WSPÓŁCZESNE PROBLEMY I ZAGROŻENIA CYBERBEZPIECZEŃSTWA W SEKTORZE USŁUG BANKOWOŚCI ELEKTRONICZNEJ

CONTEMPORARY PROBLEMS AND THREATS OF CYBER SECURITY IN THE SECTOR OF ELECTRONIC BANKING SEVICES

Rafał Pitera[1]

WYDZIAŁ EKONOMII UNIWERSYTETU RZESZOWSKIEGO

Streszczenie: Artykuł dotyczy problematyki cyberbezpieczeństwa w odniesieniu do usług bankowych. Przedstawiono różne próby wymuszeń. Następnie omówiono najważniejsze działania ze strony banków oraz instytucji finansowych w Polsce, mające na celu przeciwdziałanie cyberprzestępczości. Wzrastająca liczba użytkowników mających dostęp do bankowości internetowej oraz mobilnej, wzrost liczby płatności zbliżeniowych nie pozostają bez echa na działania przestępców. W ostatnich latach nastąpił gwałtowny wzrost liczby prób wyłudzeń i wymuszeń drogą elektroniczną. Skala zjawiska tylko podkreśla znaczenie problemu cyberprzestępczości i nadaje niewątpliwie istotną rangę omawianemu zagadnieniu.

Abstract: This article deals with the problem of banking security in relation to banking services. Various attempts at extortion were presented. Next, the most important actions taken by banks and financial institutions in Poland to combat cybercrime were discussed. The increasing number of Internet and

[1] Rafał Pitera, mgr ekonomii, absolwent Uniwersytetu Rzeszowskiego. Absolwent Wydziału Ekonomii, od kilku lat związany z dziedziną finansów i bankowości. Główne obszary zainteresowań: sprawozdawczość i analiza finansowa, badanie i ocena kondycji finansowej przedsiębiorstw, optymalizacja podatkowa, analiza ulg podatkowych i ich wpływ na rozwój przedsiębiorczości, bezpieczeństwo usług bankowych; telefon: 17 872 1645, e-mail: rpitera@ur.edu.pl, adres: ul. M. Ćwiklińskiej 2, 35-601 Rzeszów, pokój 202.

Rafał Pitera, MA, graduated from the Department of Economics of the University of Rzeszow. A graduate of the Faculty of Economics, for several years has been involved in finance and banking. Main areas of interest: financial reporting and analysis, research and assessment of the financial condition of enterprises, tax optimization, tax relief analysis and their impact on entrepreneurship development, security of banking services; phone 17 872 1645, e-mail: rpitera@ur.edu.pl, address M. Ćwiklińskiej 2, 35-601 Rzeszów, room 202.

mobile banking users, the increase in proximity payments, increases the number of offenders. In recent years there has been a sharp increase in the number of phishing attempts and eavesdropping. The scale of the phenomenon highlights the importance of cybercrime and gives importance to the issue.

Słowa kluczowe: cyberbezpieczeństwo, bankowość internetowa, bankowość mobilna, cyberprzestępczość, bezpieczeństwo usług bankowych.

Keywords: cyber security, internet banking, mobile banking, cybercrime, banking services security.

Wstęp

Wzrost znaczenia e-usług widoczny jest w wielu sektorach. Ciągły postęp dotyczy bardzo dużej liczby branż oraz szerokiego spektrum możliwości związanych z coraz to nowymi usługami. Produkty bankowości internetowej na tle pozostałych charakteryzują się bardzo dużym zainteresowaniem ze strony nie tylko instytucji kreujących poszczególne e-usługi, ale także użytkowników, organów nadzorujących i niestety także przestępców. Dynamicznemu rozwojowi bankowości elektronicznej towarzyszy również rozwój technik przestępczych. Szkodliwość działań przestępczych jest widoczna w wielu sektorach. Niestety, działania przestępcze nakierowane na bankowość internetową z pewnością stanowią jedne z największych zagrożeń. Dzieje się tak dlatego, że tego typu nielegalne działania wiążą się z utratą środków finansowych użytkowników dotkniętych takim działaniem. Problem cyberprzestępczości w ostatnich kilkudziesięciu latach staje się coraz bardziej widoczny. Przynosi też coraz większe konsekwencje. Zjawisko jest o tyle poważne, że doskonaleniu wielu nowych technologii, niemal równolegle towarzyszy rozwój „złych" technologii, wykorzystywanych do nadużyć i przestępstw[2].

