym rodzaje zagrożeń oraz możliwości skutecznego zabezpieczenia się przed włamaniem do systemów. Dokonano oceny znaczenia i rodzajów zagrożeń dotyczących funkcjonowania w Polsce usług bankowości elektronicznej. Wskazano również na zasady kształtowania bezpieczeństwa tego rodzaju usług oraz realne źródła zagrożeń inicjowane głównie przez ludzi, w tym również grupy przestępcze.

Słowa kluczowe: polityka bezpieczeństwa, systemy zabezpieczeń, zagrożenia bezpieczeństwa, nadużycia informatyczne, nieuprawniony dostęp

Wstęp

Zapewnienie właściwego poziomu bezpieczeństwa jest problemem stale towarzyszącym działalności banków. Wynika to głównie ze specyfiki instytucji, którą jest bank i konieczności utrzymania zaufania społeczeństwa. Problem bezpieczeństwa jest zatem zawsze aktualny, niezależnie od charakteru usług świadczonych przez bank. Nie ulega przy tym wątpliwości, że istnieją istotne różnice jakościowe w ocenie bezpieczeństwa i warunkach jego kształtowania, jeśli dokona się rozróżnienia bankowości tradycyjnej, opartej głównie na bezpośrednich kontaktach z klientami, i tej nowoczesnej, w której podstawą świadczenia usług są nowoczesne technologie informatyczne. Wykorzystanie nowoczesnych technik sprawia, że kategoria bezpieczeństwa nabiera znacznie szerszego, interdyscyplinarnego charakteru i obejmuje, poza problemami technologicznymi, również kwestie ekonomiczne, organizacyjne i prawne.

W bankowości tradycyjnej zapewnienie bezpieczeństwa polegało głównie na wykorzystaniu różnorodnych systemów alarmowych oraz starannej we-

ryfikacji podpisów składanych przez klientów na dokumentach i zleceniach płatniczych. Systemy bezpieczeństwa obejmowały oczywiście również odpowiednie przygotowanie pomieszczeń w budynkach banków. Całkowicie odmienny charakter usług bankowości elektronicznej powoduje natomiast konieczność stosowania przez banki zupełnie innych zabezpieczeń, dających gwarancję należytej jakości usługi i utrzymania wysokiego poziomu zaufania klientów. Zgodnie z opinią D. Wawrzyniaka, wyrażoną w początkach XXI wieku, wiele działań realizowanych przez banki w Polsce w celu ochrony danych przetwarzanych w systemach informatycznych uważanych było za zło konieczne [Wawrzyniak, 2002, s.24]. Wydaje się zatem, że same banki nierzadko nie dostrzegały konieczności stałego doskonalenia i rozwoju systemów zabezpieczających przed nadużyciami o charakterze informatycznym. Argumentowały to z jednej strony wysokim poziomem funkcjonujących już rozwiązań oraz dużymi kosztami wprowadzania najnowocześniejszych technik zabezpieczających. Nadal niestety trudno jest jednoznacznie stwierdzić, czy bankowcy dysponują skutecznymi rozwiązaniami chroniącymi klientów przed utratą własnych środków.

Celem opracowania jest ocena znaczenia i rodzajów zagrożeń dotyczących funkcjonowania w Polsce usług bankowości elektronicznej. Wskazano tu na zasady kształtowania bezpieczeństwa tego rodzaju usług oraz realne źródła zagrożeń inicjowane głównie przez ludzi, w tym również grupy przestępcze.

1. Bezpieczeństwo usług bankowych

Zapewnienie poczucia bezpieczeństwa jest nieodzownym warunkiem korzystania przez klientów z nowoczesnych rozwiązań obsługi finansowej oferowanych przez banki. Należy przy tym zwrócić uwagę, że opinie na temat tego typu usług wśród różnych grup społecznych i zawodowych są dosyć zróżnicowane i zależą w istotnym stopniu od takich czynników jak wiek, wykształcenie, wykonywany zawód, dochody, miejsce zamieszkania, itd. Zróżnicowane poglądy maja na ten temat także przedsiębiorcy.

Wydaje się, że w niczym nie straciły na aktualności uwagi A. Gospodarowicza, określającego bankowość elektroniczną jako zbiór atrybutów, funkcjonujących na odpowiednim poziomie, a mianowicie [Gospodarowicz (red.), 2005, s.55]:

- **poufność**, czyli gwarancja o dostępie do danych jedynie osób uprawnionych,
- **integralność**, czyli gwarancja, że sposób przesyłania danych jest prawidłowy i nie mogą one być zmienione,
- **autentyczność**, czyli gwarancja, że osoba, która dokonuje transakcji jest tą, za którą się podaje,
- **niezaprzeczalność**, czyli brak możliwości zanegowania faktu, że wiadomość elektroniczna została nadana bądź odebrana,
- **niezawodność**, czyli gwarancja, że system działa we właściwy sposób oraz zgodnie z jego przeznaczeniem.

Trudno jest w sposób jednoznaczny wskazać warunki, których spełnienie gwarantuje pełne bezpieczeństwo bankowych usług elektronicznych. Jak wskazuje w swoim opracowaniu J. Grzywacz, wydaje się, że nadal jedną z najważniejszych kwestii, zwłaszcza w przypadku bankowości internetowej, jest zaimplementowanie przez bank następujących funkcjonalności [Grzywacz, 2016, s.119]:

- natychmiastowego potwierdzania tożsamości osób realizujących transakcję,
- stosowania skutecznego systemu szyfrowania transmisji informacji i zapewnienia jej całkowitej poufności,
- odpowiedniego zabezpieczenia serwera instytucji, będącej dostawcą internetowych usług finansowych, przed nielegalnym dostępem,
- zabezpieczenia serwera przed celowymi atakami przeprowadzanymi zarówno z zewnątrz (Internet), jak i od środka (sieć lokalna).

Z reguły banki stosują również szereg innych, dodatkowych zabezpieczeń, takich jak np. zablokowanie konta klienta w przypadku kilkukrotnego podania błędnego hasła lub PIN-u, a także wylogowanie z systemu przy całkowitym braku aktywności ze strony klienta. Niektóre banki wykorzystują również dodatkowe zabezpieczenia w postaci listy haseł jednorazowych, przesyłanej klientowi pocztą. Zawiera ona zbiór kodów oznaczonych numerami porządkowymi, każda zaś karta kodów jednorazowych ma swój własny numer. Każde hasło z tej listy może być wykorzystane tylko jeden raz, Z kolei każdy z kodów służy do autoryzacji tylko jednego zlecenia. Ich funkcją jest potwierdzenie uprawnień klienta do przeprowadzenia operacji na rachunku, wykonanie określonych operacji jest zaś możliwe po podaniu hasła o określonym numerze.

