Radosław Balkowski

KNF
KOMISJA
NADZORU
FINANSOWEGO

Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady

Poradnik klienta usług finansowych

PORADNIK KLIENTA
USŁUG FINANSOWYCH

Radosław Balkowski

BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH – ZMIANY, TRENDY I ZASADY

Warszawa 2018

KNF | KOMISJA NADZORU FINANSOWEGO

Publikacja została wydana nakładem Komisji Nadzoru Finansowego

Warszawa 2018
Wydanie I

ISBN 978-83-63380-16-8

Nakład: 1000 szt.

Stan prawny na dzień: 19 kwietnia 2018 r.

Przygotowanie do druku i druk:
Drukarnia Biały Kruk Milewscy sp.j.

Spis treści

I. WSTĘP

Skala zagrożeń i ryzyk związanych z przestępczością internetową, szczególnie w bankowości elektronicznej, rośnie i będzie rosła wraz z nieuniknionym, dalszym rozpowszechnianiem się usług bankowości elektronicznej, rozwojem technologii mobilnych czy rozwiązań takich jak IoT (Internet of Things). Coraz łatwiejszy dostęp oraz atrakcyjność usług oferowanych drogą elektroniczną, często niewymagających osobistego udania się do banku czy innego punktu usługowego, powoduje znaczący wzrost wolumenu usług świadczonych tą drogą, a w związku z tym również wzrost zagrożeń.

Rozwój bankowości internetowej pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności wymierzonej przeciwko bezpieczeństwu danych, zagrażających bezpieczeństwu finansowemu na rynku usług bankowych, w szczególności bezpieczeństwu środków zgromadzonych na rachunku bankowym, do których możliwy jest dostęp na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak: komputer, telefon, tablet itp.

Niniejsza publikacja adresowana jest przede wszystkim do klientów usług finansowych, ale informacje, które się w niej znajdują, mogą być również, w pewnym zakresie, przydatne pracownikom instytucji finansowych.

W części pierwszej (podstawowej) przedstawiono główne zagrożenia związane z korzystaniem z usług bankowości internetowej i mobilnej. Czytelnik, zapoznając się z konkretnymi przykładami, ilustrującymi schematy działania przestępców, otrzymuje jednocześnie praktyczne wskazówki pozwalające mu na bezpieczne korzystanie z usług finansowych i ograniczające ryzyko utraty środków finansowych, kradzieży danych osobowych czy innych poufnych informacji. Gdyby jednak Czytelnik, czego nie można całkowicie wykluczyć, mimo przestrzegania przedstawionych w niniejszej publikacji podstawowych reguł bezpieczeństwa, stał się ofiarą przestępstwa, to powinien wiedzieć jakie czynności musi wtedy podjąć, aby mieć szansę na odzyskanie środków lub ograniczenie dalszych strat – te informacje zawarte są w końcowych punktach części pierwszej.

Część druga (rozszerzona), przeznaczona dla bardziej zaawansowanych i doświadczonych klientów, zawiera szeroki przegląd zagrożeń związanych z wykorzystywaniem usług finansowych oferowanych przy pomocy Internetu, obejmujący klasyfikację rodzajów szkodliwego oprogramowania, z uwzględnieniem tła historycznego oraz opisy technik najczęściej przeprowadzanych ataków (w tym DDoS, phishing, ataki z wykorzystaniem botnetów). Przedstawiono działania, jakie podejmuje Komisja Nadzoru Finansowego jako organ nadzoru, by ograniczyć ryzyko tego typu zagrożeń dla instytucji finansowych i ich klientów, w tym załączono syntetyczne opisy opublikowanych rekomendacji.

W końcowej części publikacji przedstawiono rozwiązania (w tym nowoczesne techniki autoryzacji, metody biometryczne i behawioralne) oraz usługi (w tym Cloud Computing), które mogą zasadniczo zmienić funkcjonowanie rynku usług finansowych ze względu na zaawansowane mechanizmy bezpieczeństwa, zapewniające jednocześnie wygodne korzystanie z wielu kanałów elektronicznych.

Ze względu na szeroki zakres tematu publikacji nie jest możliwy pełny przegląd przedstawionych zagadnień, niektóre są z konieczności tylko nakreślone i od Czytelnika zależy, które z nich będą warte pogłębienia poprzez lekturę innych źródeł czy publikacji.

II. SŁOWNIK POJĘĆ

0 day – podatność, która pojawiła się przed jej usunięciem przez producenta oprogramowania.

Application Programming Interface (API) – specjalnie udostępniony programistyczny interfejs aplikacji służący do komunikacji między programami, zdefiniowany na poziomie kodu źródłowego.

Autentykacja – patrz: Uwierzytelnienie

Autoryzacja – proces mający na celu potwierdzenie, czy dany podmiot lub klient jest uprawniony do uzyskania dostępu do żądanego zasobu.

Biały wywiad – wywiad źródeł jawnych. Forma pracy wywiadowczej oparta na legalnie i ogólnie dostępnych źródłach.

Card Verification Value (CVV) – 3-cyfrowy kod służący do weryfikacji, czy osoba posługująca się kartą płatniczą jest jej uprawnionym posiadaczem.

Ciastka (Cookies) – niewielkie pliki przechowywane lokalnie na komputerze lub innym urządzeniu podczas wchodzenia na strony internetowe mogące przechowywać różne informacje, np. dotyczące zalogowanej sesji.

Cloud Computing – model przetwarzania danych oparty na rozproszonych zasobach.

Content Management System (CMS) – system zarządzania treścią stron internetowych. Oprogramowanie pozwalające na łatwe tworzenie oraz modyfikację serwisów WWW.

Credit Verification Code (CVV/CVC) – numer weryfikacyjny karty, który jest wydrukowany na odwrocie karty debetowej lub kredytowej.

Crowdsourcing – proces (model), w ramach którego organizacja przeprowadza zadanie wykonywane przez pracowników do niezidentyfikowanej, zwykle bardzo szerokiej grupy ludzi, w formie powszechnego powierzenia zleconej usługi.

Cyberprzestępstwo – przestępstwo popełnione z wykorzystaniem (użyciem) sieci telekomunikacyjnych (np. publicznej komutowanej sieci telefonicznej – PSTN, sieci komputerowej, Internetu, sieci teleksowej, cyfrowej sieci z integracją usług – ISDN).

Cyberatak – atak wykonany z wykorzystaniem sieci telekomunikacyjnych (np. Internetu).

Denial of Service (DoS) – atak polegający na przeciążeniu serwera poprzez wysyłanie do niego dużych ilości danych (np. zapytań do działającej usługi) wymagających reakcji (odpowiedzi na zapytanie) w celu uniemożliwienia lub spowolnienia jego działania.

Distrubuted Denial of Service (DDoS) – rozproszona (zwielokrotniona) wersja ataku DoS.

Domain Name System (DNS) – zbiór, do którego należą: serwery, protokoły komunikacyjne oraz usługi obsługujące bazę danych adresów sieciowych. Pozwala on na zamianę adresów rozumianych przez człowieka (ciąg znakowy w określonym formacie) na adres odczytywany przez komputery (adres IP).

Entropia – najmniejsza średnia ilość informacji potrzebna do zakodowania faktu zajścia zdarzenia ze zbioru zdarzeń o danych prawdopodobieństwach. Entropia nazywana jest również „miarą nieporządku", czym wyższa, tym mniejsze prawdopodobieństwo zaistnienia konkretnego zdarzenia.

Financial Technology (FinTech) – firmy, które wykorzystują nowoczesne technologie w oferowaniu usług finansowych.

Firewall – zapora sieciowa, jeden ze sposobów zabezpieczenia i separacji zasobów poszczególnych segmentów sieci.

Framework – platforma programistyczna. Szkielet służący do budowy aplikacji, definiujący strukturę oraz ogólny mechanizm jej działania.

Iteracja – metoda w analizie matematycznej i programowaniu polegająca na wielokrotnym stosowaniu tego samego przekształcenia lub procedury; też: kolejne przekształcenie lub procedura[1].

Internet of Things (Internet rzeczy, IoT) – koncepcja, w której przedmioty mogą gromadzić, przetwarzać dane za pomocą sieci komputerowej.

JavaScript – skryptowy język programowania, działający po stronie klienta, interpretowany za pomocą przeglądarki internetowej.

Język zapytań – język wykorzystywany do formułowania zapytań bazodanowych.

Skryptowy język programowania – język programowania służący do kontrolowania aplikacji i pracujący w niej. Programy napisane w językach skryptowych są wykonywane wewnątrz danej aplikacji.

Komisja Nadzoru Finansowego (KNF) – państwowy organ nadzoru sprawujący nadzór nad rynkiem finansowym, który obejmuje: nadzór bankowy, nadzór emerytalny, nadzór ubezpieczeniowy, nadzór nad rynkiem kapitałowym, nadzór nad instytucjami płatniczymi, biurami usług płatniczych, instytucjami pieniądza elektronicznego, oddziałami zagranicznych instytucji pieniądza elektronicznego, nadzór nad agencjami ratingowymi, nadzór uzupełniający nad konglomeratami finansowymi, nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową, a także nadzór nad pośrednikami kredytu hipotecznego oraz ich agentami. Celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku.

[1] Źródło: Słownik języka polskiego PWN - http://sjp.pwn.pl/sjp/iteracja;2562037.html [dostęp 12.02.2018 r.]

Kompromitacja danych – przejęcie danych przez atakującego oszusta.

Linux – rodzaj systemu operacyjnego.

Login – nazwa użytkownika, zwykle przypisana przez system teleinformatyczny w celu identyfikacji podmiotu lub klienta.

Makro – zestaw rozkazów mających na celu wykonanie zadania przez określoną aplikację.

Mitygacja – ograniczanie, np. ryzyka wystąpienia zdarzenia.

Multimedia Messaging Service (MMS) – usługa umożliwiająca przesyłanie multimediów, takich jak: animacje, filmy, grafika czy dźwięki w postaci wiadomości wysyłanych między telefonami komórkowymi.

Oszustwo nigeryjskie (Nigeryjski szwindel, afrykański szwindel, Nigerian scam, 419 scam) – rodzaj oszustwa, polegającego na namówieniu ofiary na transfer pieniędzy do jednego z krajów afrykańskich (początkowo do Nigerii) w celu uzyskania dużej korzyści (np. udział w dużym spadku).

Outsourcing – powierzenie zadań, funkcji wykonywanych przez przedsiębiorstwo innym zewnętrznym podmiotom.

Pay-by-link – przelew bezpośredni uruchamiany specjalnie wygenerowanym linkiem. Wszystkie dane potrzebne do wykonania przelewu są wypełniane automatycznie, a klient musi tylko zatwierdzić przelew w systemie bankowości internetowej.

Podatność (vulnerability) – słabość. Brak odporności systemu na skutki wrogiego działania.

Serwer pośredniczący (proxy) – serwer (program), który dokonuje operacji w imieniu użytkownika, np. pośredniczy w komunikacji sieciowej.

Sesja – obiekt przechowujący informacje dotyczące szczegółów zainicjowanego połączenia między serwerem a klientem.

Skrypt – program napisany w języku skryptowym, służący do wykonywania pewnych zadań wewnątrz danej aplikacji.

Structured Query Language (SQL) – język zapytań używany przy komunikacji między aplikacją a bazą danych.

System operacyjny – oprogramowanie tworzące środowisko do uruchamiania kontroli zadań i aplikacji użytkownika.

Token – generator kodów jednorazowych, służący jako czynnik autoryzacyjny.

Uwierzytelnienie – proces służący do weryfikacji zadeklarowanej tożsamości podmiotu lub klienta.

WAF – firewall dedykowany ochronie aplikacji webowych.

Wtyczka – dodatkowy program rozszerzający możliwości innego programu[2].

[2] Źródło: Słownik języka polskiego PWN - http://sjp.pwn.pl/sjp/plug-in;2571775.html [dostęp 12.02.2018 r.]

III. CZĘŚĆ PODSTAWOWA

1. DZIAŁALNOŚĆ KNF

Kampania KNF „Zadbaj o swoje bezpieczeństwo w sieci”

W ramach ustawowych zadań Komisji Nadzoru Finansowego (KNF) dotyczących podejmowania działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego, Urząd Komisji Nadzoru Finansowego (UKNF) zrealizował kampanię informacyjną „Zadbaj o swoje bezpieczeństwo w sieci”, we współpracy z mediami publicznymi – Telewizją Polską SA oraz Polskim Radiem SA. Celem kampanii było zwrócenie uwagi użytkowników bankowości elektronicznej na ryzyka związane z korzystaniem z usług bankowych przez Internet oraz wskazanie podstawowych zasad zwiększających bezpieczeństwo finansowe w sieci. W czasie jej trwania na antenach TVP1, TVP2, TVP Info, TVP Regionalna oraz PR1, PR3, PR4 i PR24 wyemitowano 30-sekundowe spoty informujące o ryzyku występującym w bankowości elektronicznej. Spoty wyemitowane w ramach ww. kampanii społeczno-informacyjnej są dostępne na stronach internetowych KNF www.knf.gov.pl).