Uwzględniając powyższe, warto odnieść się do problemu związanego z bezpieczeństwem w sieci dotyczącegi usług bankowych. W obecnych czasach kanał bankowości internetowej nie jest niczym wyjątkowym. Trudno znaleźć bank, który nie oferuje swoim klientom możliwości założenia rachunku przez Internet, zrobienia przelewu online, czy skontaktowania się z doradcą za pomocą platformy internetowej. Z roku na rok zwiększa się liczba użytkowników bankowości mobilnej, płatności zbliżeniowe kartą stają się czymś powszechnym. Mówiąc o płatnościach zbliżeniowych, coraz częściej też należy dodać, czy mamy na myśli transakcję kartą, czy może telefonem komórkowym. Jak wynika z „Badania otwartości polskich konsumentów na innowacyjne metody płatności", większość badanych (55%) jest

[2] *Cyberdefence24*, *Dekalog bankowego cyberbezpieczeństwa według wiceprezesa Związku Banków Polskich*. WYWIAD, [online], witryna Internet http://www.cyberdefence24.pl/579395,dekalog-bankowego-cyberbezpieczenstwa-wedlug-wiceprezesa-zwiazku-bankow-polskich-wywiad [data dostępu: 14.06.2017]; Rzeczpospolita, Mieczyław Groszek: *Cyberbezpieczeństwo warunkiem nowoczesnej bankowości*, witryna Internet [online], http://www.rp.pl/Opinie/301249907-Mieczylaw-Groszek-Cyberbezpieczenstwo-warunkiem-nowoczesnej-bankowosci.html, [data dostępu: 14.06.2017].

otwarta na nowinki technologiczne oraz aktywnie z nich korzysta[3]. Widoczny trend w rozwoju bankowości elektronicznej w Polsce dorównuje dynamice w krajach zachodniej części Europy. A w dziedzinie takich instrumentów płatniczych, jak karty płatnicze z funkcją zbliżeniową, jesteśmy niekwestionowanym liderem w całej Unii Europejskiej. Na koniec 2014 roku 27 mln 190 tys. klientów indywidualnych oraz Małych i Średnich Przedsiębiorstw (MŚP) miało podpisaną umowę umożliwiającą korzystanie z bankowości internetowej, z czego 14 mln 280 tys. klientów indywidualnych i MŚP korzystało z niej aktywnie. W tym samym okresie w obrocie było 36 mln 70 tys. kart płatniczych, z czego 29 mln 750 tys. kart debetowych, 6 mln 40 tys. kart kredytowych oraz 282 tys. kart obciążeniowych[4]. Natomiast na koniec 2016 roku liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej wyniosła nieco ponad 33 mln osób. W odniesieniu do analogicznego okresu z roku poprzedniego był to wzrost o blisko 10% (dokładnie 9,31%). Z czego aktywnych klientów indywidualnych było 15 mln 300 tys. osób. Stanowiło to przyrost w odniesieniu do okresu analogicznego roku ubiegłego o niemal 5%. W tym samym okresie liczba klientów MSP mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej wyniosła 2 mln 3 tys. podmiotów. Liczba aktywnych klientów MSP wyniosła 1 mln 400 tys.[5]. W przytoczonych powyżej statystykach widoczny jest nadal utrzymujący się trend wzrostu zainteresowania bankowością oraz płatnościami internetowymi czy mobilnymi. Wysuwa się z tego jasny wniosek: Polacy chcą płacić łatwiej i coraz to prościej, a przez to i szybciej. Niestety, za taką tendencją podążają również cyberprzestępcy. Można wręcz sformułować określenie, że przestępstwa związane z usługami świadczonymi przez banki oraz przedsiębiorstwa świadczące usługi finansowe w dużej części przeniosły się do świata wirtualnego. Jak wynika z raportu InfoDOK, tylko w I kwartale 2017 roku próbowano wyłudzić codziennie niemal milion złotych. W okresie styczeń-marzec 2017 r. udaremniono 1746 prób wyłudzeń kredytów na łączną kwotę 90 mln 400 tys. złotych – wynika z cytowanego raportu[6].

---

3 MAISON & PARTNERS, Raport *Badanie otwartości polskich konsumentów na innowacyjne metody płatności*, witryna Internet [online], Warszawa, 27.04.2016, https://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-polscy-konsumenci-otwarci-na-cyfrowe-innowacje/, [data dostępu: 14.06.2017].

4 P.M. Balcerzak, P*otrzebujemy cybertarczy sektora bankowego*, „BANK" Miesięcznik finansowy, 5/2015, s. 40.

5 Związek Banków Polskich, Raport Netbank, *Bankowość internetowa i płatności bezgotówkowe. IV kwartał 2016*, s. 3, Warszawa 2016.12.31, witryna Internet ZBP, https://zbp.pl/public/repozytorium/wydarzenia/images/styczen_2017/konferencja_prasowa/Netbank_Q3_2016_500.pdf [data dostępu: 26.07.2017].