Chociaż zabezpieczenia stosowane obecnie przez banki mają coraz bardziej nowoczesny charakter i są stale udoskonalane, nawet bankowcy są zgodni, że nie ma w pełni bezpiecznego systemu, całkowicie gwarantującego bezpieczeństwo operacji przeprowadzanych drogą elektroniczną. Jak potwierdza praktyka, złamanie zabezpieczeń jest tylko kwestią czasu i środków niezbędnych przestępcom do zakupu odpowiedniego sprzętu komputerowego, wspomagającego łamanie szyfrów. Wraz z rozwojem nowoczesnej technologii sprzęt informatyczny staje się coraz tańszy, dlatego koszty nie stanowią dzisiaj istotnej bariery w działalności takich grup przestępczych.

Należy zwrócić uwagę, że bezpieczeństwo operacji elektronicznych zależy również w dużym stopniu od klienta, który powinien przestrzegać kilku istotnych zasad:

- posiadane hasła umożliwiające dostęp do rachunku powinny być starannie chronione (dotyczy to oczywiście również tokenów generujących jednorazowe hasła),
- każdorazowe połączenie z bankiem wymaga sprawdzenia, czy przesyłane informacje są szyfrowane,

- należy unikać przesyłania siecią jakichkolwiek informacji, które mogłyby ułatwić osobie nieupoważnionej dostęp do konta (np. adres, imię, nazwisko),
- konieczne jest wykorzystywanie sprawdzonych programów antywirusowych, które systematycznie należy aktualizować,
- odchodząc od komputera w czasie połączenia z bankiem, należy go odpowiednio zabezpieczyć bądź całkowicie wyłączyć.

Niestety, w wielu przypadkach klienci banków zapominają nawet o elementarnych zasadach korzystania z elektronicznego komunikowania się z bankiem, stwarzając tym samym okazję do nadużyć ze strony przestępców komputerowych. W takim przypadku zawodny może okazać się każdy system zabezpieczeń wykorzystywanych przez bank.

Nie ulega wątpliwości, że transakcje realizowane za pośrednictwem Internetu kosztują mniej i są łatwiejsze w dostępie, jednak jest to źródło istotnych zagrożeń. Globalny charakter sieci sprawia bowiem, że wymiana informacji pozbawiona jest kontroli nad drogą jej przesyłania. Istnieje więc techniczna możliwość przechwycenia informacji na drodze komunikacyjnej między bankiem i klientem. Sieć Internetu, do której jest podłączony zarówno system informatyczny banku, jak i klient, narażona jest na ataki „sieciowych włamywaczy" (tzw. hakerów). Mogą oni zmieniać konfigurację systemu stosowanego przez bank, ingerować w transakcje, a nawet zmieniać stany kont. Bank działający w Internecie musi zatem nie tylko zadbać o dostarczenie odpowiednich technologii zabezpieczających transakcje, ale również przekonać do tego swoich klientów. Jest to niewątpliwie trudne, może nawet najtrudniejsze w całym procesie związanym z tworzeniem systemu zabezpieczającego transakcje elektroniczne.

Jak słusznie zauważa B. Szafrański, systemy informatyczne są podstawą funkcjonowania instytucji finansowych, dlatego tak duże znaczenie przypisuje się do ich bezpieczeństwa. Sprawdzić jego poziom może tylko właściwie przeprowadzony audyt [Szafrański, 2016]. Istotnym warunkiem przygotowania i prowadzenia właściwej polityki bezpieczeństwa jest zidentyfikowanie źródeł i rodzajów zagrożeń. Jest to również istotne z punktu widzenia osób korzystających z usług elektronicznych, w tym przedsiębiorców, którym świadomość zagrożeń powinna ułatwić wprowadzenie w przedsiębiorstwie własnych procedur zabezpieczających systemy informatyczne.

Ze względu na różnorodność istniejących zagrożeń, podstawowym warunkiem prawidłowej oraz wiarygodnej realizacji transakcji elektronicznych jest opracowanie przez bank odpowiedniej **polityki bezpieczeństwa**, w ramach której istotnym elementem jest odpowiednie zarządzanie i procedury. Na przykład zarządzanie bezpieczeństwem bankowych systemów informacyjnych związane jest m.in. z monitorowaniem procesu wdrożenia i działania zabezpieczeń niezbędnych do efektywnej ochrony informacji i świadczonych usług, rozwijanie, szkolenie i wdrażanie, uświadamianie personelu co do zasad bezpieczeństwa, wykrywanie i postępowanie z incydentami itd. Realizując politykę bezpieczeństwa wyznacza się również podstawowe obszary wymagające szczególnej troski przy

stosowaniu zabezpieczeń - sprzęt, oprogramowanie, komunikacja (zapory ogniowe, szyfrowanie danych), środowisko fizyczne (ogrodzenia, identyfikatory), personel (np. procedury zwalniania pracowników, systemy szkoleń), administracja (autoryzacja).

2. Przyczyny występowania zagrożeń informatycznych

Rozwój współczesnej techniki stymulowany jest w istotnym stopniu rewolucją technologiczną, z którą nierozerwalnie związany jest rozwój łączności satelitarnej i globalnej sieci internetowej. Coraz powszechniejszemu użytkowaniu nowoczesnych technologii informatycznych sprzyja oczywiście stała obniżka cen sprzętu komputerowego oraz wprowadzenie programów przyjaznych dla użytkownika i niewymagających specjalistycznej wiedzy. Z drugiej jednak strony wraz z rozwojem nowoczesnych technologii zwiększa się zagrożenie dotyczące ludzi, związane przede wszystkim z niebezpieczeństwem nieuprawnionego dostępu do danych. Zagrożenie to wynika zatem z następujących kwestii:

- większość dokumentacji i informacji, które znajdowały się wcześniej w różnych miejscach, przechowywane są obecnie w komputerze, co znacznie ułatwia ich znalezienie;
- dane gromadzone są w systemie informatycznym i znajdują się pod opieką osoby odpowiednio przygotowanej - administratora systemu, a zatem kilka osób ma wgląd w dane i może je modyfikować w sposób praktycznie niezauważalny;
- z uwagi na wysoki koszt systemów zabezpieczeń danych, problem bezpieczeństwa zostaje nierzadko zaniedbany przez użytkowników systemów informatycznych, dotyczy to również samych banków;
- nierzadko firmy oferujące zabezpieczenia do systemów informatycznych nie są certyfikowane, przez co świadczone przez nie usługi są niejednokrotnie niskiej jakości;
- proponowane przez różne firmy systemy informatyczne są często wadliwe i pełne błędów;
- nowe zagrożenie przyniósł Internet, w którym łatwo można znaleźć wiele programów służących do łamania systemów informatycznych;
- informacja jest obecnie jednym z najbardziej poszukiwanych towarów na rynku, co w efekcie doprowadziło do poważnego wzrostu jej ceny, zwiększając tym samym pokusę, aby w nieuprawniony sposób korzystać z posiadanej wiedzy; niestety, wiele wywiadowni gospodarczych gromadzących informacje pozyskuje je kanałami nie zawsze legalnymi;
- banki, a także inne instytucje, dla których zaufanie jest kwestią kluczową, nie dopuszczają często do przekazywania opinii publicznej informacji o przypadkach naruszenia ochrony danych, z tego faktu wynika izolacja wskazanych instytucji, co w znacznym stopniu ułatwia przestępcom działanie; utrudnia to również istotnie pracę

organów ścigania, które w trakcie prowadzonych działań mają ograniczony dostęp do informacji.

Integracja w sieci informatyczne, w których gromadzi się i przetwarza miliony danych, jest zatem dziedziną szczególnie podatną na działalność przestępczą. Jak wskazuje J. Grzywacz, wśród podstawowych przyczyn takiego stanu rzeczy wyróżnić można [Grzywacz, 2016, s.123]:

- anonimowość działania, dającą sprawcy komfort psychiczny,
- bez konieczności opuszczania miejsca pobytu przestępca może popełnić wykroczenie wszędzie tam, gdzie funkcjonuje sieć internetowa,
- możliwość zdobycia wielu informacji, nieosiągalnych w innych warunkach,
- możliwość dosyć skutecznego usunięcia śladów przestępczej działalności.

Chociaż problem nadużyć informatycznych znany jest już od wielu lat i stale się powiększa, przestępczość teleinformatyczna jest zjawiskiem stosunkowo mało rozpoznanym. Dzieje się tak z wielu powodów, spośród których do najważniejszych należą:

- w dalszym ciągu niedocenione rozmiary zagrożeń tego typu przestępczością oraz jej związek z biznesem;
- trudne do określenia rzeczywiste rozmiary tej przestępczości, gdyż sprawcy działają stosunkowo długo i powodują poważne straty zarówno materialne, jak i niematerialne, a ponadto pokrzywdzeni często nie są zainteresowani ich ujawnianiem;
- często przestępstwa informatyczne ujawniane są przypadkowo, najczęściej z powodu błędów popełnionych przez sprawców;
- organy ścigania odgrywają minimalną rolę w ujawnianiu tych przestępstw i z tego powodu praktycznie znikoma jest rola śledztwa, a także wyroku.

Jak widać, funkcjonowanie systemów informatycznych wiąże się z istotnymi zagrożeniami, które odnoszą się bezpośrednio do możliwości korzystania z danych zawartych w systemie przez nieuprawnione osoby, a także do możliwości oddziaływania na system, w szczególności zaś na któryś z jego elementów: sprzęt elektroniczny, oprogramowanie, dane użytkowników systemu i jego administratorów.

Zagrożenia bezpieczeństwa mogą mieć charakter elektroniczny i fizyczny. Te pierwsze występują ze strony hakerów i intruzów, którzy atakują strony internetowe, systemy poczty elektronicznej lub wewnętrzne oprogramowanie firm. Zagrożenia fizyczne natomiast są powodowane przez nieuczciwych administratorów sieci, pracowników i kontrahentów, mogą je również wywoływać pożary, ładunki wybuchowe, powodzie i trzęsienia ziemi.

Przyczyny te mogą więc mieć charakter losowy bądź być celowym działaniem, efekty tych zdarzeń można zaś sklasyfikować w następujących grupach:

- Ujawnienie przetwarzanej informacji. Z reguły związane jest to z włamaniem do systemu, przy słabych algorytmach oraz braku ochrony lub właściwego zabezpieczenia klucza, co powoduje naruszenie poufności danych.
- Utrata bądź zniekształcenie informacji. Dochodzi do nich przez nieautoryzowany dostęp do systemu z powodu braku zapewnienia odpowiedniej procedury uwierzytelniania, czyli określenia tożsamości użytkownika.
- Wymuszenie przerwy w pracy systemu i zaburzenie toku pracy użytkownika bądź grupy użytkowników w celu zajęcia zasobów komputera. Blokada usług służy również tzw. podszywaniu sieciowemu i polega na podszyciu się przez komputer hakera pod zablokowany komputer, przez co może nastąpić przepływ informacji do niepowołanych rąk.
- Wykorzystanie danego systemu do działań niezgodnych z prawem. Może to być np. włamanie do systemu informatycznego banku i wykonanie przelewu środków.

Podsumowując, oczywisty jest fakt, że główny powód zagrożeń informatycznych stanowi motyw zysku, którym kierują się przestępcy informatyczni. Są to z jednej strony całe grupy przestępcze, dobrze zorganizowane i znakomicie wyposażone w najnowocześniejsze technologie, z drugiej zaś pojedyncze osoby, wywodzące się z różnorodnych grup społecznych i środowisk zawodowych. Osoby te doskonale poruszają się w świecie technologii informatycznej wykorzystywanej w gospodarce, w tym również przez instytucje finansowe. W przypadku pojawiających się kolejnych rozwiązań mających skuteczniej chronić w bankach przed nieuprawnionym dostępem do kont, osoby te wykorzystują równie nowoczesne systemy służące łamaniu istniejących zabezpieczeń.

3. Rodzaje i źródła zagrożeń

Nie ulega wątpliwości, że banki coraz lepiej radzą sobie z zagrożeniami, zwłaszcza o charakterze zewnętrznym. Jak słusznie zauważa B. Szafrański, znacznie trudniej przeciwdziałać jest nadużyciom wewnętrznym, potencjalne szkody mogą zaś osiągnąć znaczne rozmiary, zagrażające nawet funkcjonowaniu banku [Szafrański, 2013].

Lista zagrożeń systemów informatycznych jest dosyć obszerna i trudno jest w sposób jednoznaczny dokonać jej klasyfikacji, zwłaszcza że literatura podaje szereg różnych kryteriów.