Kampania społeczna „Zadbaj o swoje bezpieczeństwo w sieci” została silnie wsparta także działaniami w mediach społecznościowych. UKNF za pośrednictwem mediów społecznościowych (Facebook i Twitter), aktywnie promował podstawowe zasady bezpieczeństwa przy korzystaniu z bankowości elektronicznej. Specjalnie przygotowane plansze graficzne codziennie przez okres trzech tygodni przypominały, jak w prosty sposób można zmniejszyć ryzyko utraty środków finansowych przy próbie przeprowadzenia cyberataku[3].

W ramach tej kampanii UKNF skierował list do konsumentów, w którym przypomina o świadomym korzystaniu z bankowości elektronicznej:

„Drogi Użytkowniku bankowości elektronicznej!

Zmiany technologiczne i cywilizacyjne sprawiają, że usługi oferowane przez Internet dynamicznie zyskują na znaczeniu. Aktywnie korzysta z nich kilkanaście milionów mieszkańców Polski. To kanał wygodny i stosunkowo tani, ale jednym ze skutków ubocznych jest zwiększone zainteresowanie wykorzystaniem go przez przestępców. Istotne stały się takie zagrożenia jak wyłudzanie danych pozwalających na dysponowanie środkami pieniężnymi, kradzieże z wykorzystaniem złośliwego oprogramowania, kradzieże przy użyciu danych karty płatniczej, kradzieże tożsamości, „oszustwa nigeryjskie”, czy kradzieże w sklepach internetowych. Banki i inne instytucje finansowe, jako dostawcy usług internetowych, są zobowiązane do stosowania zabezpieczeń przed cyberprzestępstwami. Słabym

[3] Źródło: Sprawozdanie z działalności Komisji Nadzoru Finansowego w 2015 roku, s. 179.

ogniwem pozostaje jednak człowiek. Dlatego o bezpieczeństwo swoich środków i danych powinniśmy zadbać także my – konsumenci, zachowując podstawowe zasady bezpieczeństwa.

Pamiętaj, chroń swoje dane. *Login i hasło powinny być znane tylko Tobie. Udostępnienie ich osobom trzecim naraża Cię na utratę środków finansowych. Zachowaj szczególną ostrożność wobec osób, które chcą te dane pozyskać. Jeśli w systemie internetowym lub w swoim sprzęcie dostrzegłeś podejrzane zmiany albo masz jakiekolwiek inne wątpliwości w zakresie bezpieczeństwa, upewnij się w swojej instytucji finansowej, że wszystko jest w porządku. Sprawdź, czy w ostatnim czasie nie przestrzegała ona przed podejrzanymi wiadomościami rozsyłanymi drogą elektroniczną. Zachowanie poufności, spokoju i zdrowego rozsądku zwiększy Twoje bezpieczeństwo finansowe w sieci.*

Urząd Komisji Nadzoru Finansowego" [4]

Oprócz spotów i zacytowanego listu, opublikowano na stronie internetowej plansze graficzne z podstawowymi zasadami bezpieczeństwa przy korzystaniu z bankowości internetowej:

1. Nie udostępniaj nikomu loginu i hasła do systemu bankowości elektronicznej.
2. Cyklicznie zmieniaj hasło do logowania w systemie bankowości elektronicznej.
3. Nie otwieraj podejrzanych linków w otrzymanych wiadomościach e-mail i SMS.
4. Zainstaluj i aktualizuj oprogramowanie antywirusowe, które może uchronić komputer i urządzenia mobilne przed wirusami oraz oprogramowaniem szpiegującym. Na bieżąco aktualizuj system operacyjny urządzenia oraz cyklicznie skanuj każde urządzenie programem antywirusowym.
5. Cyklicznie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie.
6. Przed potwierdzeniem transakcji zawsze weryfikuj zgodność numeru konta, na które przelewasz środki pieniężne z numerem odbiorcy oraz numerem, który jest w kodzie potwierdzającym transakcję, przekazanym z wykorzystaniem SMS (jeżeli ta funkcjonalność jest udostępniona).
7. Na bieżąco przeglądaj historię rachunku i operacji na każdej karcie płatniczej pod kątem podejrzanych transakcji. Jeżeli jest to możliwe, to włącz powiadomienia SMS o każdej wykonywanej transakcji.
8. Nie kopiuj numerów rachunków bankowych do przelewów („kopiuj-wklej"), ale wpisuj je samodzielnie i dokładnie weryfikuj.
9. Nie korzystaj z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń (np. publicznej WiFi).

[4] Źródło: http://www.knf.gov.pl/bezpieczenstwo_w_sieci [dostęp 12.02.2018 r.]

10. Zadbaj, aby każde używane oprogramowanie pochodziło z legalnego i zaufanego źródła.
11. Jeżeli zaobserwujesz nietypowe lub podejrzane działania, niezwłocznie zgłoś ten fakt do banku, z którego usług korzystasz w ramach bankowości elektronicznej.

PAMIĘTAJ! Twoje bezpieczeństwo finansowe w sieci zależy w pierwszej kolejności od Ciebie[5].

2. BEZPIECZNE KORZYSTANIE Z BANKOWOŚCI INTERNETOWEJ

Żadne zabezpieczenia techniczne nie pomogą nam, jeśli sami nie będziemy stosować się do podstawowych zasad bezpieczeństwa!

Przykład 1

Pani Eulalia, starsza, niedosłysząca osoba, w ramach wdzięczności za troskę i opiekę, jaką otrzymała od swojego wnuczka, postanowiła, że na jego osiemnaste urodziny kupi mu upragniony, nieduży, używany samochód.

Wymarzony pojazd znalazła szybko. Z bardzo atrakcyjną ofertą zjawił się sąsiad z klatki obok. Sąsiada znała wiele lat, więc przystała na złożoną jej ofertę. Niestety, starsza Pani nie dysponowała taką gotówką, więc postanowiła udać się do banku po kredyt. Po otrzymaniu odmowy postanowiła skorzystać z oferty instytucji pożyczkowej. Część wkładu już miała, więc uznała, że weźmie niedużą pożyczkę na kilka miesięcy. Pani Eulalia jechała autobusem, kiedy zadzwonił wyczekiwany telefon z firmy oferującej szybkie pożyczki.

Miły Pan konsultant instytucji pożyczkowej poprosił o przekazanie danych znajdujących się na dowodzie osobistym. Pani Eulalia poirytowała współpasażerów, ponieważ ze względu na problemy ze słuchem robiła to bardzo głośno.

Blisko niej siedział młody człowiek ze słuchawkami na uszach, smartphonem w ręku i uważnie słuchał.

Zanim Pani Eulalia wyszła z autobusu, na swoje nazwisko miała wziętą nie jedną, ale dwie szybkie pożyczki.

Zapamiętaj!

Nie powinno się podawać danych osobowych w miejscach, gdzie mogą one być podsłuchane lub zapisane przez inną osobę. Dane te mogą zostać wykorzystane do włamania na nasze konto.

[5] Źródło:https://www.knf.gov.pl/knf/pl/komponenty/img/knf_140954_KNF_bezpieczenstwo_w_bankowosci_elektronicznej_21_42826.09_42826.2015_42826.pdf [dostęp 12.02.2018 r.]

Przykład 2

Maurycy był zmęczony ciągłymi problemami finansowymi. Pomyślał, że najwyższa pora poszukać dodatkowej pracy.

Podczas przeszukiwania setek ogłoszeń dla freelancerów, grafików, handlowców czy konsultantów, znalazł interesujące ogłoszenie o następującej treści:

„PHU Kazimierz W. z Kazimierza Górnego poszukuje:

Skręcacza długopisów – 50zł/h

Pracownik na to stanowisko zostanie wyłoniony drogą konkursową. Aby wziąć udział w konkursie, proszę przesłać swoje CV na nasz adres e-mail".

Czym prędzej zabrał się za przygotowanie CV i aplikacji.

Po kilkunastu dniach otrzymał list. Z lekkim niepokojem zaczął go czytać.

W wiadomości oprócz informacji o wygranej była również instrukcja służąca do dokonania finalizacji wymagań formalnych i podpisania umowy.

Maurycy został poproszony o przesłanie podstawowych informacji potrzebnych do podpisania umowy, w tym PESEL, nazwisko panieńskie matki, imię ojca, imię matki oraz skan dowodu osobistego.

Został również poinformowany, że dalsza część procesu może trochę potrwać, ponieważ obsługująca firma księgowa mieści się na Pomorzu, a umowa zostanie wysłana listem zwykłym.

Maurycy czekał długo na list z umową, ale on nigdy do niego nie dotarł.

Z czasem zaczęły się pojawiać listy od firm windykacyjnych. Na początku Maurycy próbował sprawy wyjaśniać, tłumacząc wszystko najzwyklejszą pomyłką. Nawet kolejne listy z innych firm windykacyjnych nie wzbudziły u niego żadnych podejrzeń. Dopiero wizyta dzielnicowego uświadomiła mu, że padł ofiarą oszustwa, a dane, które przekazał firmie „PHU Kazimierz W. z Kazimierza Górnego", zostały wykorzystane do licznych wyłudzeń.

Przekazywanie swoich poufnych danych osobom, których nie znamy, może narazić nas na niebezpieczeństwo wykorzystania danych przez przestępców. W każdej sytuacji, gdy jesteśmy proszeni o podanie swoich danych osobowych, powinniśmy być czujni, nawet w sytuacji, gdy ktoś proponuje nam pracę lub prowadzenie własnej firmy.

Przykład 3

Bartosz jest studentem, który stara się wykorzystywać różne możliwości zarabiania pieniędzy. Dlatego też, gdy w jednym z portali społecznościowych zobaczył ogłoszenie o konkursie, w którym można wygrać pewną kwotę pieniędzy, postanowił wziąć w nim udział.

Treść ogłoszenia o konkursie:

„Karta Twój kumpel! Pokaż jak karta naszego banku towarzyszy Ci podczas codziennych czynności. Jeżeli Twoje zdjęcie będzie wystarczająco kreatywne, dostaniesz nagrodę w wysokości 50 PLN!"

Informacja o konkursie ucieszyła Bartosza tym bardziej, że był on organizowany przez bank, który wydał mu złotą kartę kredytową z limitem 1500 zł. Pracę konkursową zamieścił w wyznaczonym miejscu w portalu społecznościowym.

Po kilku dniach sprawdził stan swojego rachunku bankowego i wówczas okazało się, że owszem, wygrał konkurs, ale jednocześnie zobaczył, że jego kartą dokonano zakupów o łącznej kwocie 1500 zł.

Umieszczanie poufnych danych (takich jak np. dane karty kredytowej, szczególnie jeżeli widoczny jest numer karty i numer CVV/CVC) w Internecie może narazić nas na niebezpieczeństwo związane z działaniem przestępców.

Nigdy nie mamy pełnej kontroli nad tym, kto ma dostęp do naszych danych i co dalej z nimi robi, zwłaszcza jeżeli dane są trzymane w środowisku rozproszonym (np. w technologii przetwarzania w chmurze). Należy również pamiętać, że informacja raz umieszczona w Internecie, nawet po jej usunięciu, dalej tam pozostaje. W powszechnym użyciu są narzędzia, które pozwalają na sprawdzenie historycznej zawartości poszczególnych stron czy serwisów internetowych.

Dane podawane w systemach autoryzacyjnych instytucji płatniczych są zwykle bezpieczne, ale pod żadnym pozorem nie wolno tych danych przekazywać w e-mailu bądź w inny sposób umożliwiający ich pozyskanie przez osoby niepowołane.

Zapamiętaj!

Bank nie będzie wymagał podania danych służących logowaniu do bankowości internetowej (loginy, hasła, w tym jednorazowe hasła przesyłane SMS-em) czy to telefonicznie, czy za pomocą poczty elektronicznej, czy w jakikolwiek inny sposób – poza serwisem internetowym bankowości elektronicznej i udostępnianymi przez bank aplikacjami (np. mobilnymi aplikacjami instalowanymi na smartphonach).

Przykład 4

Pani Mariola, główna księgowa jednej z opolskich firm, zajmującej się produkcją stali, jechała z pracy do domu. Na służbowy telefon otrzymała SMS z przypomnieniem o zapłaceniu faktury za prąd.

Zwykle jej firma realizowała opłaty w ostatniej chwili. Pani Mariola postanowiła wykorzystać służbowy smartphone z aplikacją do bankowości mobilnej. Firma Pani Marioli, jeżeli chodzi o elektroniczny obieg dokumentów, była w dwudziestym pierwszym wieku, więc miała dostęp do wszystkich faktur z domu, za pomocą bezpiecznego łącza opartego na wirtualnych sieciach prywatnych (VPN). Po odnalezieniu stosownej faktury Pani Mariola rozpoczęła proces płatności. Zawsze tego typu przelewy robiła w pracy, przy użyciu firmowego stacjonarnego komputera, więc proces wpisywania danych do przelewu zajął jej trochę czasu.