6 Związek Banków Polskich, Raport InfoDOK: W I kwartale 2017 r. codziennie próbowano wyłudzić niemal milion złotych [online], Warszawa 2016.07.04, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2017/czerwiec/raport-infodok-w-i-kwartale-2017-r-codziennie-probowano-wyludzic-niemal-milion-zlotych [data dostępu: 26.07.2017].

W związku z powyższym należy bardzo poważnie podchodzić do sfery bezpieczeństwa przy korzystaniu z usług, jakie oferują banki. Ważny podkreślenia jest także fakt, iż w przypadku tego typu zagrożeń tak naprawdę wiele zależy od banku i tego, jak podchodzi do kwestii bezpieczeństwa. Ale także od samych użytkowników – czy potrafią w sposób właściwy korzystać z dostępnych usług, zachowując tak zwany „zdrowy rozsądek" oraz czy postępują racjonalnie. Jest także trzecia strona, czyli przestępcy. To właśnie oni są główną siłą sprawczą, inicjującą i podejmującą działanie w celu uzyskania informacji, które mogą posłużyć w dalszej kolejności do przejęcia środków finansowych. Przestępcy stosując coraz to nowsze sposoby wyłudzeń, atakują ten podmiot – bank lub klienta, który w danym momencie jest „słabszym ogniwem" – według przestępców. Uwzględniając liczne problemy oraz zagrożenia, w dalszej części artykułu przybliżone zostaną najczęstsze próby ataków na klientów banków korzystających z usług elektronicznych (internetowych oraz mobilnych). Następnie przedstawione zostaną najważniejsze działania instytucji bankowych w zakresie cyberbezpieczeństwa.

1. Charakterystyka najczęstszych zagrożeń cyberbezpieczeństwa

Rocznie straty spowodowane cyberatakami są szacowane dziś na 500 mld dolarów. W wielu państwach szkody związane z internetowymi przestępstwami przekraczają 1 procent PKB[7]. Niestety, wraz z rozwojem usług bankowości internetowej, rośnie też liczba ataków na odbiorców tego kanału, a także obserwowany jest stały przyrost coraz to nowych sposobów wyłudzeń środków pieniężnych klientów. I tak obecnie do najczęstszych ataków związanych z usługami „w sieci" można wymienić:

- włamania do systemów banków w celu malwersacji środków czy też wykradzenia danych klientów,
- podszywanie się pod strony firmowe w celu wyłudzenia haseł, loginów, czy kodów SMS,
- ataki typu *ransomware*,
- *phishing*,
- *spear phishing*,
- wysyłanie maili z plikami typu *malware,*
- wirusy na aplikacjach mobilnych, podobnie jak w przeglądarkach internetowych komputerów, działających również w celu wymuszenia informacji o hasłach, loginach czy kodach SMS,
- ataki hybrydowe, które łączą w sobie kilka technik.

[7] K. Podgórski, *Poradzić sobie z wyzwaniami*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 32.

Pierwszy z wymienionych sposobów dotyczy włamania do systemów informatycznych banków czy też różnego rodzaju instytucji (duże korporacje itp.). Jest to atak mający na celu dostanie się do systemu danej organizacji w celu bądź to bezpośredniego uzyskania dostępu do środków finansowych (najrzadszy przypadek), bądź – co częściej się zdarza – w celu przechwycenia poufnych informacji. Ataki są przeprowadzane na różnego rodzaju przedsiębiorstwa. Jednak ze względu na specyfikę banków i instytucji finansowych, tego typu organizacje znajdują się w czołówce zainteresowań hakerów. Ma to oczywiście związek z tym, że instytucje takie dysponują zarówno wieloma informacjami poufnymi, ale także środkami finansowymi. Warto dodać, że w Polsce banki corocznie wydają duże kwoty związane z cyberbezpieczeństwem, starając się zapewnić swoim klientom pełną ochronę. W związku z tym, duża ilość ataków następuje na ostatni element łańcucha, często ten najsłabszy – mianowicie bezpośrednio ataki wymierzane są na klientów.

Kolejny sposób ataku hakerów jest skierowany na odbiorców usług bankowych. Poprzez sfałszowanie strony internetowej, przestępcy próbują uzyskać poufne informacje od mało spostrzegawczych klientów, którzy nie rozpoznali faktu, że strona internetowa w rzeczywistości nie jest oryginalną stroną banku, ale jej kopią. Po podaniu haseł oraz loginu przestępcy dysponują informacjami pozwalającymi w wielu przypadkach uzyskać dostęp do konta bankowego przez Internet. Dodatkowo w trakcie przeprowadzania operacji na takiej stronie, gdy klient wpisze otrzymane hasło SMS jako autoryzację operacji – może okazać się, że kod dotyczył zupełnie innego rodzaju transakcji niż klient myśli.