Wydaje się jednak, że podstawową kwestią jest **sposób ingerencji w system informatyczny**. W tym przypadku zagrożenia można podzielić na: bierne (pasywne) i czynne (aktywne).

Zagrożenia **pasywne**, skutkują ujawnieniem informacji w nieuprawniony sposób, jednak bez oddziaływania na system informatyczny. Mowa jest tu zatem o infiltracji biernej, czyli śledzeniu informacji w określonym miejscu jej obiegu.

Do najbardziej popularnych metod tego typu działalności zalicza się: przechwytywanie elektromagnetyczne, polegające na uzyskaniu dostępu do połączeń między komputerem a terminalem bądź też do kierunkowej emisji promieniowania (i analizie sygnału odbitego od promieniującego urządzenia), dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów drogą radiową, badanie i kopiowanie zbiorów niezabezpieczonych, analiza makulatury lub pozostałości po magnetycznych nośnikach informacji oraz stosowanie ukrytych nadajników. Najczęściej jednak zagrożenia te urzeczywistniają się w postaci podsłuchu danych przesyłanych sieciami komputerowymi (sniffing) i jest to trudne do wykrycia. W sektorze bankowym działania te wywoływane są z reguły przez pracowników banków.

Zagrożenia **aktywne** oddziałują czynnie na system informatyczny. Polegają na modyfikacji lub zniszczeniu zasobów i powiązane są z reguły z celową dezinformacją. Najczęściej praktykowaną formą jest łamanie zabezpieczeń w celu uzyskania dostępu do dowolnego miejsca w systemie dzięki ominięciu środków ochrony stosowanych przez legalnego użytkownika systemu. Ponadto występuje tu ingerencja w struktury systemów operacyjnych i podszywanie się pod uprawnionego użytkownika systemu.

Kolejną klasyfikacją zagrożeń jest ich podział na **wewnętrzne** i **zewnętrzne**. Zagrożenia **wewnętrzne** są wynikiem działania użytkowników uprawnionych do korzystania z systemu. Ataki dokonywane od wewnątrz stanowią 60-80% wszystkich zagrożeń i wynikają z niedopełnienia obowiązków lub przekraczania (nadużycia) uprawnień przez własnych pracowników. Wydaje się, że podstawowymi przyczynami tego typu zagrożeń jest m.in. niewłaściwa polityka bezpieczeństwa banku (bądź całkowity jej brak), nadmierne przywileje pracowników czy brak właściwej reakcji na występujące nieprawidłowości.

Zagrożenia **zewnętrzne** występują natomiast ze strony osób nieuprawnionych do dostępu lub używania systemu informatycznego i są skutkiem niedoskonałości systemu zabezpieczeń zewnętrznych. Zagrożenia zewnętrzne mogą być również związane ze środowiskiem naturalnym (trzęsienia ziemi, wyładowania atmosferyczne itp.), a także z otoczeniem, w którym znajduje się komputer (kurz, wilgoć, ogień itp.).

Innym podziałem niebezpieczeństw jest wyróżnienie **naruszeń przypadkowych**, powstających głównie wskutek błędów użytkowników, awarii sprzętu i błędów w oprogramowaniu, oraz **celowych**, będących rezultatem świadomego działania użytkowników systemu.

Przyjmując z kolei za kryterium podziału **przedmiot zagrożeń**, niebezpieczeństwo nadużyć może dotyczyć:

– transakcji elektronicznych, w których zagrożenie obejmuje wszystkie strony uczestniczące w nich; włamywacz może np. przechwycić numery kont bądź umieścić w bazie danych polecenie przelewu na swoje konto;

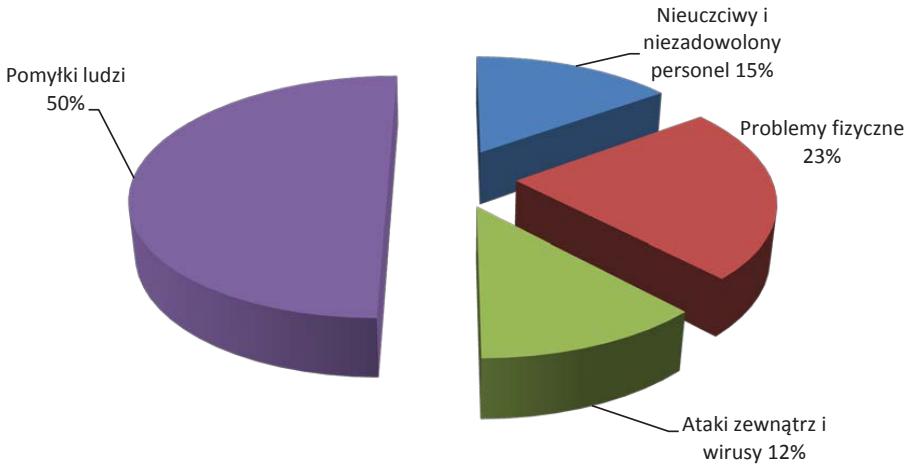
- zasobów danych, gdzie przedmiotem ataku może stać się cała baza danych, dane przechowywane w sieci albo archiwizowane i niedostępne w sieci bądź dane znajdujące się w kopiach zapasowych;
- środków technicznych – komputerów, linii transmisji danych, środków komunikacji oraz oprogramowania systemowego, użytkowego, plików z kodem źródłowym i narzędzi diagnostycznych;
- dokumentacji dotyczącej programów, sprzętu, systemów administracyjnych oraz zasad bezpieczeństwa systemu.

Ważnym kryterium podziału zagrożeń jest ich **rodzaj**. Z tego punktu widzenia, zdaniem J. Grzywacza wyróżnić można 5 grup [Grzywacz, 2016, s.127]:

1) nieuprawniony dostęp do transmisji elektronicznych i do zasobów danych oraz nielegalne operacje na tych zasobach, np. realizacja własnych transmisji z wykorzystaniem zasobów systemu, przechwycenie pliku haseł, penetracja systemu, przełamanie lub obejście istniejących zabezpieczeń (hacking), kradzież i kopiowanie danych;
2) zmiana działania oprogramowania, poprzez np. kradzież elementów oprogramowania, modyfikację działań programów, wprowadzenie wirusów komputerowych;
3) uszkodzenia sprzętu informatycznego, np. kradzież, uszkodzenie mechaniczne, uszkodzenie za pomocą promieniowania elektromagnetycznego i optycznego, logiczne blokowanie sprzętu, monitorowanie fałszywych elementów sprzętowych (układów procesora, pamięci itp.);
4) zagrożenia linii transmisji danych, np. kradzież linii i elementów funkcjonalnych, ich uszkodzenia fizyczne, zawieranie lub przekierowanie połączeń, nielegalne korzystanie z linii;
5) zagrożenia dotyczące dokumentacji, może ona zostać narażona na kopiowanie, kradzież, fizyczne uszkodzenie czy też wprowadzenie do niej fałszywych informacji.