Po akceptacji wykonania przelewu jak zawsze otrzymała SMS z hasłem jednorazowym, który dzięki skorzystaniu z aplikacji mobilnej mogła od razu skopiować, zamiast przepisywać.

Po kilku dniach otrzymała kolejny, ponaglający SMS od dostawcy energii. Wstępnie uznała to za pomyłkę systemu, który jeszcze prawidłowo nie zaksięgował wpłaty. Stwierdziła, że zajmie się tym po powrocie do pracy.

Po powrocie pierwszą rzeczą, jaką postanowiła się zająć, była weryfikacja zapłaty faktury za energię.

Na pierwszy rzut oka wszystko wyglądało jak należy, dopiero bardziej szczegółowa weryfikacja poprzedzona kontaktem ze sprzedawcą energii wykazała, że przelew został zrealizowany na inny rachunek.

W tym przykładzie trudno dokonać jednoznacznej oceny, w jaki sposób został przeprowadzony atak. Co pewien czas w mediach podawane są informacje o bardzo trudnych, a niekiedy niemożliwych do wykrycia atakach przestępców, w celu pozyskania danych indywidualnych klientów banków.

Obecnie coraz częściej przeprowadzane są ataki na urządzenia mobilne, dlatego też korzystanie z tego samego urządzenia w celu dokonywania płatności oraz ich uwierzytelniania jest ryzykowne. Idea dwuskładnikowego uwierzytelniania traci sens, ponieważ udany atak na jedno urządzenie oznacza przejęcie przez atakującego obydwu składników dwuskładnikowego procesu uwierzytelnienia.

Jednym z bezpieczniejszych rozwiązań może być posiadanie specjalnego urządzenia, najlepiej prostego telefonu z dedykowanym numerem (kartą SIM), służącego jedynie do autoryzacji transakcji. Wówczas transakcję inicjujemy w aplikacji mobilnej na smartphonie, a autoryzujemy na bezpiecznym urządzeniu, np. dedykowanym do tego telefonie. Wtedy idea dwuskładnikowego uwierzytelnienia jest w pełni spełniona, a ryzyko bycia ofiarą ataku na ten kanał jest zminimalizowane.

4. ATAKI UKIERUNKOWANE

Kilka lat temu pojawiła się zorganizowana akcja ukierunkowanych ataków phishingowych. Dotyczyła ona konkretnych grup odbiorców, np. kancelarii prawnych lub osób powiązanych z danym podmiotem. Na pierwszy rzut oka nie różniły się one niczym od standardowych ataków phishingowych.

Przykład 5

Treść wiadomości e-mail skierowanej do kancelarii prawnej:

„Szanowni Państwo

Zwracam się z pytaniem o przedstawienie cennika analizy dla naszego klienta biznesowego. Kluczową sprawą jest dla nas czas, analiza będzie niezbędną w trwającym postępowaniu i musi zostać przedłożona w terminie nie późniejszym niż 30 września (środa). Oczywiście gdyby takowa usługa spowodowała wzrost ceny zlecenia, jesteśmy na to przygotowani.

Nasz klient przekształcił formę prawną firmy, z tego powodu powstały problemy związane z zaległościami księgowymi oraz poprzednimi wierzycielami. Potrzebujemy możliwie jak najszybszej informacji zwrotnej, czy są w stanie Państwo podjąć się tego typu zlecenia.

Przedstawiam wszystkie niezbędne dokumenty dla poglądu sytuacji i proszę o odpowiedź.

http://xxx.xxx.xxx/?fname=xxx_dokumenty_podatnik_xxx.doc

Liczę, że jest to wystarczający rozpis dokumentów, który posłuży do wyceny.

Z poważaniem,

XXX
Adwokat prowadzący
Kancelaria XXX
xxx@xxx.xxx
NIP:XXX REGON: XXX
XXX"

W opisanym przykładzie kliknięcie w link prowadziło do strony wyglądającej jak wtyczka MS Office, której ładowanie kończyło się błędem. Na formatce informującej o błędzie pojawiła się prośba o aktualizację wtyczki, którą należy pobrać i zainstalować, klikając przycisk „Aktualizuj". Po kliknięciu pobierał się plik wykonywalny, później następował proces instalacji szkodliwego oprogramowania, który udawał proces instalatora prawdziwego programu. Atakujący przygotował również stronę rzekomej „kancelarii", która miała być nadawcą wiadomości. Strona jest klonem istniejącej strony internetowej prowadzącej legalną działalność kancelarii, a atakujący zmienił jedynie logo i dane kontaktowe. NIP i REGON były prawdziwe.

Przykład 6

Treść wiadomości e-mail:

„Od: XXX <xxx@xxx.xxx>
Data: 2016-09-09 13:22
Temat: Prośba o korektę w fakturze od XXX

Szanowni Państwo

Piszę do Państwa w sprawie XXX – na naszą firmową skrzynkę trafiają faktury wraz z Państwa adresem poczty elektronicznej i danymi firmowymi/osobowymi. Faktura jest już prawdopodobnie nieaktualna, jednakże z racji, iż zawsze staramy się utrzymywać należyty porządek w dokumentacji, proszę o weryfikację. Na fakturze znajdują się szczegółowe dane, za co była wystawiona i kto podpisał odbiór. Jeśli są poprawne, wystarczy wiadomość zwrotna z taką informacją, jeśli nie – proszę wskazać, gdzie leży problem, my się tym zajmiemy. Dokument jest ważny przy corocznych rozliczeniach podatkowych przez 5 lat, stąd też nasze zapytanie.
Faktura w formacie dokumentu dostępna tylko dla Państwa w naszej chmurze plików:
http://xxx.xxx.xxx/?fname=xxx_biuro_korekta.doc

Przepraszam za wszelkie kłopoty, liczę na Państwa odpowiedź.
Z poważaniem,
XXX
Asystent Działu Księgowego"

Stwierdzono, że w bardzo wielu przypadkach firmy, których faktury należało rzekomo skorygować, były wcześniej powiązane korespondencją z firmami będącymi celem ataku. Może to sugerować, że nie są one przypadkowe, a atak ten był poprzedzony innym, za pomocą którego wykradziono korespondencję lub listy kontaktowe firm, które posłużyły do uwiarygodnienia ataku.

To, co wyróżnia te ataki od innych, to ich dopracowanie i wyjątkowa (jak na ten typ ataku) troska o szczegóły. Atakujący poświęcił dużo czasu na ich przygotowanie, a sam atak był wieloetapowy.

Nawet jeżeli dopełnimy wszelakich starań co do bezpieczeństwa naszych danych, musimy mieć świadomość, że mogą one zostać wykorzystane przez przestępców.

W kolejnym przykładzie celem byli klienci banku, a atak miał na celu wykradzenie danych logowania do serwisu bankowości internetowej. Cała kampania wyglądała pozornie na zwykłą akcję phishingową.

Przykład 7

Treść wiadomości e-mail:

„Od: NazwaBanku <rozne@adresy.e-mail>
Data: 06.05.2016 15:59 (GMT+01:00)
Temat: Blokada rachunku NazwaBanku

Data: 06.05.2016 r.
Dostęp do Twojego konta NazwaBanku został zablokowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy konto w systemie NazwaBanku internet, powodem czego jest nieautoryzowany dostęp do konta. W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www. NazwaBanku.pl/weryfikacja
[link prowadził do: hxxp://xxx.xxx/?email=email@ofiary.pl]

Serdecznie pozdrawiamy,
Zespół NazwaBanku
W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinią XXX

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. NazwaBanku z siedzibą we XXX, ul. XXX, XX-XXX XXX, zarejestrowany w Sądzie Rejonowym dla XXX – XXX, XXX pod numerem KRS XXX, REGON XXX, NIP XXX, kapitał zakładowy i wpłacony XXX zł."

Atak przebiegał standardowo. Łącze, które wyglądało jakby miało prowadzić do adresu prawdziwej strony banku, w rzeczywistości przekierowywało do strony oszustów, która przechwytywała login i hasło do systemu bankowości elektronicznej.

Ta akcja przestępców okazała się wyjątkowo skuteczna, ponieważ przez zmianę w polityce banku do kradzieży pieniędzy wystarczyły jedynie login i hasło.

Warto uważnie czytać wszystkie powiadomienia wysyłane nam przez bank, cyklicznie sprawdzać limity, blokady na rachunkach oraz nie wolno otwierać łącza, które otrzymaliśmy w wiadomości e-mail!

5. JAK SIĘ CHRONIĆ PRZED ZAGROŻENIAMI PŁYNĄCYMI Z INTERNETU?

Podstawowe zasady, jak się chronić przed zagrożeniami płynącymi z Internetu, szczególnie w kontekście korzystania z bankowości internetowej, zostały przytoczone w rozdziale – Kampania KNF „Zadbaj o swoje bezpieczeństwo w sieci".

5.1. Ochrona przed szkodliwym oprogramowaniem

Istnieje kilka zasad, które powinniśmy stosować, aby zapobiec zainfekowaniu szkodliwym oprogramowaniem naszych komputerów i urządzeń mobilnych:

- używanie tylko legalnego oprogramowania pochodzącego z zaufanego źródła; w szczególności dotyczy to systemu operacyjnego i systemów zapobiegających szkodliwemu oprogramowaniu,
- nie otwieranie przesyłek poczty elektronicznej niewiadomego pochodzenia oraz załączonych do nich plików lub linków, szczególnie w przypadkach, gdyby wskazywały na okoliczności zdarzeń, które nie miały miejsca z naszym udziałem,
- używanie oprogramowania zabezpieczającego przed uruchomieniem szkodliwych aplikacji,
- regularne skanowanie komputera oraz urządzeń mobilnych,
- uważne czytanie informacji przekazywanych podczas instalacji oprogramowania oraz ich licencji (nieświadoma zgoda na przekazywanie informacji),
- wyłączenie obsługi makr i skryptów w aplikacjach biurowych przy korzystaniu z plików pochodzących z niezaufanego źródła,
- regularna aktualizacja oprogramowania,
- używanie dodatkowych mechanizmów zabezpieczeń, takich jak zapory ogniowe (firewall).

5.2. System operacyjny

System operacyjny to najważniejszy program w naszym komputerze i urządzeniu mobilnym. To od jego stanu zależy zarówno szybkość działania, jak i poziom bezpieczeństwa.

Jest kilka zasad, którymi należy się kierować podczas użytkowania systemu operacyjnego. Najważniejsze to:

1. Uprawnienia. Zaleca się, aby użytkownicy systemu nie korzystali na co dzień z konta z uprawnieniami administracyjnymi oraz ustawiali hasło na konta administracyjne. Takie postępowanie minimalizuje zakres szkód, jakie może wyrządzić atakujący w przypadku przejęcia konta z ograniczonymi uprawnieniami.
2. Domyślne repozytoria oprogramowania. Niektóre systemy operacyjne posiadają centralne repozytoria zawierające pakiety reprezentujące poszczególne programy, zbudowane i przygotowane przez twórców pod kątem konkretnego systemu. Takie centralne repozytoria oprogramowania stano-

wią zweryfikowane, bezpieczne źródło programów. Ogranicza to w znaczący sposób instalację programów z niezaufanych źródeł, które mogą zawierać szkodliwe oprogramowanie.

3. Aktualizacja. Bieżąca aktualizacja systemu operacyjnego to jedna z podstawowych zasad skutkująca zmniejszeniem ryzyka, że zostaniemy ofiarą przestępcy. Aktualizacje mają jeszcze jedną ważną zaletę – przedłużenie wsparcia producenta systemu o kolejny okres.

5.3. Wieloskładnikowe uwierzytelnienie

Jednym z najlepszych sposobów weryfikacji tożsamości klienta końcowego jest wieloskładnikowe uwierzytelnienie. Polega ono na rozszerzeniu standardowej weryfikacji opartej na nazwie użytkownika i haśle o dodatkowy „składnik". Najczęściej jest to hasło jednorazowe, które może być przesłane za pomocą SMS-a, możemy je odczytać z listy haseł jednorazowych lub z tokenu. Aktualnie najbardziej powszechne jest uwierzytelnienie dwuskładnikowe, które jest spotykane przy dostępie do danych i systemów o szczególnie wysokiej wartości. Wykorzystują je np. systemy bankowości elektronicznej przy autoryzacji przelewów. Należy pamiętać, że rozwiązanie to musi być wdrożone i wykorzystywane w odpowiedni sposób, jednakże nawet wówczas nie będzie chronić w stu procentach naszych komputerów przed działaniami przestępców.