Ataki typu ransomware to szyfrowanie dokumentów na dysku i żądanie okupu za odblokowanie danych. Najczęstszym celem tego typu ataków są osoby prywatne. Jednak zdarzają się również ataki na różnego rodzaju instytucje. Jak wynika z raportu opublikowanego przez amerykańskiego Google: ponad 19 milionów funtów zarobili w ciągu ostatnich dwóch lat hakerzy odpowiedzialni za szkodliwe oprogramowanie ransomware. W raporcie amerykański gigant technologiczny podkreślił również, że do tego typu ataków w przyszłości będzie dochodzić coraz częściej. W maju 2017 ofiarą tego typu ataku typu padł brytyjski system publicznej opieki zdrowotnej NHS. Po infekcji wirusem WannaCry w opiece medycznej zapanował kilkudniowy chaos w szpitalach i przychodniach, zmuszając lekarzy do odwołania tysięcy wizyt i konsultacji z pacjentami[8].

Phishing to z kolei wyłudzenie poufnych danych. Zdaniem ekspertów liczba tego typu ataków będzie coraz większa. Mimo że w bardzo dużej liczbie prób klient nie daje się nabrać na ten rodzaj ataku, to ze względu na prostotę oraz możliwości

[8] PAP, *Ataki ransomware to żyła złota dla cyberprzestępców. Google ujawnił kwoty*, [online], Warszawa 2017.07.27, witryna Internet Businessinsider, Warshttp://businessinsider.com.pl/technologie/ile-pieniedzy-przenosza-ataki-ransomware/db6vghl [data dostępu: 29.07.2017].

dotarcia do bardzo dużej liczby użytkowników przestępcy chętnie sięgają po tego typu narzędzie przy próbach wyłudzeń.

Spear phishing to atak typu phishing, ale przeprowadzany na ściśle określonej grupie osób. Tego rodzaju atak wymaga od crakerów zdecydowanie większego nakładu pracy niż w przypadku tradycyjnego phishingu. Każda wiadomość jest przygotowywana oddzielnie, a osoba przygotowująca taki atak musi posiadać odpowiednią porcję informacji o celu ataku. Jednakże wzrasta w związku z tym skuteczność tego rodzaju ataku. Grupą docelową tego ataku są głównie osoby zaliczane do kadry kierowniczej, dzięki czemu w przypadku uzyskania informacji haker dostaje komplet informacji „na talerzu". Dzięki uzyskanym informacjom hakerzy uzyskują dostęp do danych finansowych, kadrowych, handlowych[9].

Wysyłanie maili z plikami typu malware. Jest to przesyłanie wiadomości wraz ze złośliwym oprogramowaniem. Rodzaj i cel działania takiego programu może być różnorodny, w zależności od zamysłu osoby przesyłającej taką wiadomość. Jednym z możliwych działań tego typu programów może być aplikacja, której celem jest podstawianie fałszywego linku do przelewów. Inny rodzaj to oprogramowania szpiegujące, mające na celu przechwycenie jak największej liczby informacji o użytkowniku. Można także wymienić programy typu exploit, które służą do włamania się do komputera w celu wprowadzenia na nim zmian.

Wirusy na aplikacjach mobilnych, podobnie jak w przeglądarkach internetowych komputerów, działających również w celu wymuszenia informacji o hasłach, loginach czy kodach SMS. Można wspomnieć o często pojawiających się czysto mobilnych exploit kitach, dzięki którym coraz więcej odnotowuje się ataków na urządzenia mobilne – prym w tym zakresie wiedzie Android, aplikacje iOS w mniejszym stopniu są atakowane[10].

Ataki hybrydowe, które łączą w sobie kilka technik. Jako przykład można przytoczyć malware finansowy Dyre, który w 2015 roku był jednym z najczęściej wykorzystywanych na świecie do kradzieży pieniędzy z kont. Był on także dostępny w wariancie razem z mechanizmami ransomware oraz DDoS dla zatarcia śladów ataków[11].

Przedstawione powyżej ataki na użytkowników aplikacji internetowych oraz mobilnych wykorzystywane są przez hakerów nie tylko w odniesieniu do korzystania z usług bankowych, czy szerzej finansowych. Częstymi atakami są także użytkownicy innych rodzajów usług, przez co zagrożenie atakiem jest tym większe. Dodać należy również, że oprócz powyżej wymienionych rodzajów ataków istnieje wiele więcej. Dlatego należy zdawać sobie sprawę z powagi i istotności problemu.