Jak widać, systematyka zagrożeń informatycznych jest bardzo obszerna, zwłaszcza że wiele z nich wzajemnie się przenika. Nie powinien jednak budzić wątpliwości fakt, że główną przyczyną i jednocześnie źródłem zagrożeń komputerowych jest działalność **ludzka** (wykres 1).

Wykres 1. Podstawowe źródła zagrożeń dla systemów informatycznych



Źródło: opracowanie własne na podstawie Komendy Głównej Policji.

Błędy i przeoczenia personelu są, jak widać, główną przyczyną zagrożeń, wymienianą zresztą od wielu lat. Wynika to głównie z pośpiechu, zmęczenia, niewiedzy, złej organizacji pracy czy kłopotów zdrowotnych. Do tego typu zagrożeń zalicza się głównie przypadkowe ujawnienie informacji na skutek błędu operatorskiego (np. przesłanie danych pod niewłaściwy adres), przypadkowa zmiana atrybutu pliku (np. ukrytego na jawny) czy praw dostępu, wykorzystywanie „słabych" haseł, niezamierzone ujawnienie hasła dostępu lub pozostawienie włączonego komputera niezabezpieczonego hasłem dostępu, przypadkowe wprowadzenie do systemu niewłaściwych danych, niewłaściwy sposób usunięcia danych o charakterze poufnym, zgubienie karty służącej do identyfikowania i uwierzytelniania.

Mimo że zawodność sprzętu nie znajduje się wśród czołowych zagrożeń informatycznych, nie wolno tej kwestii bagatelizować. Problem ten wiąże się z zagrożeniami fizycznymi i dotyczy niebezpieczeństwa umyślnego lub losowego unieruchomienia centrum obliczeniowego. Najczęściej są to przerwy w zasilaniu energetycznym, awarie sprzętu, utrata danych w wyniku zniszczenia dysków lub innych nośników pamięci oraz inne zdarzenia o charakterze losowym, np. włamania, pożary.

Warto wreszcie zauważyć, że istotnym źródłem zagrożeń jest niewłaściwe zabezpieczenie systemu przed czynnikami naturalnymi (środowiskowymi). Należą do nich woda i ogień, jednak należy również w tym miejscu wskazać na destrukcyjne działanie kurzu. Dostaje się on głównie do wnętrza systemu z powietrzem używanym do chłodzenia. Drobiny kurzu mogą powodować mikrozwarcia, które doprowadzają do uszkodzenia układów półprzewodnikowych. Niekorzystnym zjawiskiem są również wahania temperatury, która dla komputera powinna wynosić 10-40 stopni Celsjusza. Zbyt niska temperatura może spowodować pękanie ścieżek układów elektronicznych, natomiast zbyt wysoka topnienie

plastikowych elementów. Niekorzystne dla komputera są również wstrząsy i wibracje, wynikające np. z bliskości arterii komunikacyjnych o dużym natężeniu ruchu. Również nadajniki radiowe, czy telefony komórkowe mogą zakłócać działanie poszczególnych elementów. Warto zatem stosować ekrany z filtrami elektromagnetycznymi, chroniącymi poszczególne pomieszczenia przed negatywnym wpływem fal. Poza tym wilgoć w pomieszczeniach ze sprzętem elektronicznym musi być utrzymywana na niezmiennym poziomie, dostosowanym do rodzaju użytkowanego sprzętu.

Zagrożeniem dla systemu są także różnego rodzaju insekty oraz dym, w tym nikotynowy, który może nawet zniszczyć takie urządzenia jak stacje dysków czy dyski twarde.

4. Zagrożenia ze strony ludzi

Jak uprzednio wspomniano, najważniejszym zagrożeniem dla systemów informatycznych jest działalność ludzka. Należy przy tym zauważyć, że dzisiejsze motywy działania sprawców włamań do systemów bankowych nie mają na celu jedynie bezpośredniego zdobycia środków finansowych. Ogólnie rzecz ujmując, warto zwrócić uwagę na następujące aspekty tych działań:

- szpiegostwo, polegające na kradzieży cennych informacji i przekazaniu ich konkurencyjnemu bankowi,
- chęć osiągnięcia zysku,
- uzyskanie rozgłosu, poprzez ujawnienie faktu włamania.

Trudno jest jednoznacznie wskazać, które z przestępstw komputerowych są najbardziej niebezpieczne. Obserwacja rynku informatycznego i rozwoju nadużyć zdaje się potwierdzać konieczność zwrócenia uwagi na następujące formy przestępstw:

- oszustwa komputerowe,
- fałszerstwo komputerowe,
- nieuprawnione włamanie się do systemu (hacking),
- wykorzystywanie programów komputerowych w celach przestępczych.

Oszustwa komputerowe można uznać za uboczny skutek informatyzacji systemów bankowych i finansowo-księgowych. Głównym celem tego typu nadużyć jest zdobycie środków finansowych przez wykorzystanie następujących technik:

- manipulacja danymi; jest to najbardziej popularny sposób uzyskania korzyści finansowych, który polega na wprowadzeniu fałszywych danych do systemu (głównie tzw. martwych dusz); przestępstw takich dopuszczają się najczęściej operatorzy sprzętu i mogą one przynieść instytucji duże straty;
- manipulacja programem; w tym wypadku przestępcy (np. autorzy oprogramowania, administratorzy bądź osoby spoza instytucji posiadające dużą wiedzę informatyczną) ingerują w program w taki sposób, aby wykonywał on określone czynności niezależnie od woli

operatora; przykładem może być tzw. metoda „salami", w której np. program bankowy przy rozliczaniu środków na rachunku *a vista* sam minimalnie zmniejsza stan środków na rachunku i przekazuje uzyskaną w ten sposób kwotę na wskazany rachunek (sprawcy bądź innej osoby);

– manipulacja wynikiem (urządzeniami wyjścia-wejścia), polegająca na wykorzystywaniu ogólnie dostępnych peryferii komputerów i systemów, przykładem mogą być bankomaty pracujące w trybie off-line, z których przestępcy wypłacają środki poniżej salda na rachunku.