Podstawową zasadą skutecznego wykorzystania wieloskładnikowego uwierzytelnienia jest odpowiednia separacja „składników" zestawionych w jego pełnym procesie lub odpowiednie oddzielenie kanałów, jakimi wspomniane składniki są przesyłane.

Przykład 8

Podczas zakładania rachunku inwestycyjnego Dom Maklerski przekazał klientowi specjalny formularz, na którym znajduje się login, hasło oraz lista haseł jednorazowych. W celu przeprowadzenia procesu uwierzytelnienia do systemu transakcyjnego klient musi podać login i hasło, które otrzymał podczas procesu zakładania rachunku, a każda transakcja jest potwierdzana przy pomocy hasła jednorazowego.

Teoretycznie mamy do czynienia z autoryzacją wieloskładnikową, ale utrata jednego formularza powoduje kompromitację całego rachunku i nie zabezpiecza w żaden sposób przed nieuprawnionymi zmianami na rachunku.

Taki sposób zabezpieczenia jest zdecydowanie lepszy, niż ograniczenie się do autoryzacji opartej na samym loginie i haśle, ale bezdyskusyjnie wymaga usprawnienia.

Godnym uwagi zjawiskiem jest rozpowszechnianie się idei wieloskładnikowego uwierzytelnienia na inne sfery naszej działalności w Internecie, nie tylko tej

związanej z systemami zawierającymi dane o szczególnie wysokiej wartości. Jest to możliwe dzięki rozwojowi technologii informatycznych i elektronicznych, a w szczególności technologii mobilnych.

Przykładem takiego pozytywnego rozpowszechnienia się wieloskładnikowego uwierzytelnienia są dodatki (wtyczki) do jednego z najpopularniejszych systemów do zarządzania treścią (CMS) Wordpress.

Jedną z „wtyczek", odpowiedzialnych za dwuskładnikowe uwierzytelnienie w systemie Wordpress, jest dodatek o nazwie Clef. Do uwierzytelniania dwuskładnikowego w tym dodatku używana jest aplikacja mobilna, przy pomocy której logujemy się do panelu administratora Wordpress. Działanie tej aplikacji jest bardzo efektywne.

Do uwierzytelnienia można wykorzystać również technologie Google za pomocą mechanizmu Two-Factor Authentication (Google Authenticator), który umożliwia zabezpieczenie logowania poprzez potwierdzenie e-mailowe, aplikację mobilną, skaner kodów QR, pytanie weryfikacyjne, a w wersji płatnej poprzez SMS lub rozmowę telefoniczną.

5.4. Przezorność

Jednym z największych obecnie zagrożeń jest phishing, dlatego też na tego typu zagrożenie trzeba zwracać szczególną uwagę. Jednym z popularniejszych mechanizmów wykorzystywanych przez przestępców jest wysyłanie na pocztę elektroniczną danego użytkownika wiadomości e-mail zawierającej link do strony internetowej, wyglądającej jak strona bankowości elektronicznej banku, ale będącej stroną służącą do wyłudzania poświadczeń.

W szczególności nie wolno klikać w łącza, które prowadzą do stron internetowych wymagających wpisania danych poufnych (np. prośba o weryfikację poświadczeń do konta).

6. JAK UCHRONIĆ SWOJE ŚRODKI PRZED ZAISTNIENIEM INCYDENTU BEZPIECZEŃSTWA?

6.1. Dywersyfikacja i segmentacja

W przypadku dokonywania płatności w miejscach niezaufanych oraz narażonych na ataki i kompromitację danych uwierzytelniających, w każdym przypadku prowadzenia działalności w Internecie, wskazane jest zadbanie o separację środków finansowych, dedykowanych prowadzonej działalności gospodarczej, od osobistych.

6.2. Karta internetowa

Jednym z najlepszych produktów do wykonywania płatności w Internecie jest „karta internetowa" (wirtualna), czyli elektroniczny instrument płatniczy, będący narzędziem służącym do zdalnego dostępu do środków (pieniędzy),

stworzonym do płatności w Internecie, której rachunek jest odseparowany od rachunku głównego czy oszczędnościowego. Ten instrument należy do kategorii przedpłaconych produktów finansowych (prepaid), czyli aby karta miała dostęp do środków, musi zostać najpierw zasilona. Karty wirtualne (internetowe) w przeciwieństwie do innych kart płatniczych nie muszą mieć postaci fizycznej.

Wspomniany instrument wykorzystuje się do transakcji, w których nie jest potrzebna jej fizyczna obecność, czyli przede wszystkim do transakcji typu e-commerce. Kartą internetową można płacić w sklepach internetowych oraz finalizować zamówienia złożone przez telefon (obecnie ten sposób zatwierdzania zakupu wygasa). Z drugiej strony nie zapłacimy nią w tradycyjnym sklepie ani nie pobierzemy pieniędzy w bankomacie.

Posiadacz ma wpływ na maksymalną kwotę transakcji bądź to przez ustalenie limitu, bądź przez załadowanie odpowiedniej kwoty na rachunek. Karta internetowa to rodzaj elektronicznej portmonetki.

Bardzo ważna w tym przypadku jest możliwość szybkiego, awaryjnego przelania środków na rachunek rozliczeniowy lub oszczędnościowy, np. z poziomu aplikacji mobilnej bez konieczności dodatkowego uwierzytelniania. Największą zaletą tego narzędzia jest to, że nawet w przypadku kompromitacji wszystkich danych kartowych nasze środki są bezpieczne, ponieważ domyślnie na rachunku karty nie trzymamy żadnych środków.

Dodatkowym atutem ww. karty jest kontrola wydatków. Nie tylko w kontekście ilości pieniędzy, jakie wydajemy na zakupy w Internecie lub dokonywanie bieżących opłat, ale również w celu uniknięcia dodatkowych kosztów, jakie możemy ponieść, szczególnie w przypadku płatności dokonywanych w innej walucie niż tej, w której prowadzimy rachunek.

6.3. Dodatkowy rachunek do płatności internetowych

W celu separacji naszych oszczędności możemy również założyć nowy dodatkowy rachunek służący tylko do płatności za zakupy lub płatności dokonywane w Internecie.

Najważniejsze to pamiętać, żeby rachunek, na którym trzymamy nasze oszczędności, nie był bezpośrednio wykorzystywany do realizacji płatności w Internecie. Najlepszym podejściem jest założenie, że nasze dane, które przekazujemy za pomocą sieci Internet wcześniej czy później mogą zostać wykorzystane w nieuprawniony sposób. Mając świadomość wystąpienia zagrożeń będziemy mogli w przyszłości ograniczyć ewentualne skutki ataku.

Rachunek, z którego dokonywana jest płatność nie powinien mieć możliwości wypłacenia środków ponad stan zasilenia (debet, kredyt odnawialny).

Dodatkowo bardzo ważne jest, aby z rachunku, który nie jest przeznaczony do dokonywania płatności w Internecie, nie można było dokonywać płatności w sieci. Realizacja takiego ograniczenia powinna być możliwa poprzez ustanowienie odpowiednich blokad lub zerowanie limitów na płatności internetowe.

6.4. Płatności ubezpieczone

Kolejnym sposobem na zabezpieczenie się przed stratami finansowymi powstałymi w wyniku ataków hakerskich jest korzystanie z usług, które są w jakiś sposób ubezpieczone przed ewentualnym oszustwem. Niektórzy oferenci płatności online lub pośrednicy posiadają program ochrony kupującego, dzięki któremu można odzyskać pieniądze w przypadku problemów z transakcją. Przykładowo w sytuacji nieotrzymania towaru, za który dokonaliśmy opłaty, możemy domagać się zwrotu całości zapłaconej kwoty. Korzystanie z tego typu programów czasami wiąże się z dodatkowymi kosztami (cena ubezpieczenia), ale warto je ponieść, jeżeli chcemy zminimalizować straty, które mogą wystąpić w przypadku nieotrzymania towaru bądź usługi.

6.5. Karty z „chargeback"

Przykład 9

Pan Janusz jest amatorem biegania, fanem dobrych i markowych butów sportowych. Pan Janusz jest również osobą oszczędną, która stara się nie przepłacać za kupowane towary oraz racjonalnie zarządzać swoimi finansami. Okazji zakupowych szuka na aukcjach i w sklepach internetowych. Po wielu dniach poszukiwań najnowszego modelu butów ulubionej marki w końcu trafił na ciekawą ofertę. Pan Janusz znalazł sklep, gdzie mógł dokonać zakupu w bardzo okazyjnej cenie – 30 procent wartości rynkowej. Kilka dni po dokonaniu zakupu otrzymał przesyłkę, która od razu wydawała mu się podejrzana. Była ona dosyć ciężka. Firmy często do swoich przesyłek dołączały dużą liczbę ulotek albo gadżetów. Niestety nie w tym przypadku. Po rozpakowaniu paczki Pan Janusz z przerażeniem stwierdził, że w środku jest czerwona cegła.

Każdy może zostać ofiarą takiego oszustwa. Zdarza się, że nawet znane sklepy z bardzo dobrą reputacją nie wywiązują się ze swoich zobowiązań.

Za jedną z najbezpieczniejszych form płatności w sklepach internetowych uznaje się płacenie kartą. W ten sposób, w razie problemów, możemy w swoim banku uruchomić procedurę tzw. „chargeback" (obciążenie zwrotne).

Dzięki „chargeback" organizacje specjalizujące się w zakresie rozwiązań płatniczych, jak VISA i Mastercard, zabezpieczają swoich klientów przed oszustwami. Po wszczęciu wspomnianej procedury to zwykle bank podejmuje działania mające na celu odzyskanie utraconych przez poszkodowanego pieniędzy z banku, w którym rachunek posiadają przestępcy. Procedura ta polega na złożeniu reklamacji u wydawcy karty, który ją rozpatruje, i jeżeli zostanie

rozpatrzona pomyślnie, to w ciągu kilkudziesięciu dni możemy dostać zwrot pieniędzy na konto.

Karty płatnicze z dodatkową gwarancją „chargeback" to jedna z najprostszych metod zabezpieczenia się przed nieuczciwymi sprzedawcami. Procedura ta jest alternatywą dla standardowych ścieżek reklamacyjnych. Ma ona zastosowanie nie tylko w przypadku nieuczciwych sprzedawców, ale może być też wykorzystana w wielu innych sytuacjach, takich jak:

- niewydanie pieniędzy przez bankomat,
- podejrzenie oszustwa kartowego,
- błędy autoryzacji,
- nieotrzymanie zakupionych dóbr lub usług.

To jest oczywiście przykładowa lista procedur reklamacyjnych, a u każdego wydawcy karty może wyglądać inaczej. Warto mieć świadomość istnienia takiej możliwości, szczególnie że istnieje bardzo duże prawdopodobieństwo, że jesteśmy już posiadaczami karty z funkcją „chargeback" lub możemy taką kartę zamówić w naszym banku. Warto dokładnie sprawdzić, dopytać o możliwości, warunki, jakie oferuje nam wydawca karty w materii możliwości składania reklamacji.

Jeśli jesteśmy niezadowoleni z rozstrzygnięcia reklamacji posiadacz karty płatniczej może wystąpić:

- z wnioskiem do Rzecznika Finansowego,
- ze skargą do KNF,
- do Bankowego Arbitrażu Konsumenckiego,
- do powiatowego (miejskiego) rzecznika konsumentów.

6.6. Co należy zrobić po incydencie bezpieczeństwa?

Mimo zachowania najwyższej staranności, ostrożności i stosowania wszystkich zasad bezpiecznego korzystania z usług finansowych, może zdarzyć się, że staniemy się ofiarami przestępstwa. Najważniejsze jest utrzymywanie ciągłej czujności i weryfikowanie na bieżąco wyciągów z rachunków i kart, a także analizowanie historii transakcji dokonanych na naszych rachunkach. Kiedy zauważymy transakcje, które nie były realizowane przez nas, po pierwsze należy zachować spokój. Przed poinformowaniem banku należy ponownie zweryfikować wszystkie przeprowadzone transakcje w celu upewnienia się, czy nie były one zrealizowane przez inne osoby upoważnione do naszego rachunku. Gdy tylko zauważymy, że nastąpiła nieoczekiwana utrata środków, należy w pierwszej kolejności zabezpieczyć środki pozostałe na rachunku bankowym

poprzez zablokowanie kart i rachunków, które mogłyby zostać wykorzystane w sposób nielegalny.

W następnej kolejności należy poinformować naszego dostawcę usług finansowych (bank, pośrednik w płatnościach). Jednym z najszybszych sposobów poinformowania banku o podejrzeniu popełnienia przestępstwa jest złożenie reklamacji przez telefon, podczas której musimy wskazać transakcje niezrealizowane przez nas i oświadczyć, że nikomu nie udostępnialiśmy swojej karty i jej numeru, jak również nie przekazaliśmy innym osobom naszych loginów i haseł do bankowości elektronicznej. W trakcie przyjmowania reklamacji pracownik banku może zastrzec naszą kartę bądź zablokować dostęp do bankowości elektronicznej, a bank rozpocznie procedurę wyjaśniania naszego zgłoszenia.