---

9 M. Złoch, *Atak na szczyt*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 62-63.

10 A. Król, *Po owocach poznacie, że to atak*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 46.

11 Ibidem.

Jak poważne zagrożenie wiąże się z atakiem hakerów, może uzmysłowić nie tylko ogromna liczba prób wymuszeń, ale również straty związane z przeprowadzanymi atakami, które okazały się skuteczne. Bardzo mało jest organizacji, które decydują się „głośno mówić" o tym fakcie. Jednak można odnaleźć pojedyncze przykłady firm, które zdecydowały się nagłośnić przypadek ataku na ich przedsiębiorstwo. Jako przykład można podać brytyjskiego operatora telekomunikacyjnego „Talk Talk", który w związku z cyberatakiem w październiku 2015 roku na bieżąco informował swoich klientów o działaniach, jakie podejmuje w tej kwestii. Wstępny raport wewnętrzny przeprowadzony przez firmę pokazał, że całe zdarzenie oraz podejście do problemu zostało pozytywnie ocenione przez klientów. Docenili oni fakt, iż przedsiębiorstwo, z którego usług korzystają, było w stosunku do nich szczere i na bieżąco informowało o zaistniałej sytuacji. Podejście takie – rzadko spotykane – jak się okazało przyniosło efekt w postaci wzrostu dynamiki przychodów oraz obniżenia poziomu odejść klientów[12].

Jak jest to duży problem, pokazują także dane ogólnoświatowe. Badania wykazały, że tylko w 2013 r. uzyskano dostęp do 800 milionów rekordów danych osobowych. Zaś według wyliczeń McAfee roczne straty dla globalnej gospodarki związane z cyberprzestępczością to ponad 400 mld dolarów (dane z 2014 roku), a obecnie 500 mld dolarów (dane z 2016 r.). W samej Unii Europejskiej jest to 16 mld dolarów (dane z czerwca 2014 r.). W Polsce co minutę 15 osób pada ofiarą cyberataku, a straty związane z naruszeniem cyberbezpieczeństwa wyniosły ok. 13 mld PLN (dane z 2011 r.). Liczba wykrytych cyberataków na firmy (według Komendy Głównej Policji) w 2015 roku w stosunku do roku poprzedniego wzrosła o 46%[13].

Wiele przytoczonych zagrożeń potwierdza, że w chwili obecnej przestępcy internetowi próbują w coraz to bardziej wyszukany i bardzo skomplikowany sposób dokonać wyłudzeń nie tylko od instytucji finansowych, ale i ich klientów.

2. Charakterystyka głównych działań banków oraz instytucji finansowych w celu zapewnienia cyberbezpieczeństwa

Zaawansowane zagrożenia dotyczące usług bankowości internetowej oraz mobilnej spowodowały liczne działania ze strony instytucji finansowych zmierzających do zapewnienia oraz poprawy bezpieczeństwa świadczonych usług. Jak wcześniej zaznaczono, wiele firm, które padły atakiem hakerów nie ujawnia tego faktu. Głównie ze względu na spadek zaufania w oczach klientów, strach przed postrzeganiem

[12] S. Dolecki, *Brutalna cyberrzeczywistość*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 51.

[13] A. Matusiak, S. Szepietowski, *Banking Tech & Security. Odpowiedzialność banku za zapewnienie cyberbezpieczeństwa*, Bird & Bird, Warszawa 27 stycznia 2016, s. 3-4; Miesięcznik finansowy BANK, nr 4 (276) 2016, s. 32.

jako podmiotu, który nie potrafi skutecznie bronić się przed cyberprzestępcami. Niestety, takie działania często skutkują tym, iż pomagają przestępcom w kolejnych ich atakach oraz sprzyjają unikaniu odpowiedzialności.

Warto dodać, że na ataki narażeni są nie tylko indywidualni klienci. Można odnotować także wiele ataków na największe instytucje finansowe na świecie. Dla przykładu hakerzy skutecznie włamali się do Europejskiego Banku Centralnego. Inny przykład to kradzież ponad 27 tysięcy poufnych danych klientów banku Barclays, albo kradzież około 100 mln dolarów z konta banku centralnego Bangladeszu zdeponowanych w Banku Rezerwy Federalnej w Nowym Jorku[14].