Fałszerstwa komputerowe dotyczą przede wszystkim dokumentów – zarówno klasycznych (papierowych), jak i elektronicznych. Narzędziem do fałszowania dokumentów papierowych są komputer, oprogramowanie i urządzenia zewnętrzne (skaner, drukarka itp.). Odpowiedni dobór papieru oraz zidentyfikowanie zabezpieczeń technicznych umożliwia oszustowi stworzenie wiernej kopii dowolnego dokumentu. Fałszerstwa elektroniczne polegają na wprowadzeniu zmian w dokumentach elektronicznych (księgi handlowe i podatkowe, kartoteki pojazdów). W przypadku banku wymiana informacji pomiędzy pracownikami jest narażona na penetrację. Takie dane mogą być nie tylko kradzione, lecz także modyfikowane. Wykrycie tego rodzaju przestępstwa jest utrudnione, gdyż zmiany są niezauważalne i ich wykrycie wymaga specyficznej wiedzy oraz odpowiednich narzędzi. Z pomocą przychodzi tutaj podpis elektroniczny oraz odpowiednie uregulowania prawne. Banki zachęcają klientów do korzystania z odpowiednich kluczy przy wymianie informacji, umieszczając jednocześnie swoje publiczne klucze na stronach internetowych. Należy zwrócić uwagę, że przechwycenie przez oszusta dokumentów elektronicznych może nastąpić zarówno w wewnętrznym obiegu, jak i przy przesyłaniu za pośrednictwem sieci ogólnego użytku.

Kolejnym zagrożeniem bezpieczeństwa systemu informatycznego banku ze strony świadomej działalności ludzkiej jest obecność w sieci włamywaczy komputerowych (intruderów, hackerów, krackerów). Skala tego zjawiska jest ogromna i rośnie z roku na rok.

Nie ulega wątpliwości, że hackerzy nie decydują się zbyt często na próby przełamania infrastruktury zabezpieczeń systemów banków. Jak zauważa J. Trzaska, hackerzy nie łamią zabezpieczeń bankowych, bo im się to po prostu nie opłaca [Trzaska, 2015]. Łatwiej i szybciej jest im pozyskać tzw. *credentials*, czyli zbiór loginów i haseł klientów przy zastosowaniu socjotechniki lub zainfekowaniu komputerów szkodliwym oprogramowaniem.

Często spotykanym działaniem hackerów jest dokonanie takich zmian w komputerach obsługujących nazwy serwerów internetowych, aby próby wywołania banku skutkowały zgłoszeniem się zupełnie innego serwisu, podszywającego się pod ten, z którym połączenie chciał zrealizować klient. Wykorzystuje się tutaj obce komputery oraz stosunkowo słabe zabezpieczenia oprogramowania serwerów nazw internetowych.

Na kradzieżach witryn komputerowych nie kończy się działalność włamywaczy internetowych. Grupa ta potrafi wykorzystać specyficzne programy, umożliwiające penetrację systemów. Poza tym ataki włamywaczy mogą również przybrać formę różnorodnych działań, takich jak:

- *Kracking*, czyli zgadywanie haseł.
- *Sniffing* (podglądanie, podsłuchiwanie); jest to atak polegający na analizowaniu informacji przesłanych siecią oraz przechwytywanie w ruchu sieciowym haseł użytkownika, prywatnych danych, nazw programów, z których korzystają użytkownicy; za pomocą sniffera można poznać topologię sieci oraz serwisy udostępnione przez wybrane komputery. Sama nazwa tej metody pochodzi od słowa *sniffer*, które używane jest do określenia programu komputerowego lub urządzenia, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci.
- *Snooping*, czyli pasywne podpięcie do kabla transmisji.
- *Network snooping*, czyli wstępne rozpoznawanie parametrów sieci, w szczególności pod katem stosowanych zabezpieczeń.
- *Spoofing*, aktywne podpięcie do kabla, polegające na podszywaniu się pod inny komputer w sieci, czyli wysyłanie sfałszowanych pakietów do danej maszyny aż do momentu przejęcia całej sesji użytkownika, z daną maszyną włącznie. Komputer hackera oszukuje „nasz" komputer i zbiera wysyłane przez nas dane. W ten sposób może być identyfikowany przez nasz komputer, jako np. serwer, przez co uzyskuje dostęp do naszych danych. Tego typu oprogramowanie może być instalowane przez hackerów nie tylko na komputerach, ale także na routerach dostępnych w sieci. Stwarza to większe niebezpieczeństwo, ponieważ hacker uzyskuje wówczas dostęp do danych wysyłanych przez całą sieć podłączoną do routera, a nie tylko przez jeden komputer.
- *Trap doors*, czyli uzyskanie dostępu przez tzw. furtki, a więc zdobycie poufnych danych przez nieudokumentowanie wejścia do legalnych programów, pozwalające zorientowanemu użytkownikowi na omijanie zabezpieczeń.
- *Back door* (tylne drzwi), instalację oprogramowania umożliwiającego dostanie się do systemu w inny sposób niż przez logowanie.
- Denial of service (DoS), czyli atak, w którym jeden użytkownik zajmuje tak dużo dzielonych zasobów systemu, że następny użytkownik nie może z nich już skorzystać.

Phishing, czyli wyłudzanie poufnych informacji takich jak dane osobowe, hasła czy szczegółowe dane karty kredytowej, poprzez podszywanie się przez osobę lub instytucję godną zaufania. Często zdarza się, że osoba próbująca wyłudzić takie dane przesyła informację o charakterze spamu, która często przekierowuje na imitację strony bankowej. Po wpisaniu danych na tej „udawanej" stronie internetowej następuje przechwycenie poufnych informacji. Aby się przed

tym bronić banki często na swoich stronach internetowych zamieszczają przypomnienie o tym, że bank nigdy nie wysyła informacji z prośbą o podanie poufnych danych drogą mailową ani SMS-em. Najbezpieczniej jest za każdym razem logować się na konto bankowe za pomocą autoryzowanej strony banku albo sprawdzić prawdziwość otrzymanej wiadomości, aby zbyt pochopnie nie przesłać osobie niepowołanej poufnych informacji.