Istotne jest przekazanie jak największej liczby, jak najbardziej szczegółowych informacji dotyczących zaistniałego incydentu. Następnym bardzo ważnym krokiem jest złożenie doniesienia na policji o popełnieniu przestępstwa.

Można tego dokonać na dwa sposoby: udać się na najbliższą nam komendę policji i złożyć zawiadomienie, z którego sporządzony zostanie protokół lub złożyć zawiadomienie w formie pisemnej, przesyłając je do prokuratury rejonowej właściwej ze względu na nasze miejsce zamieszkania. Jeżeli udamy się osobiście na komendę, zostaniemy wówczas przesłuchani w charakterze pokrzywdzonego, dlatego też należy mieć ze sobą wyciąg z karty bądź wydruk z historii rachunku, aby udokumentować naszą stratę. W przypadku zgłoszenia podejrzenia przestępstwa w pierwszej kolejności do prokuratury i tak będziemy zobowiązani do złożenia zeznań w charakterze pokrzywdzonego na komendzie policji. Prokuratura jest zobowiązana do przekazania naszego zawiadomienia do właściwej komendy policji. Dlatego najmniej kłopotliwym i najszybszym sposobem jest stawienie się osobiście w najbliższej jednostce policji.

Prewencyjnie dobrze jest poinformować właścicieli sklepów lub innych placówek, w których użyto naszej karty. Duże firmy zwykle posiadają procedury postępowania w przypadku nieuprawnionego użycia karty i mogą pomóc w działaniach mających na celu odzyskanie utraconych środków lub złapanie przestępców. Zarówno bank, jak i organy ścigania, mają prawo zwrócić się do danej firmy z zapytaniem w przedmiotowej sprawie.

Należy pamiętać, że liczy się czas!

IV. CZĘŚĆ ROZSZERZONA

1. DZIAŁALNOŚĆ KNF

"Rekomendacje oraz wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego"

Podstawowym elementem działań systemowych podejmowanych przez KNF jest szereg inicjatyw regulacyjnych, gdzie w kontekście cyberbezpieczeństwa sektora finansowego należy wskazać na wydane przez KNF rekomendacje i wytyczne:

- „Rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach”[6] (dalej: Rekomendacja D),
- „Rekomendację D-SKOK dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych”[7],
- „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych”,
- „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji”,
- „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego”,
- „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych”,
- „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych”,

[6] Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach zastąpiła poprzedzającą ją Rekomendację D dotyczącą zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki wydaną przez Komisję Nadzoru Bankowego w formie uchwały z dnia 11 grudnia 2002 r., której stosowanie zostało wydłużone do dnia 31 grudnia 2014 r. na podstawie § 2 pkt 2 uchwały Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz. Urz. KNF z 2013 r., poz. 5).

[7] Zgodnie z uchwałą Nr 615/2016 z 30 sierpnia 2016 r., Komisja Nadzoru Finansowego oczekuje, że Rekomendacja D-SKOK, zostanie wprowadzona do dnia 31 grudnia 2018 r.

- „Rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe".

Rekomendacja D, dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, stanowi załącznik do uchwały Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz. Urz. KNF z 2013 r., poz. 5).

Rekomendacja D ma na celu wskazanie bankom oczekiwań nadzorczych, dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami. Ryzyko to można określić jako niepewność związaną z prawidłowym, efektywnym i bezpiecznym wspieraniem działalności banku przez jego środowisko teleinformatyczne. Wiąże się ono przede wszystkim z ryzykiem operacyjnym (dlatego też niniejsza Rekomendacja powinna być traktowana jako uzupełnienie „Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach" w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego), ale również m.in. z ryzykiem utraty reputacji i ryzykiem strategicznym. Rekomendację stosuje się również odpowiednio wobec oddziałów instytucji kredytowych.

Rekomendacja D zawiera 22 rekomendacje, które podzielone zostały na następujące obszary:

- strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
- rozwój środowiska teleinformatycznego,
- utrzymanie i eksploatacja środowiska teleinformatycznego,
- zarządzanie bezpieczeństwem środowiska teleinformatycznego.

Rekomendacja jest skierowana do wszystkich banków, biorąc jednak pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego, różnice w zakresie uwarunkowań, skali działalności oraz profili ryzyka banków, sposób realizacji tych rekomendacji i wskazanych w nich celów może być odmienny.

W przypadku banków spółdzielczych oczekiwaniem nadzoru jest, by banki zrzeszające wspierały proces wdrażania niniejszej Rekomendacji z uwzględnieniem skali i specyfiki działalności danego banku spółdzielczego, stosując zasadę proporcjonalności. Skala działalności i wykorzystywane technologie informatyczne powinny decydować o zakresie i stopniu przyjmowanych rozwiązań. Proces

wdrażania tych rozwiązań w bankach spółdzielczych, pomimo aktywnej roli banku zrzeszającego, nie może jednak stać w sprzeczności ze zdefiniowanym w poszczególnych rekomendacjach zakresem obowiązków i odpowiedzialnością statutowych organów zrzeszonych banków spółdzielczych.

Wspomniane wcześniej „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego" są odpowiednikami Rekomendacji D dla innych sektorów rynku finansowego.

W dniu 5 października 2016 r. weszła w życie uchwała Nr 615/2016 Komisji Nadzoru Finansowego z dnia 30 sierpnia 2016 r. w sprawie wydania Rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych (Dz. Urz. KNF z 2016 r., poz. 31).

Istotne w Rekomendacji D-SKOK jest to, że wyróżnia ona kasy najmniejsze, które nie muszą stosować wszystkich jej zapisów. Podział ten oparty jest na dwóch jednoznacznych kryteriach: sumy bilansowej oraz liczbie członków.

W dniu 17 listopada 2015 r. weszła w życie uchwała Nr 584/2015 Komisji Nadzoru Finansowego z dnia 17 listopada 2015 r. w sprawie wydania Rekomendacji dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe (Dz. Urz. KNF z 2015 r., poz. 56), stanowiącej załącznik do ww. uchwały. Na mocy uchwały wspomniana Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie z zastrzeżeniem wyjątków, jest stosowana począwszy od dnia następującego po dniu opublikowania jej w Dzienniku Urzędowym KNF, tj. od dnia 5 grudnia 2015 r.

Rekomendacja ta ma na celu ujednolicenie zakresu minimalnych wymogów dotyczących zapewnienia bezpieczeństwa płatności internetowych w związku ze świadczeniem usług płatniczych oferowanych przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe (dalej: dostawcy usług płatniczych) przez Internet.

Dokument zawiera 14 rekomendacji, które podzielone zostały na następujące obszary:

1) Zasady i organizacja procesu zarządzania i oceny ryzyka.

Dostawcy usług płatniczych powinni posiadać formalną politykę bezpieczeństwa i regularnie dokonywać szczegółowych ocen ryzyka w stosunku do płatności internetowych oraz usług powiązanych, a w razie potrzeby dokonywać niezbędnych zmian. Analizy powinny uwzględnić m.in. wykorzystywane rozwiązania technologiczne, środowisko techniczne, w jakim działa klient czy zagadnienia outsourcingu.

2) Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych.

Dostawcy usług płatniczych powinni stosować mechanizm silnego uwierzytelniania klienta zawsze, gdy klient inicjuje płatność internetową lub chce uzyskać dostęp do wrażliwych danych płatniczych. Od tej zasady można odstąpić tylko w wyjątkowych przypadkach. Dostawcy powinni udostępniać klientom bezpieczne narzędzia do autoryzacji transakcji internetowych oraz zapewnić ogólną dbałość o bezpieczeństwo całej transakcji, poprzez jasne określenie obowiązków i zakresu odpowiedzialności odpowiednio dostawcy usług płatniczych i klienta w związku z korzystaniem z usług płatności internetowych, wynikających m.in. z zakazu udostępniania (ujawniania) podmiotom trzecim danych do logowania. Dostawcy powinni również stosować systemy, które pomogą zidentyfikować i zablokować oszukańcze transakcje.

3) Świadomość i edukowanie klientów oraz komunikacja z nimi.

Działania edukacyjne powinny się odbywać zarówno poprzez regularne akcje, jak i poprzez incydentalne ostrzeganie o zagrożeniach oraz bieżący kontakt z klientem za pomocą bezpiecznego kanału komunikacji.

Rekomendacja wskazuje na konieczność zasadniczego ograniczenia ryzyka wykorzystywania rachunków płatniczych do operacji fraudowych na podstawie skradzionych tożsamości klientów, wynikającego z obecnie możliwej praktyki otwierania kolejnych rachunków w instytucjach z wykorzystaniem przelewu jako sposobu potwierdzania tożsamości. Wprowadzenie w szczegółowej Rekomendacji 6.1. (zdanie 2) wymogu, zgodnie z którym rachunek założony zdalnie z wykorzystaniem przelewu potwierdzającego tożsamość klienta nie może służyć do otwarcia tym sposobem kolejnego rachunku płatniczego u innego dostawcy usług płatniczych, nie wpłynie na model funkcjonowania instytucji płatniczych prowadzących rachunki z natury swojej nie dające możliwości dokonywania przelewów, w celu otwarcia kolejnego rachunku. Ustalenie i przyjęcie skutecznych metod stosowanych w tym celu, pozostawione jest instytucjom otwierającym rachunki. Z tego względu Rekomendacja ma charakter szczególny w stosunku do tych regulacji i w przypadku ewentualnych rozbieżności powinna mieć pierwszeństwo w zastosowaniu.

2. TYPY ZAGROŻEŃ

2.1. Malware

Malware to ogólna nazwa każdego typu szkodliwego oprogramowania. Pod pojęciem malware znajdziemy wirusy, robaki, trojany, backdoory itp. Niektóre z nich, bardziej aktywne w ostatnim czasie, zostały opisane na dalszych stronach tego rozdziału. Ze względu na powszechność tego zjawiska, słowem będącym synonimem szkodliwego oprogramowania był wirus. Od pewnego czasu w związku z rozwojem technologii, a przede wszystkim sieci Internet, pojawiło

się bardzo dużo nowych zagrożeń, których nie można już było nazwać wirusami. W związku z tym coraz bardziej popularne stało się słowo jednoznacznie definiujące złośliwe oprogramowanie na wystarczającym poziomie ogólności. Dodatkowym powodem popularyzacji słowa „malware" była zmienność nowo powstającego szkodliwego oprogramowania, uniemożliwiająca jednoznaczny sposób przypisania do istniejących znanych kategorii. Wirusy zaczęły mieć cechy robaków, robaki trojanów albo łączyć w sobie cechy kilku typów szkodliwego oprogramowania, zupełnie wymykając się z podstawowej kategoryzacji.

2.2. Wirusy

Jak wspomniano wyżej, dotychczas słowo „wirus" było synonimem szkodliwego oprogramowania, ale wraz z rozwojem sieci Internet wirusy stały się jednym z wielu typów zagrożeń obecnych w środowiskach teleinformatycznych. W czasach kiedy głównym sposobem przekazywania informacji między komputerami były napędy miękkie, wirusy stanowiły główne zagrożenie dla komputerów. Niektóre potrafiły być tak destrukcyjne, że niszczyły fizycznie napędy stałe (dyski twarde). Obecnie wirusy straciły na znaczeniu, ale ich roli nie można bagatelizować.

Obecnie jednym z powszechniejszych sposobów pozyskiwania informacji z komputerów jest wykorzystywanie szkodliwego oprogramowania typu spyware (opisane w punkcie 2.10. rozdziału IV).

2.3. Robaki

Są bardzo podobne do wirusów z tą różnicą, że „rozmnażają" się za pomocą sieci teleinformatycznej i nie potrzebują programu gospodarza (zwykle pliku wykonywalnego). Najczęściej dystrybuowane są za pomocą poczty elektronicznej.

2.4. Exploity

Exploity są bardzo groźnym narzędziem w rękach przestępców. Exploit to kod umożliwiający bezpośrednie włamanie do komputera ofiary, które może zakończyć się przejęciem kontroli nad zaatakowanym komputerem. Działanie exploita wykorzystuje lukę w zainstalowanym oprogramowaniu. Bardzo często celem ataków są strony internetowe, napisane w językach skryptowych oraz aplikacje użytkowe. Należy wspomnieć o jednym z najbardziej znanych exploitów na Androida, czyli Stagefright. Błąd systemu umożliwiał zdalne wykonanie kodu na zaatakowanym urządzeniu za pomocą specjalnie przygotowanej wiadomości. Dzięki bardzo prostemu mechanizmowi ataku (za pomocą MMS) wystarczyło znać numer telefonu ofiary. Dobrze przygotowany przez przestępców atak na dany system mógł pozostać niezauważony przez jego użytkownika. Według skrajnych szacunków zagrożonych było 1 400 000 000 (jeden miliard czterysta milionów) urządzeń![8]

[8] Źródło: http://searchsecurity.techtarget.com/news/4500254709/Android-Stagefright-20-affects-all-14-billion-Android-devices [dostęp 12.02.2018 r.]