W nawiązaniu do powyższego, w Polsce również najważniejsze instytucje dostrzegają problem, jaki wiąże się z cyberprzestępczością. Wraz z rozwojem platform informatycznych oraz technologii ich wykorzystania, rosną możliwości niepowołanego dostępu do danych. Każdego dnia atakowanych jest wiele systemów teleinformatycznych oraz ich użytkownicy. Skala włamań do systemów rośnie lawinowo. Banki jako instytucje zaufania publicznego, ale także dysponujące szczególnie cennymi informacjami, zdają sobie sprawę z zagrożeń współczesnego świata.

Wspomnieć należy tutaj, iż banki w ramach działań wewnętrznych prowadzonych przez Związek Banków Polskich (ZBP) nawiązały współpracę pomiędzy sobą. Oprócz stosowanych zabezpieczeń wewnętrznych, banki – świadome zagrożeń ze strony hakerów – coraz mocniej współpracują ze sobą w celu wyeliminowania jak największej liczby zagrożeń. Współpracują one ze sobą wraz z ZBP w ramach dwóch grup tematycznych w obszarze cyberbezpieczeństwa, by dzielić się doświadczeniami z zakresu bezpieczeństwa transakcji internetowych i mobilnych oraz transakcji dokonywanych przy użyciu kart płatniczych. W ramach Związku Banków Polskich funkcjonuje ponadto inna jednostka, która zajmuje się bezpieczeństwem w pozostałych obszarach. Współpraca pomiędzy tymi trzema ciałami świadczy o wysokim priorytecie traktowania zagrożeń związanych z atakami cyberprzestępców[15].

Należy wymienić także organizowane pod egidą Związku Banków Polskich „Forum Bezpieczeństwa Banków". Organizowane od 2012 roku konferencje mają na celu wymianę doświadczeń z zakresu bezpieczeństwa oraz ich zagrożeń. Przyczynić się to ma do poprawy ogólnego poziomu bezpieczeństwa zarówno instytucji finansowych, jak i ich klientów. IV Forum Bezpieczeństwa Banków poświęcone było niemal w całości doktrynie cyberbezpieczeństwa[16].

Kolejnym krokiem w kierunku poprawy bezpieczeństwa w sieci swoich klientów są publikowane przez banki ogłoszenia oraz komunikaty na ich stronach

[14] Prezentacja Quest *Dystrybucja, Zintegrowane i efektywne zarządzanie bezpieczeństwem w banku. Skuteczne sposoby zapobiegania największym zagrożeniom bezpieczeństwa informacji*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 60.

[15] P.M. Balcerzak, *Potrzebujemy cybertarczy sektora bankowego*, BANK Miesięcznik finansowy, 5/2015, s. 40-41.

[16] J. Trzaska, *Bankowa cybertarcza 2015*, BANK Miesięcznik finansowy, nr 5 (266) 2015, s. 43-45.

internetowych. Działania takie mają zarówno charakter stały – publikowanie podstawowych zasad bezpieczeństwa związanych z korzystaniem z urządzeń mobilnych czy w trakcie korzystania z aplikacji internetowych, jak również doraźny – publikacja komunikatów w związku z wystąpieniem konkretnego zagrożenia czy ataku.

W zakresie cyberbezpieczeństwa należy podkreślić bardzo dużą rolę Związku Banków Polskich – nie tylko jako inicjatora we współpracy pomiędzy bankami czy instytucji współtworzącej forum bezpieczeństwa banków. ZBP wydał ponadto poradnik „Cyberbezpieczny portfel", który w swej treści zawiera dużo cennych informacji oraz wskazówek dla użytkowników kart płatniczych, ale także bankowości internetowej oraz mobilnej. Dzięki poradom można znacząco ograniczyć ryzyko utraty środków.

Do grona działań ZBP należy zaliczyć także otwarcie 4 lipca 2016 roku Narodowego Centrum Cyberbezpieczeństwa. Jedną z kluczowych platform tego nowoczesnego projektu jest Bankowe Centrum Cyberbepieczeństwa. Instytucji, której celem będzie wykrywanie cyberzagrożeń, ich analiza, ale także operacyjne przeciwdziałanie skutkom ataków hakerskich na systemy informatyczne banków i innych instytucji publicznych[17].