Należy również zwrócić uwagę, że jedną z bardziej wyrafinowanych form nadużyć, jest tzw. kradzież tożsamości (*Identity Theft*). Polega ona na udawaniu innej osoby z wykorzystaniem nie tylko np. nazwiska i numerów kart płatniczych czy rachunków bankowych, ale również pozycji społecznej, adresu, historii dotychczasowych stosunków z bankami, sprzedawcami, firmami kredytowymi itp. W przypadku klasycznej bankowości oddziałowej ryzyko wykrycia mistyfikacji jest wysokie, szanse uniknięcia odpowiedzialności sądowej niewielkie, toteż skala udanych przestępstw tego typu jest tam nieznaczna. Działanie za pośrednictwem telefonu lub Internetu minimalizuje takie ryzyko do poziomu pozwalającego je ignorować. Twierdzi się, że sprawca oszustwa, działając tylko przez Internet i wykorzystując luki bezpieczeństwa na wszystkich poziomach (klient, sprzedawca, bank), może uzyskiwać tą droga nawet kilkadziesiąt tysięcy dolarów tygodniowo.

Jak uprzednio wspomniano, istotną grupę zagrożeń dla systemów komputerowych stanowią **programy komputerowe** o charakterze inwazyjnym, których zadaniem jest utrudnienie lub uniemożliwienie pracy użytkownikom komputerów. Wiele z nich posiada mechanizmy, których celem jest niszczenie danych zawartych na twardych dyskach komputerów. Niektóre powodują zablokowanie sieci, paraliżując w ten sposób pracę oddziałów lub serwisów internetowych banku. Programy te, wg. wskazań J. Grzywacza można podzielić na kilka grup [Grzywacz, 2016, s.132]:

- **bakterie**, czyli programy, których jedynym przeznaczeniem jest powielenie się w celu zniszczenia systemu przez jego zablokowanie;
- **wirusy**, czyli programy dopisujące się do innych programów i ujawniające się w chwili uruchomienia zainfekowanego programu; mogą one powodować np. utratę danych, blokowanie działania komputera, uszkodzenie sprzętu, spowolnienie działania komputera, wyświetlanie obrazów, przechwytywanie i modyfikowanie informacji wprowadzonych do komputera;
- **bomby pocztowe**, czyli przesyłki wysyłane na konto pocztowe adresata – ofiary ataku; po otwarciu uaktywnia się ich zawartość, a skrzynka odbiorcy zasypywana jest tysiącami bezwartościowych listów - śmieci, on sam zaś zapisywany jest na dziesiątki grup dyskusyjnych;
- **robaki**, czyli programy przenoszące się za pośrednictwem sieci z systemu na system pozostawiające niekiedy wirusy;
- **ataki odmowy usług** (denial of service, DoS), polegające na takim działaniu hackera, które blokuje docelowy system komputerowy (często całą sieć) i uniemożliwia użytkownikom korzystanie z niego;

- **programy skanujące** – badające poszczególne porty konkretnego serwera i analizujące odpowiedzi otrzymywane od nich; w ten sposób możliwe jest określenie, jakie usługi są aktywne na danym serwerze oraz jakie oprogramowanie je realizuje, dzięki temu można wykryć słabe strony zabezpieczeń systemów;
- **konie trojańskie**, polegające na działaniu aplikacji niezgodnym z intencjami użytkownika; programy te najczęściej, podszywając się pod aplikacje komercyjne, realizują niepożądane, również przestępcze działania - pobieranie haseł lub plików bez wiedzy użytkownika komputera. Głównym zagrożeniem w tym wypadku jest specjalnie przygotowane złośliwe oprogramowanie w formie wirusów komputerowych, „koni trojańskich" lub oprogramowania typu *spyware*, które wykorzystują luki w systemach operacyjnych oraz luki w systemach zabezpieczeń naszych komputerów. *Spyware* to złośliwe programy, zbierające i wysyłające bez zgody użytkownika informacje o systemach komputerowych, z których korzysta użytkownik. W tym przypadku dane autoryzacyjne są kopiowane z naszego komputera lub odczytywane w trakcie korzystania z systemów bankowych poprzez odczytywanie wprowadzanych danych z klawiatury. W ten sposób oprogramowanie to kradnie nasze hasła oraz loginy do systemów. Na ataki tego typu oprogramowania możemy być bardziej narażeni w przypadku, gdy korzystamy z usług bankowych na komputerach ogólnodostępnych, np. w kawiarenkach internetowych, bibliotekach lub innych miejscach, gdzie dostęp do komputera ma wiele osób. Takie komputery często wykorzystywane są przez przestępców do kra-dzieży danych ze względu na łatwość instalacji złośliwego oprogramowania na takim sprzęcie. To samo zagrożenie dotyczy korzystania z ogólnodostępnych i niezabezpieczonych sieci WIFI czy to za pomocą naszego komputera osobistego czy też telefonu komórkowego z zainstalowanym systemem bankowości elektronicznej.

Podsumowując, wśród zewnętrznych zagrożeń dla systemów IT od lat w czołówce znajdują się *spyware*, wirusy, robaki, spam, *phishing* i *hacking*. Wszelkie statystyki potwierdzają, że one właśnie w najbardziej dotkliwy sposób dotykają nie tylko przedsiębiorstw, ale również osób indywidualnych. Należy również zwrócić uwagę na fakt częstego przesyłania na internetową skrzynkę pocztową wiadomości nieznanego pochodzenia. Ciekawość powoduje, że adresaci otwierają takie wiadomości i zapoznają się z ich treścią, otwierają linki zawarte w takich wiadomościach czy zdjęcia znajdujące się w załącznikach. Hackerzy umieszczają pod takimi plikami czy linkami kody złośliwego oprogramowania, które jest w stanie uzyskać dostęp do naszych danych lub wykraść nasze zapisane hasła dostępowe.

Innym rodzajem tego typu zagrożeń są wiadomości e-mail o treści podszywającej się pod bank, z prośbą o weryfikację danych dostępowych do konta

internetowego. Takie wiadomości często są łudząco podobne do korespondencji banków, należy jednak pamiętać, żeby w takich przypadkach pod żadnym pozorem nie powinno się wysyłać ani podawać w wiadomościach lub na stronach internetowych, do których przenoszą nas takie wiadomości, naszych danych identyfikacyjnych.

Możliwości działań przestępczych są jak widać, w środowisku informatycznym bardzo szerokie: szkodliwość ich różna w zależności od stopnia ingerencji w system użytkownika. W przypadku usług bankowych zagrożenia tego typu są szczególnie niebezpieczne, dotyczą one bowiem często odbiorców tych usług, a ich wiedza informatyczna jest często znikoma. Ufają oni zapewnieniom bankowców o wysokim stopniu bezpieczeństwa tego typu usług, same banki natomiast niechętnie ujawniają jakiekolwiek informacje o przypadkach włamań do swych systemów informatycznych bądź innych zakłóceniach. Na przykład większość banków potwierdza fakt pojawienia się w ich systemach wirusów, z kolei żaden bank w Polsce nie przyznał, jak dotąd, że wykryty wirus wyrządził poważne szkody.