2.5. SQL/URL Injections

Najczęściej spotykana pod nazwą SQL Injection, rzadziej URL Injection, podatność aplikacji wykorzystująca niewystarczający lub błędny sposób filtrowania zapytań do bazy danych.

Działa ona na zasadzie „wstrzyknięcia" dodatkowego fragmentu do zapytania SQL wysyłanego do bazy danych przez kod aplikacji.

Przykład 10

Fragment pseudokodu z zapytaniem SQL programu obsługującego formularz logowania: `sql_query(„SELECT * FROM użytkownicy WHERE użytkownik = ,zmienna_użytkownik'")`

Poprawne zapytanie będzie wyglądało np. tak:

```
SELECT * FROM użytkownicy WHERE użytkownik = ,Nowak'
```

Natomiast przy braku odpowiednich zabezpieczeń atakujący może w pole użytkownik wpisać np. „Nowak' or ,1'='1" i wtedy zapytanie do bazy będzie wyglądało tak:

```
SELECT * FROM użytkownicy WHERE użytkownik = ,Nowak' or ,1' = ,1'
```

Wtedy program pobierze wszystkie rekordy z bazy danych, a nie tylko jeden.

2.6. Dialery

Dialery to programy łączące się z siecią za pomocą modemu przez wysoko płatne numery dostępowe. Wraz z odejściem modemów dialery przestały stanowić realne zagrożenie dla portfeli użytkowników połączeń wdzwanianych.

2.7. Trojany

Trojany to programy, które ukrywają się w zasobach komputera i wykonują w tle operacje na żądanie atakującego np. uruchamiają inną złośliwą aplikację. Do trojanów zalicza się rootkity, backdoory, spyware oraz wabbity, forki i bomby logiczne. Trojany stanowią dużą grupę zagrożeń.

2.8. Rootkity

Rootkity to niebezpieczne, ukryte programy i procesy, które umożliwiają hakerom przejęcie kontroli nad systemem operacyjnym urządzenia (komputer, telefon) ofiary i pozwalają na ukrycie innego potencjalnie niebezpiecznego oprogramowania. Maskują one niebezpieczne pliki i procesy, które zwykle mają za zadanie kontrolowanie systemu operacyjnego urządzenia, np. komputera, telefonu. Systemy antywirusowe raczej nie mają problemów z wykryciem rootkitów do momentu ich uruchomienia. Wykrycie rootkita w już zarażonym systemie jest natomiast bardzo trudne. Jedną z najczęstszych technik wykrywania rootkitów jest technika porównania krzyżowego, polegająca na zestawieniu listy plików zwróconej przez API systemu z odczytaną bezpośrednio z systemu

plików. Rootkity mogą aktywnie wpływać na procesy wykrywania i dlatego między innymi są one bardzo groźnym narzędziem w rękach przestępców.

2.9. Backdoory

Backdoory to rozmyślnie utworzone luki w zabezpieczeniach systemu, służące do późniejszego wykorzystania przez atakującego w przypadku wykrycia i załatania podatności użytej w pierwotnym ataku.

2.10. Spyware

Wraz z rozwojem społeczeństwa informatycznego w sieci Internet, zaczęły pojawiać się nowe zagrożenia oraz ataki ukierunkowane na kradzież danych. Celem oprogramowania spyware jest gromadzenie informacji o użytkowniku oraz przesyłanie ich innym osobom bez zgody i wiedzy osoby inwigilowanej. W momencie rozwoju bankowości elektronicznej dane dla przestępców zaczęły nabierać coraz większej, materialnej wartości.

2.11. Wabbity, Forki i Bomby logiczne

Wabbity i Forki to grupa programów, które mają za zadanie wykonanie określonej operacji mającej na celu wyczerpanie zasobów komputera.

Wabbit w tym celu wykonuje jedną określoną operację, np. kopiowanie folderu, a Fork duplikuje procesy w systemie operacyjnym.

Bomba logiczna natomiast wykonuje określone zadanie (zmiana hasła, kasowanie danych itp.), kiedy zajdą pewne okoliczności (np. określona data, liczba uruchomień), konieczne do aktywacji procesu.

2.12. Keyloggery

Keyloggery to urządzenia lub programy mające na celu przechwytywanie znaków wpisywanych na klawiaturze oraz przekazywanie ich atakującemu. W ten sposób mogą wyciec ważne dane, jak hasła, kody jednorazowe, poufne oraz prywatne dane. Keyloggery, będące fizycznymi urządzeniami, są praktycznie niewykrywalne przez programistyczne narzędzia do wykrywania zagrożeń.

2.13. Stealware

Ogólne określenie oprogramowania ukierunkowanego na okradanie nieświadomego użytkownika. Zwykle jego działanie opiera się na podmienianiu numerów kont w przypadku wykrycia próby wykonania przelewu za pośrednictwem bankowości internetowej.

2.14. Ransomware

Kolejnym zagrożeniem, które zyskuje na popularności, jest rozpowszechnianie aplikacji służących do wyłudzania okupu, czyli ransomware. Taka aplikacja po uruchomieniu szyfruje zawartość dysku twardego oraz innych nośników obecnych w komputerze. Historia ransomware sięga 1989 roku. Wówczas złośliwe

oprogramowanie trzeba było rozdystrybuować fizycznie wysyłając dyskietki, a „okup" należało przesłać na skrytkę pocztową. Aktualnie zarówno dystrybucja ransomware, jak i zbieranie okupu stało się o wiele prostsze i przez to rozprzestrzeniło się na wielką skalę.

Jednym ze sposobów ochrony przed ransomware jest cykliczne robienie kopii zapasowych. Konieczności ich tworzenia nie trzeba nikomu tłumaczyć. Ochrona przed zagrożeniami, jakie niesie ze sobą ransomware (zaszyfrowanie dysku), stanowi dodatkową korzyść.

Należy pamiętać o dwóch głównych wymaganiach dotyczących przygotowania kopii zapasowej. Kopia powinna być zapisana na zewnętrznym nośniku oraz odpowiednio odseparowana od reszty zasobów. Chodzi o to, że szkodliwe oprogramowanie często szyfruje wszystkie dostępne zasoby. Mogą to być zarówno fizycznie znajdujące się w komputerze dyski twarde, jak i zasoby sieciowe. Zdarzało się, że atak na jeden komputer spowodował paraliż całej firmy, ponieważ zaatakowany komputer miał dostęp do wszystkich zasobów sieciowych firmy.

2.15. Botnet

To grupa komputerów zainfekowanych złośliwym oprogramowaniem stanowiącym „armię" dla osoby lub osób ją kontrolujących.

„W skali świata ok. 2 mln komputerów pracowało w sieciach botnet. Polska znalazła się na 10. miejscu wśród krajów o największym współczynniku zagrożenia z 2,8% komputerów pracujących w sieciach botnet (…)"[9].

Komputery będące częścią botnetu mogą nie wykazywać żadnych zachowań sugerujących obecność szkodliwego oprogramowania aż do czasu aktywacji. Wtedy komputery zamieniają się w narzędzia, które wykonują polecenia przesyłane przez przestępców. Takie komputery są wykorzystywane najczęściej do rozsyłania spamu, czyli niechcianych, szkodliwych wiadomości e-mailowych oraz do ataków rozproszonej odmowy usługi (DDoS), mającej na celu zablokowanie możliwości realizacji usługi przez podmiot atakowany. Choć ataki DDoS z wykorzystaniem botnetu są bardzo groźne, to duże podmioty, które posiadają odpowiednie urządzenia oraz umowy z dostawcami usług sieciowych radzą sobie z nimi coraz lepiej. W gorszej sytuacji mogą znajdować się mniejsze podmioty. W ich przypadku atak DDoS może stanowić duży problem. Powszechne zjawisko otrzymywania niechcianych wiadomości, określanych mianem spam, na pocztę elektroniczną, może niekiedy być wykorzystywane przez przestępców w celu dokonania phishingu, czyli pozyskania danych użytkownika.

[9] „Założenia Strategii Cyberbezpieczeństwa Dla Rzeczypospolitej Polskiej", Zespół zadaniowy Ministerstwa Cyfryzacji, 2016 r. https://www.gov.pl/documents/31305/0/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf/7005e3e7-c9d0-2840-bc7a-3261e573627e [dostęp 12.02.2018 r.]

2.16. Cross-Site-Scripting – XSS

Ataki XSS to wycelowane w klientów korzystających z podatnej aplikacji webowej „wstrzyknięcie" wykonywanego po stronie przeglądarki fragmentu skryptu (może to być np. JavaScript).

Na pierwszy rzut oka ta podatność nie wydaje się groźna, ale może być bardzo sprytnie wykorzystana do kilku rzeczy, takich jak wykradanie zapisywanych na komputerze użytkownika plików, potocznie określanych mianem „ciastek", co może umożliwić przestępcom przejęcie sesji użytkownika (również danych logowania), a także podmienienie strony użytkowanej w danym momencie.

2.17. Phishing

Jest to obecnie jedno z najpoważniejszych zagrożeń klientów bankowości internetowej usług sektora finansowego. Phishing to przestępcza metoda oszustwa, dystrybuowana przy użyciu poczty elektronicznej, w której klient jest najczęściej wprowadzany w błąd za pomocą informacji fałszywej, sugerującej, że pochodzi z instytucji finansowej (np. banku) oraz odpowiednio spreparowanej strony internetowej, udającej stronę usługodawcy finansowego. Klient, logując się na fałszywej stronie, przekazuje dane swojego logowania przestępcom, którzy później mogą za ich pomocą dokonywać kradzieży lub transakcji oszukańczych (fraudowych). Obecnie coraz powszechniejszym zjawiskiem jest rozsyłanie przez przestępców wiadomości e-mail, które łudząco przypominają wiadomości pochodzące z banków. Bardzo często w tego rodzaju wiadomościach podane są dokładne dane banku oraz link do jego strony internetowej, pod którym w rzeczywistości ukryta jest fałszywa strona internetowa, za pośrednictwem której przestępcy mogą pozyskiwać wrażliwe dane klientów.

Wraz z rozwojem wiadomości przesyłanych w ramach ataku phishingowego, modyfikacjom i ulepszeniom podlegają mechanizmy ukrywania ataku, takie jak „zielona kłódka" przy oszukańczym adresie internetowym, czy podmiana wpisów DNS dla uwiarygodnienia adresu aplikacji przechwytującej dane.

Wykorzystywany w takich atakach program instaluje skrypt, który zmienia konfigurację serwera pośredniczącego (proxy) i w przypadku adresów bankowości internetowej wskazuje na serwery przestępców. W zainfekowanym systemie program instaluje również dodatkowy certyfikat nadrzędnego urzędu certyfikacji i dzięki temu fałszywa strona banku może pokazywać „zieloną kłódkę", będącą symbolem zaufanego połączenia zgodnego z wyświetlaną nazwą domeny.

Najprostszym sposobem wykrycia takiego ataku jest przeanalizowanie informacji zawartych w certyfikacie oraz sprawdzenie, czy nie nastąpiły zmiany w ustawieniach serwera pośredniczącego komputera.

Szczegółowy opis, jak wykryć i usunąć podobny atak, pojawił się w komunikacie Związku Banków Polskich z dnia 10 czerwca 2016 r.[10]

[10] http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci [dostęp 12.02.2018 r.]

2.18. Socjotechnika

Jednym z powszechniejszych mechanizmów wykorzystywanych przez przestępców, a wykraczających poza obszar działań technicznych, jest stosowanie socjotechniki – zarówno w przypadku osób indywidualnych, jak i pracowników firm.

Obecnie techniki manipulacyjne najczęściej stosowane są w omawianych wcześniej atakach phishingowych.

Należy również pamiętać, że pomimo przestrzegania zasad bezpieczeństwa w bankowości elektronicznej akcje przestępców mogą zakończyć się powodzeniem.

Dobrze przeprowadzony atak socjotechniczny może być bardzo groźny i niemożliwe jest niekiedy uchronienie się przed nim, nawet mimo posiadania odpowiedniego systemu zabezpieczeń.

Nie oznacza to jednak, że nie można znacząco zmniejszyć ryzyka skutecznego ataku socjotechnicznego na nas samych oraz naszych pracowników.