Z kolei, jednym z najnowszych projektów realizowanych przez wcześniej wymienioną instytucję w zakresie poprawy cyberbezpieczeństwa jest projekt „Bezpieczeństwo w Cyberprzestrzeni" podpisany podczas Kongresu Edukacji Finansowej 2017 w dniu 28 marca 2017 roku na PGE Narodowym w Warszawie. Pod dokumentem inicjującym podpisy złożyli przedstawiciele: Związku Banków Polskich, Banku Pekao S.A., Banku Zachodniego WBK S.A., ING Banku Śląskiego S.A., Fundacji KIR na rzecz Rozwoju Cyfryzacji Cyberium oraz firm technologicznych: IBM Polska i MICROSOFT. Porozumienie zakłada podjęcie wspólnych działań na rzecz szerokiej budowy podstawowej wiedzy z zakresu cyberbezpieczeństwa, z uwzględnieniem zapewnienia ochrony systemów, infrastruktury teleinformatycznej oraz samych informacji. Temat cyberbezpieczeństwa był jednym z motywów pierwszej edycji Kongresu, który w salach PGE Narodowego zgromadził ponad 300 przedstawicieli reprezentujących około 150 instytucji i podmiotów z obszaru finansów, edukacji i szkoleń[18].

Kończąc rozważania z zakresu działań związanych z przeciwdziałaniem ataków na użytkowników w sieci, Związek Banków Polskich opublikował na swojej stronie internetowej informację na temat podstawowych zasad związanych z korzystaniem z kanałów elektronicznych zatytułowany „Cyberbezpieczeństwo Twoich pieniędzy".

---

[17] Związek Banków Polskich, Otwarcie Bankowego Centrum Cyberbezpieczeństwa [online], Warszawa 04.07.2016, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [data dostępu: 26.07.2017].

[18] Związek Banków Polskich, Banki dla edukacji w obszarze cyberbezpieczeństwa [online], Warszawa 28.03.2017, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2017/marzec/banki-dla-edukacji-w-obszarze-cyberbezpieczenstwa [data dostępu: 26.07.2017].

W informacji odnaleźć można podstawowe zasady bezpieczeństwa, którymi powinien się kierować każdy użytkownik produktów bankowych. Przedstawiono także najczęstsze błędy, jakie popełnia statystyczny klient banków przy korzystaniu z produktów elektronicznych. Komunikat ma na celu ustrzec klientów instytucji finansowych przed niewłaściwym korzystaniem ze swoich produktów, co skutkować by mogło narażeniem na utratę posiadanych pieniędzy[19].

Zakończenie

Przedstawione pokrótce zagrożenia oraz ich skala dowodzą wysokiej szkodliwości działań przestępczych, która jest widoczna w wielu obszarach. Nieustannemu i bardzo szybkiemu rozwojowi oraz doskonaleniu się nowych technologii niemal równolegle towarzyszy rozwój „złych" technologii, które wykorzystywane są do nadużyć i przestępstw. Należy odnotować, iż w bankowości nacisk na ostrożność i bezpieczeństwo jest dużo większy niż w innych sektorach, bo tu cybernadużycie przynosi skutki natychmiast odczuwalne. Ponadto jest duża przestrzeń do powstawania zagrożeń – szacuje się, że obecnie w Polsce są 32 miliony rachunków internetowych i 35 milionów kart płatniczych. Te dwa obszary są bardzo narażone na ataki. Dlatego ważne jest dokładne zlokalizowanie segmentów, w których takie ataki mogą wystąpić, a następnie podjęcie działań mających na celu możliwie jak największe wyeliminowanie zagrożeń. Na uwagę zasługuje ponadto fakt, iż w chwili obecnej w Polsce nie ma banku, który by nie spełniał podstawowych wymogów bezpieczeństwa elektronicznego. W tym zakresie podejście banków jest solidarne, chociażby ze względu na brak konkurencji w tym zakresie między bankami, czy konfliktu interesów. Tam, gdzie w grę wchodzi bezpieczeństwo, banki nie konkurują ze sobą, tylko współdziałają. Kolejną instytucją stojącą na straży cyberbezpieczeństwa jest Komisja Nadzoru Finansowego, która wydała dyrektywę D w sprawie bezpieczeństwa systemów IT w bankach, podnosząc rangę tej sfery. W myśl tej dyrektywy za cyberbezpieczeństwo nie jest odpowiedzialny już tylko dział IT, ale cały zarząd. Warto mieć na uwadze, że mimo coraz to nowszych zagrożeń i wzrastającej liczby ataków cyberprzestępców zarówno w Polsce, jak i na całym świecie, wzrasta świadomość ważności problemu oraz towarzyszą temu nieustanne próby przeciwdziałania ze strony najważniejszych instytucji finansowych. Warto także pamiętać, iż za poprawę bezpieczeństwa odpowiada sam użytkownik, który jest tym elementem, który obecnie bywa najczęściej narażony na potencjalny atak ze strony hakerów. Stąd tak ważne jest stosowanie podstawowych zasad bezpieczeństwa.

[19] Związek Banków Polskich, Cyberbezpieczeństwo Twoich pieniędzy [online], Warszawa 17.10.2016, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/pazdziernik/cyberbezpieczenstwo-twoich-pieniedzy [data dostępu: 26.07.2017].