Należy wreszcie wyraźnie podkreślić, że wśród wielu zagrożeń największą ich część stanowią pomyłki ludzkie. Są one wynikiem braku wiedzy, zmęczenia, pośpiechu czy wręcz lenistwa. Dotyczy to np. nieumyślnego ujawnienia hasła, zapomnienia hasła dostępu przez pracownika, pozostawienia włączonego komputera bez zabezpieczenia hasłem dostępu, zgubienia karty magnetycznej przez pracownika, niezamierzonego wprowadzenia wirusa komputerowego do systemu, używania służbowej poczty elektronicznej do prywatnych celów. Z kolei celowymi i zamierzonymi działaniami są czynności wykonywane przez niezadowolonych i nieuczciwych pracowników. Najczęściej występują tu przelewanie środków pieniężnych na prywatne konta, umyślna modyfikacja systemu bądź jego niszczenie, ujawnianie osobom postronnym tajemnic związanych z systemem, wprowadzanie wirusów do systemów oraz sporządzanie kopii poufnych informacji na urządzenia zewnętrzne. W takich przypadkach nawet najlepiej działające procedury nie są skuteczne.

Podsumowanie

Nie ulega wątpliwości, że rozwój bankowości elektronicznej istotnie wpływa na wzrost jakości obsługi finansowej przedsiębiorstwa oraz obniżanie kosztów tej obsługi. Warunkiem wzrostu zainteresowania tą formą jest jednak odpowiedni poziom bezpieczeństwa funkcjonujących systemów informatycznych. Bez spełnienia tego warunku trudno jest oczekiwać, że tego typu usługi będą cieszyły się popularnością, zwłaszcza w świetle doniesień medialnych, informujących o wzrastającej przestępczości komputerowej.

Zagrożenia systemów informatycznych dotyczą zarówno możliwości korzystania z danych zawartych w systemie przez nieuprawnione osoby, jak i oddziaływania na system i jego różne elementy - sprzęt elektroniczny, oprogramowanie, dane użytkowników systemu i jego administratorów. Szczególnie niebezpieczne

są zagrożenia wywoływane przez ludzi - hakerów włamujących się z zewnątrz do systemów oraz osób bezpośrednio je obsługujących, w szczególności administratorów systemu. Warto przy tym zauważyć, że dzisiejsze motywy działania przestępców nie dotyczą jedynie wykradania środków pieniężnych, przedmiotem ich zainteresowania są bowiem nierzadko cenne informacje przekazywane innym instytucjom (np. konkurencyjnym bankom) czy też uzyskanie rozgłosu przez ujawnienie faktu włamania się do obcego systemu informatycznego.

Funkcjonujące w bankach systemy zabezpieczeń mają obecnie różnorodny, rozbudowany charakter. Systemy te można sklasyfikować jako organizacyjne, administracyjne, fizyczne i programowe. Szczególne znaczenie ma wykorzystanie różnorodnych metod kryptograficznych, wykorzystujących algorytmy będące matematycznymi kombinacjami liczb i liter. Coraz większe znaczenie ma podpis elektroniczny, który dzięki swoistym cechom (np. jest niepowtarzalny i inny dla każdego dokumentu, daje się oddzielić od przesłanej razem z nim wiadomości) stanowi duży krok w kierunku wzmocnienia bezpieczeństwa przeprowadzanych operacji elektronicznych. Nie wolno jednak zapominać o istniejących tu zagrożeniach, wśród których warto wyróżnić niewystarczającą wiedzę osób używających podpisu cyfrowego, co do zasad stosowania go, czy też niski poziom bezpieczeństwa infrastruktury sieciowej.

Dokonując oceny systemów informatycznych w bankach, można postawić tezę, że stosowane obecnie rozwiązania w istotnym stopniu wpływają pozytywnie na wzrost bezpieczeństwa. Z drugiej jednak strony rosnące zagrożenia przestępcze wskazują na konieczność doskonalenia rozwiązań, w tym proceduralnych. Istnieje również potrzeba poprawy w bankach jakości szkoleń w zakresie funkcjonowania nowoczesnych technologii informatycznych i wzmożenia wysiłków w kierunku edukacji samych klientów. Banki stale powinny informować klientów o zasadach poufności i prywatności informacji przekazywanych drogą elektroniczną, muszą również posiadać odpowiednie procedury i mechanizmy kontrolne oceniające stosowaną infrastrukturę bankowości elektronicznej.

Literatura

1. Gospodarowicz Andrzej (red.). 2005. Bankowość elektroniczna. Warszawa: Polskie Wydawnictwo Ekonomiczne.
2. Grzywacz Jacek. 2016. *Bankowość elektroniczna w przedsiębiorstwie*. Warszawa: Oficyna Wydawnicza SGH.
3. Szafrański Bohdan. 2013. „Bank i klient. Nadużycia wewnętrzne w banku". Bank nr 1: 38
4. Szafrański Bohdan. 2016. „Audyt bezpieczeństwa IT w banku.". Bank nr 7-8: 42
5. Trzaska Jerzy. 2015. „Bank i klient. Bezpieczeństwo jest bezcenne". Bank nr 6: 153
6. Wawrzyniak Dariusz. 2002. *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*. Warszawa: Biblioteka Menedżera i Bankowca.

SECURITY RISKS IN ONLINE BANKING

Summary

Online service is needed in today's banking. However, the threat landscape for online banking has changed dramatically resulting in the need for multiple layers of security. Delivering online banking offer requires a solid security framework that protects clients and companies institution's data from outside intrusion. The article summarizes security framework, which incorporates the latest proven technology. Part of it also summarizes person's responsibilities as a user of the internet banking system with regard to security. There are several levels of security within security framework. User Level deals with cryptography and Secure Sockets Layer (SSL) protocol, and is the first line of defence used by all customers accessing Banking Server from the public Internet. Server Level focuses on firewalls, filtering routers, and other trusted operating systems. Host Level deals specifically with internet banking and the processing of secure financial transactions. This article shows the main kinds of threats to online banking and divides them to different sections. The main aim of this paper is to emphasise the importance of secure Policy in online banking.

Key words: threats of online banking, security Policy, security framework, cryptography