Są dwie proste i skuteczne metody przeciwdziałania takim zagrożeniom:

1. Szkolenia pracowników – szkolenia te muszą być bardzo dobrze przygotowane pod względem merytorycznym, ze szczególnym uwzględnieniem zagrożeń występujących w danym sektorze. Omawiane podczas nich zagadnienia powinny być zobrazowane odpowiednio dobranymi przykładami.
2. Cykliczne przeprowadzanie kontrolowanych kampanii socjotechnicznych skierowanych do podległych pracowników – najważniejsze jest, aby wszyscy pracownicy byli świadomi, że firma przeprowadza takie kampanie oraz robi to cyklicznie. Dzięki temu pracownicy nie będą obawiać się zgłaszania zauważonych nieprawidłowości i incydentów bezpieczeństwa, co umożliwi zwiększenie skuteczności oddziaływania szkoleń.

2.19. Powrót DoS – ataki na warstwę aplikacyjną

W ostatnim czasie można zauważyć niepokojący powrót do ataków DoS ukierunkowanych na warstwę aplikacyjną.

Ataki oparte na powolnym odsyłaniu nagłówków żądań HTTP („Slow http DoS") znane są od około 10 lat. Ze względu na swoją specyfikę przewiduje się, że tego typu zagrożenia będą aktualne jeszcze przez kilka następnych lat. Atak tego typu może zostać przeprowadzony skutecznie w prosty sposób przy pomocy jednego węzła (komputera), więc pod tym względem stanowi duże zagrożenie.

Aplikacje webowe nieustannie są modyfikowane i ulepszane, m.in. w zakresie ich funkcjonalności. Ponadto aplikacje te stają się coraz bardziej skomplikowane i korzystają z coraz to większej ilości warstw pośredniczących i towarzyszących (aplikacje, moduły podmiotów trzecich).

Nowe światło na ataki DoS warstwy aplikacji rzucił Robert „RSnake" Hansen przy pomocy skryptu Slowloris. Przedstawił on inne podejście do ataku. W typowym ataku wysyłanych jest kilka tysięcy żądań HTTP GET, które nie obciążają zbytnio łącza. Slowloris wykorzystuje koncepcje protokołu HTTP oraz sposób obsługi żądań serwera WWW, za pomocą których jest w stanie skutecznie sparaliżować działanie usługi w ciągu kilku sekund.

Skrypt generuje dużą liczbę gniazd (sockets), a następnie w specyficzny („powolny") sposób wysyła dane częściowych żądań HTTP, co w efekcie skutkuje wyczerpaniem puli wolnych wątków obsługujących żądania HTTP serwera. Utrzymywanie kilkuset równoczesnych połączeń z atakowanym serwerem powoduje, że po krótkim czasie całe zasoby serwera WWW skierowane są na obsługę atakującego. Zwiększa to nie tylko obciążenie systemu, ale przede wszystkim blokuje możliwość podłączenia się do serwera innym klientom. Atak w pewnych okolicznościach może nie zostawić po sobie śladów w logach.

Nieodpowiednia konstrukcja aplikacji, niewystarczająca obsługa błędów, niestaranność, błędy programistyczne lub niewystarczające przetestowanie aplikacji i obsługa wyjątków też może zwiększyć podatność na ataki ze strony przestępców.

Przykład 11

Mirosław jest młodym człowiekiem, któremu rodzice właśnie założyli pierwszy rachunek w banku. Mirek jest bardzo ciekawy nowoczesnych technologii i dlatego z wielką ekscytacją zabrał się za sprawdzenie możliwości systemu bankowości elektronicznej. Choć nie miał na koncie żadnych środków, a historia rachunku była zupełnie pusta, postanowił sprawdzić dostępne funkcjonalności we wszystkich możliwych wariantach. Mirek nie zdawał sobie sprawy, że zaczął zdobywać pierwsze szlify w swoim przyszłym zawodzie, czyli testera oprogramowania.

Zainteresowały go szczególnie możliwości eksportu danych do plików. Ciekawiły go formaty, kolumny, zakresy i możliwości obróbki danych w zewnętrznych programach. Ze względu na małą ilość danych, jakie zasilały jego konto, możliwości poznawania sposobów obróbki danych były ograniczone.

Po ostudzeniu początkowej fascynacji, Mirek postanowił wpisać przy eksporcie historii rachunku do pliku PDF wartość „-1" w polu generacji ilości stron. Podczas wykonywania tej operacji na pewien czas wyłączono prąd. Po jego przywróceniu okazało się, że Mirek nie może ponownie zalogować się do panelu bankowości elektronicznej.

Aplikacja, która nie została poddana kompleksowym testom, w tym testom penetracyjnym, stanowi źródło wielu potencjalnych podatności na zagrożenia i może okazać się, że zwykła pomyłka użytkownika spowoduje zawieszenie ważnego systemu.

W świecie rzeczywistym nie istnieją aplikacje, które nie zawierałyby błędów w pierwszej iteracji tworzenia. Pierwsze nieprawidłowości są wychwytywane już podczas tworzenia oprogramowania. Może okazać się jednak, że na tym etapie niemożliwe było zauważenie i naprawienie wszystkich błędów.

Szczególnie dużą uwagę należy poświęcić najnowszym i jeszcze nie do końca poznanym technologiom.

Przykładem takiej technologii, zdobywającej obecnie coraz większą popularność, jest Node.js. Serwer Node.js nie zawiera żadnej domyślnej konfiguracji. Kod jest wykonywany „ad hoc" po uruchomieniu aplikacji. Konsekwencją takiej budowy jest brak domyślnej obsługi błędów. Generuje to podatność wyłączenia serwera w przypadku wywołania nieobsłużonego błędu. Jego wygenerowanie w skrajnych przypadkach może być bardzo prozaiczne, np. poprzez wpisanie wartości tekstowej w pole, które może przyjąć wartość tylko liczbową. Celowe wywoływanie takich błędów może się zakończyć skutecznym atakiem DoS.

Częściowo problem braku domyślnej konfiguracji mitygują coraz częściej pojawiające się frameworki dla Node.js. Celowe wywoływanie takich błędów może powodować skuteczny atak DoS.

3. WIELOWARSTWOWA MITYGACJA ZAGROŻEŃ

Ze względu na duże ryzyko wystąpienia zagrożenia przechwycenia danych użytkownika należy pamiętać, że nie można już polegać na ochronie jednopoziomowej opartej na jednym narzędziu czy sposobie mitygacji zagrożeń.

W przypadku użytkowników domowych oprogramowanie antywirusowe przestało być skutecznym środkiem zapobiegającym działaniu szkodliwego oprogramowania w komputerach. Jednym z powodów tego stanu rzeczy jest niewystarczająca skuteczność tego typu oprogramowania, często opartego na nieaktualnych bazach sygnatur. W świecie obecnych zagrożeń za nieaktualną można uznać już bazę starszą niż kilka godzin. Drugim powodem jest to, że wirusy przestały być głównym zagrożeniem. Podatności oparte na błędach w logice biznesowej oraz niezałatane luki w oprogramowaniu (0 day) mogą poczynić o wiele większe szkody niż wirusy, a do tego są bardzo trudno wykrywalne.

Oprócz programu antywirusowego, zainstalowanego na komputerze stacjonarnym, powinno znaleźć się na nim oprogramowanie typu zapora ogniowa (firewall). Ciekawym rozwiązaniem dla użytkowników domowych jest oprogramowanie służące do filtrowania ruchu danych w sieci. Potrafi ono odfiltrować ruch wchodzący do naszego komputera, jak i wychodzący. Użytkownik dostaje możliwość kontroli i narzędzie do monitoringu nad tym, który program i jaki rodzaj danych są odbierane oraz wysyłane z jego komputera. Tego typu oprogramowanie zyskuje na popularności w przeciwieństwie do malejącej skuteczności „antywirusów".

Podobna sytuacja jest po stronie serwerowej, czyli usługodawcy. Oparcie bezpieczeństwa sieciowego wyłącznie na jednym rozwiązaniu technicznym jest bardzo ryzykowne i skuteczny atak na taką infrastrukturę jest tylko kwestią czasu (o ile już nie nastąpił).

Najbardziej wyrafinowane narzędzia, oparte na analizie behawioralnej, potrafią wykryć zagrożenia, zanim one wystąpią. Robią to na podstawie schematów zachowań, które występują przed materializacją ryzyka. Przykładem tego typu oprogramowania jest oprogramowanie przeciwdziałające transakcjom oszukańczym (antyfraud), czego przykładem może być próba wypłaty dużej sumy środków finansowych za granicą, w przypadku kiedy z informacji zawartych w profilu klienta jednoznacznie wynika, że nie wyjeżdża on poza granice kraju.

4. BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH W PRZYSZŁOŚCI

Katalog działań przestępców stale poszerza się, co przyczynia się do pojawiania się nowych rodzajów zagrożeń, dlatego też w najbliższych latach zapewnienie bezpieczeństwa sieci teleinformatycznych powinno być jednym z priorytetów. Nieustanny rozwój technologii, szczególnie mobilnych, może być czynnikiem kluczowym dla rozwoju firmy, ale również źródłem nowych ryzyk.

Rozwój nowych technologii webowych również będzie stanowił wyzwanie dla pracowników odpowiedzialnych za bezpieczeństwo teleinformatyczne, zarówno jeśli chodzi o zabezpieczenie przed wypływem informacji czy ataków mających na celu dokonanie przestępstw finansowych, jak i zapewnienie ciągłości działania na odpowiednim poziomie.

Niezaprzeczalnie nie tylko wprowadzanie nowych usług wykorzystujących nowe technologie, ale i bezpieczeństwo teleinformatyczne będzie w niedługim czasie stanowić o przewadze konkurencyjnej na rynku usług.

5. NOWOCZESNE TECHNIKI AUTORYZACJI

5.1. Biometria

Biometryczne techniki autoryzacji są znane od bardzo dawna. Biometrię opartą na odcisku palca, czy na skanowaniu siatkówki oka, widzieliśmy w niejednym filmie.

Technologie biometryczne już kilka lat temu zostały wdrożone jako dodatkowa funkcjonalność w komputerach przenośnych. Były to przede wszystkim technologie oparte na weryfikacji linii papilarnych, ale nie tylko. Na rynku można spotkać komputery, które pozwalają zalogować się do nich za pomocą skanowania własnej twarzy.

Proces polega na wykonaniu serii zdjęć głowy w różnych pozycjach (patrząc w dół, w górę itd.), które później są porównywane z danymi, jakie rejestruje kamera. Po zdefiniowaniu takiej funkcjonalności przy standardowym ekranie

logowania pojawia się dodatkowy przycisk, dzięki któremu możemy skorzystać z możliwości zalogowania cechami biometrycznymi.

„Polska, jako pierwszy kraj w Europie wdrożyła biometrię w sektorze bankowym. W 2010 r. rozpoczęto wdrożenie pierwszych w Europie bankomatów biometrycznych, a w 2012 utworzono pierwszy w Europie system oddziałów biometrycznych. Największym rynkiem europejskim stosującym biometrię w bankowości jest Turcja, gdzie czołowe banki wdrożyły biometrię w bankomatach. Macierzą bankowości biometrycznej jest jednak Japonia, gdzie uwierzytelnianie biometryczne w bankach funkcjonuje od 2005 roku i korzysta z niego ponad 40 mln osób”[11].

W Polsce w 2010 roku został oddany do użytkowania również pierwszy w Europie bankomat ze skanerem układu naczyń krwionośnych.

Można wyróżnić 7 głównych metod biometrycznych:

- Odcisk palca – opiera się na analizie charakterystycznych punktów linii papilarnych.
- Tęczówka oka – opiera się na analizie charakterystycznych cech tęczówki oka.
- Naczynia krwionośne palca – opiera się na analizie charakterystycznych wzorów układu naczyń krwionośnych wewnątrz ludzkiego palca.
- Rozpoznawanie twarzy – opiera się na analizie obrazu twarzy.
- Geometria dłoni – opiera się na analizie charakterystycznych cech geometrycznych dłoni.
- Głos – opiera się na analizie charakterystyki głosu.
- Podpis odręczny – opiera się na analizie wizualnej charakterystycznych cech podpisu oraz sposobie jego złożenia (dynamika pióra).

Biometria w bankowości to przede wszystkim coraz szerzej pojawiające się bankomaty wykorzystujące odcisk palca i skaning naczyń krwionośnych. Choć do Japonii czy Turcji pod względem upowszechnienia biometrii nam daleko, to w Europie można nas nazwać pionierem wprowadzania tych metod autoryzacji. Techniki biometryczne, a w szczególności rozpoznawanie naczyń krwionośnych palca, są uważane za stosunkowo bezpieczne, ale nie można zapomnieć, że żadne zabezpieczenie nie daje stuprocentowej pewności.

Jak w przypadku każdych nowych rozwiązań, bardzo ważny jest proces ich wdrożenia, często kluczowy dla bezpieczeństwa użytkowników. Same urządzenia odpowiedzialne za realizację akwizycji oraz analizę danych biome-

[11] Źródło: Raport biometryczny 2.0 „Bankowość biometryczna” Grupa FTB ds. Biometrii Warszawa 2013, praca zbiorowa pod redakcją Tadeusza Woszczyńskiego.

trycznych mogą zachowywać najwyższe standardy bezpieczeństwa, natomiast przesyłanie ich może być niedostatecznie zabezpieczone.