LITERATURA

[1] Anderson R., *Inżynieria zabezpieczeń*, Wydawnictwa Naukowo-Techniczne, Warszawa 2005.

[2] Balcerzak P.M., *Potrzebujemy cybertarczy sektora bankowego*, BANK Miesięcznik finansowy, 5/2015 s. 40-42.

[3] Cole E., Krutz R. L., Conley J., *Bezpieczeństwo sieci – Biblia*, Wydawnictwo HELION, Gliwice 2005.

[4] Dolecki S., *Brutalna cyberrzeczywistość*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 50-51.

[5] Król A., *Po owocach poznacie, że to atak*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 46-49.

[6] Matusiak A., Szepietowski S., *Banking Tech & Security. Odpowiedzialność banku za zapewnienie cyberbezpieczeństwa*, Bird & Bird, Warszawa 27 stycznia 2016.

[7] Podgórski K., *Poradzić sobie z wyzwaniami*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 30-33.

[8] Prezentacja Quest *Dystrybucja, Zintegrowane i efektywne zarządzanie bezpieczeństwem w banku. Skuteczne sposoby zapobiegania największym zagrożeniom bezpieczeństwa informacji*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 60-61.

[9] Strebe M., *Bezpieczeństwo sieci – podstawy*, Wydawnictwo MIKOM, Warszawa 2005.

[10] Trzaska J., *Bankowa cybertarcza 2015*, BANK Miesięcznik finansowy, nr 5 (266) 2015, s. 43-45.

[11] Złoch M., *Atak na szczyt*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 62-63.

ONLINE SOURCES

[1] *Cyberdefence24, Dekalog bankowego cyberbezpieczeństwa według wiceprezesa Związku Banków Polskich*. WYWIAD. [online], witryna Internet http://www.cyberdefence24.pl/579395,dekalog-bankowego-cyberbezpieczenstwa-wedlug-wiceprezesa-zwiazku-bankow-polskich-wywiad, [data dostępu: 14.06.2017].

[2] MAISON & PARTNERS, Raport Badanie otwartości polskich konsumentów na innowacyjne metody płatności. witryna Internet [online], Warszawa, 27.04.2016, https://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-polscy-konsumenci-otwarci-na-cyfrowe-innowacje/, [data dostępu: 14.06.2017].

[3] PAP, Ataki ransomware to żyła złota dla cyberprzestępców. Google ujawnił kwoty, Związek Banków Polskich, Banki dla edukacji w obszarze cyberbezpieczeństwa [online], Warszawa 28.03.2017, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2017/marzec/banki-dla-edukacji-w-obszarze-cyberbezpieczenstwa [data dostępu: 26.07.2017].

[4] Związek Banków Polskich, Cyberbezpieczeństwo Twoich pieniędzy [online], Warszawa 17.10.2016, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/pazdziernik/cyberbezpieczenstwo-twoich-pieniedzy [data dostępu: 26.07.2017].

[5] Związek Banków Polskich, Otwarcie Bankowego Centrum Cyberbezpieczeństwa [online], Warszawa 04.07.2016, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [data dostępu: 26.07.2017].

[6] Związek Banków Polskich, Raport InfoDOK: W I kwartale 2017 r. codziennie próbowano wyłudzić niemal milion złotych [online], Warszawa 2016.07.04, witryna Internet ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2017/czerwiec/raport-infodok-w-i-kwartale-2017-r-codziennie-probowano-wyludzic-niemal-milion-zlotych [data dostępu: 26.07.2017].

[7] Związek Banków Polskich, Raport Netbank, Bankowość internetowa i płatności bezgotówkowe. IV kwartał 2016, s. 3. Warszawa 2016.12.31, witryna Internet ZBP, https://zbp.pl/public/repozytorium/wydarzenia/images/styczen_2017/konferencja_prasowa/Netbank_Q3_2016_500.pdf [data dostępu: 26.07.2017].

[8] [online], Warszawa 2017.07.27, witryna Internet Businessinsider, Warshttp://businessinsider.com.pl/technologie/ile-pieniedzy-przenosza-ataki-ransomware/db6vghl [data dostępu: 29.07.2017].

[9] Rzeczpospolita, Mieczyław Groszek: Cyberbezpieczeństwo warunkiem nowoczesnej bankowości, witryna Internet [online], http://www.rp.pl/Opinie/301249907-Mieczylaw-Groszek-Cyberbezpieczenstwo-warunkiem-nowoczesnej-bankowosci.html, [data dostępu: 14.06.2017].