System teleinformatyczny jest tak bezpieczny, jak jego najsłabiej zabezpieczony komponent.

5.2. Biometryka behawioralna – Project Abacus

Podczas konferencji I/O 2016 firma Google zaprezentowała nowy sposób uwierzytelniania o nazwie Project Abacus.

Z danych pozyskanych przez Google wynika, że 70 procent użytkowników zapomina hasła do panelu logowania raz na miesiąc, a do poprawnego zalogowania potrzeba średnio 2,4 prób. Ludzki umysł ma tendencję do zapominania haseł, tym bardziej, że wymagania co do poziomu ich skomplikowania nieustannie rosną (użycie znaków specjalnych, dużych i małych liter, hasła „nie krótsze niż", niepowtarzalność haseł do kilku wstecz). Abacus ma docelowo znieść konieczność tradycyjnej autoryzacji. „Hasłem" autoryzacyjnym według projektu mamy być my sami.

Google zbiera o nas tak dużo informacji, że sami stajemy się hasłem, a konkretnie kombinacją kilku unikalnych parametrów, takich jak sposób korzystania z telefonu połączony z metodą mówienia, pisania, chodzenia, z lokalizacją użytkownika. Każdy z tych czynników brany pod uwagę osobno nie jest niepowtarzalny, by zapewnić nam bezpieczeństwo, ale w zestawieniu tworzy unikalną wartość.

Google twierdzi, że sztuczna inteligencja jest w stanie zidentyfikować zestaw kluczowych czynników „autoryzujących" każdego z nas automatycznie. Abacus ma opierać się na przypisanym każdemu użytkownikowi parametrze o nazwie Trust Score. Kiedy utworzymy wypadkową korelacyjną powyższych parametrów okazuje się, że zabezpieczenie wykazuje się wysoką entropią i jest o wiele silniejsze niż np. czytniki linii papilarnych.

Funkcjonalność Abacusa miałaby umożliwić użytkownikom automatyczne logowanie, autoryzację, włączanie usług itp.

Wkrótce mają rozpocząć się testy, jednak data wdrożenia projektu nie została jeszcze wskazana.

Rozwój technologii informatycznych jest bardzo dynamiczny, dlatego też może okazać się, że pewne funkcjonalności zostaną wdrożone szybciej niż zdążymy się do nich przygotować. Dlatego też już teraz powinniśmy pilnie obserwować trendy i przyglądać się ewentualnym nowo powstającym ryzykom.

6. ROZWÓJ TECHNOLOGII

Obserwując liczbę i skalę zagrożeń, jakie pojawiają się wraz z rozwojem nowych technologii, można odnieść wrażenie, że implementacja nowych funkcjonalności dominuje nad zapewnieniem odpowiedniego poziomu bezpieczeństwa. Dlatego też w przypadku użycia nowych zdobyczy techniki w systemach o kluczowym znaczeniu, takich jak usługi finansowe czy medyczne, trzeba do nich podchodzić z pewną dozą nieufności. Czasami lepiej jest nie korzystać z jakiejś technologii lub poczekać do osiągnięcia pełnej dojrzałości nowego produktu, niż narażać się na straty finansowe lub wizerunkowe.

6.1. Rozwój technologii mobilnych

Technologie mobilne stale są poddawane modyfikacjom mającym na celu ich dalszy rozwój. Niestety patrząc na liczbę pojawiających się nowych podatności na ataki trudno stwierdzić, że wspomniany rozwój ma znaczący wpływ na wzrost poziomu bezpieczeństwa.

Urządzenia, takie jak smartphony czy tablety, są coraz częściej przez nas użytkowane. Z tego typu urządzeń korzystamy coraz śmielej i wykorzystujemy je do rozwiązywania coraz to bardziej wymagających problemów, często nie mając świadomości skali ryzyka, jakie się z tym wiąże.

6.2. Coraz szersze wykorzystanie kanałów elektronicznych

Środek ciężkości korzystania z usług finansowych coraz bardziej przenosi się ze sfery tradycyjnej, tj. „fizycznej", do „wirtualnej", czyli internetowej. Przewiduje się, że wkrótce może zostać zlikwidowana duża część oddziałów banków, co będzie skutkowało zmianą dotychczasowego modelu ich działania. Oferta będzie skupiała się wokół zindywidualizowanych potrzeb klienta, a nie na liniach produktowych. Rozwój biznesu nie będzie już oparty o ekspansję terytorialną, lecz o innowacyjność w podejściu do klienta, lepsze zarządzanie ryzykiem i udoskonalone techniki marketingowe w przestrzeni wirtualnej. Wynikać to będzie z jednej strony z wykorzystania bardziej skutecznych spersonalizowanych metod marketingu, w oparciu np. o dane z mediów społecznościowych, białego wywiadu, jak również bardzo silnego nacisku pozabankowego sektora usług finansowych (np. FinTech). Może on efektywniej wprowadzać innowacje w teleinformatycznej przestrzeni, zarówno technologiczne, jak i biznesowe (jak np. różne modele crowdsourcingu czy usług płatniczych). Dotychczasowy model biznesowy banków i przedsiębiorstw międzynarodowych niezajmujących się usługami finansowymi, może zostać zakłócony przez usługi i produkty podmiotów dotychczas niefunkcjonujących na rynku usług finansowych, które wykorzystując swoją pozycję i doświadczenie w przestrzeni wirtualnej potrafią szybko i niedrogo zdobyć znaczącą część rynku usług finansowych. Z technologicznego punktu widzenia już dziś nie ma przeszkód w opracowaniu przez nie, wspólnie lub oddzielnie, schematu obiegu i płatności pieniądza elektronicznego, i uruchomienie tego rozwiązania w znaczącej skali.

W tym kontekście zupełnie podstawową kwestią jest zapewnienie stabilności działania systemu finansowego poprzez wypracowanie skutecznych mechanizmów zabezpieczeń i ich monitoringu, zarówno co do procesów realizacji nowego typu usług, jak i samych komponentów (urządzeń) wykorzystywanych w takich usługach. Pierwszorzędną kwestią jest tutaj skuteczne zapewnienie bezpieczeństwa urządzeń przenośnych jako wiodących komponentów, za pomocą których użytkownicy będą wykorzystywać nowe usługi w przyszłości. Niestety praktycznie wszystkie wiodące systemy mobilne mają już w swej historii zaliczonych wiele „wpadek" w dziedzinie skuteczności mechanizmów zabezpieczeń.

6.3. Przetwarzanie w chmurze

Cloud computing („przetwarzanie w chmurze") to model świadczenia usług zapewniający, niezależnie od lokalizacji, dogodny dostęp sieciowy „na żądanie" do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług[12].

Można zaobserwować wzmożone zainteresowanie usługami realizowanymi w modelu chmury obliczeniowej na rynku usług finansowych.

W zależności od sposobu realizacji wyróżniamy cztery typy chmur obliczeniowych:

- publiczną,
- prywatną,
- hybrydową,
- współdzieloną.

Chmura publiczna

Na największy zbiór ryzyk narażona jest realizacja chmury obliczeniowej w modelu publicznym.

Cechą chmury publicznej jest jej pełna realizacja przez dostawcę usługi, tzn. cała infrastruktura oraz odpowiedzialność za jej działanie leży po stronie dostawcy.

Zidentyfikowane przykłady ryzyk w modelu publicznej chmury obliczeniowej to:

1. Uzależnienie od dostawcy – realizacja w przypadku woli zakończenia współpracy z usługodawcą może stać się bardzo trudna, co wynika m.in. z tego, że często brak jest odpowiednich narzędzi pozwalających na efektywne przeniesienie danych i systemów teleinformatycznych na inną platformę.

[12] Na podstawie NIST Special Publication 800-145 „The NIST Definition of Cloud Computing", National Institute of Standards and Technology, 2011, Peter Mell, Timothy Grance http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp 12.02.2018 r.]

2. Utrata możliwości nadzoru – w modelu cloud computing klient przekazuje sprawowanie kontroli nad wieloma aspektami bezpieczeństwa dostawcy usług.
3. Utrudnione ustalenie sprawcy włamania – proces przetwarzania w chmurze przenosi obowiązek identyfikacji zagrożeń w systemach informatycznych na dostawcę. Skompromitowanie zabezpieczeń usługodawcy może wiązać się z utratą zaufania i negatywną oceną, co może powodować rezygnację z korzystania z usług tego dostawcy w przyszłości.
4. Niewłaściwe usuwanie danych – w przypadku chęci usunięcia danych przez dostawcę usług cloud computing, znacząco utrudniona jest weryfikacja procesu usuwania danych.
5. Błędy w zakresie izolacji – usługi w modelu cloud computing świadczone są zwykle dla wielu klientów na wspólnej platformie infrastrukturalnej i przez to mogą potencjalnie wystąpić sytuacje, w których jeden klient uzyska nieautoryzowany dostęp do systemów lub danych innego klienta.
6. Bezpieczeństwo danych podlegających ochronie (dane osobowe, dane objęte tajemnicą bankową) – w niektórych przypadkach modelu cloud computing znacząco utrudniona może być weryfikacja poprawności i efektywności procedur przetwarzania danych przez dostawcę usług. Czasami trudność sprawia nawet uzyskanie podstawowych informacji, jak np. czy dane będą przetwarzane tylko w Europejskim Obszarze Gospodarczym (EOG).
7. Otoczenie prawne – firmy dostarczające usługi w krajach podlegają jurysdykcjom, które mogą wymuszać stały, pełny dostęp do danych zgromadzonych na serwerach firm usługodawców.

Chmura prywatna

Chmura prywatna jest realizacją koncepcji przetwarzania rozproszonego w oparciu o swoją własną infrastrukturę. Z racji tego, że całość infrastruktury jest u klienta, poziom bezpieczeństwa pozostaje pod jego kontrolą, co jednak nie oznacza, że ten typ rozwiązania nie niesie za sobą zagrożeń.

Zidentyfikowane przykłady ryzyk w modelu prywatnej chmury obliczeniowej to:

1. możliwe błędy w zakresie izolacji (segmentacji) danych i procesów,
2. problemy z trwałym usuwaniem informacji,
3. wydajność i odporność na awarię ograniczona zasobami własnymi firmy.

Chmura hybrydowa

Chmura hybrydowa to połączenie rozwiązania chmury publicznej i prywatnej. Głównym problemem może tu być separacja infrastruktury własnej klienta (chmury prywatnej) od infrastruktury dostarczanej przez usługodawcę rozwiązań chmurowych (chmury publicznej). Ryzyka, zgodnie z zasadą, że techno-

logia jest tak silna jak jej najsłabsze ogniwo, są tożsame z ryzykami występującymi w realizacji publicznego modelu przetwarzania w chmurze. Dobrym przykładem realizacji wykorzystania chmury hybrydowej są kampanie marketingowe, które mogą znacząco, ale chwilowo, zwiększyć zapotrzebowanie na przestrzeń dla danych lub możliwości obliczeniowe.

Chmura współdzielona

Ostatnim typem realizacji modelu przetwarzania w chmurze jest chmura współdzielona. Koncepcja chmury współdzielonej jest bardzo interesująca, bo chociaż jest to formalnie chmura publiczna, to z uwagi na ograniczony zakres klientów oraz realizację modelu przez interesariuszy, ryzyka są tutaj o wiele bardziej ograniczone niż w przypadku tradycyjnego modelu chmury publicznej. Kontrolę nad procesem przetwarzania danych realizuje podmiot zaufany, co znacząco wpływa na bezpieczeństwo, w kontekście np. nieuprawnionego dostępu do danych czy stosowanych metod kryptograficznych. Przykładem takiej realizacji jest projekt cloud.gov przeznaczony dla agencji federalnych rządu Stanów Zjednoczonych Ameryki Północnej. Odpowiada za niego zespół 18F będący częścią General Services Administration, czyli niezależnej agencji wspierającej inne agencje w realizacji zadań administracyjnych[13].

Innym przykładem mogą być chmury obliczeniowe stworzone w ramach jednej grupy kapitałowej.

6.4. Bezpieczeństwo teleinformatyczne – wyzwanie dla zarządu i wyższej kadry menedżerskiej

Zwiększający się poziom zagrożeń, na jakie narażone są systemy teleinformatyczne banków powoduje, że zakres kompetencyjny z obszaru bezpieczeństwa teleinformatycznego musi piąć się na coraz wyższe stanowiska struktur przedsiębiorstw zajmujących się wrażliwymi gałęziami gospodarki. Coraz większy poziom rozwoju i skomplikowania technologii wymuszają wyrafinowane rozwiązania przeciwdziałające atakom oraz ograniczające ryzyka mogące powstać na drodze działalności przestępczej w tym obszarze. Obecnie bardzo trudno jest kreować wizję i strategię IT bez znajomości nowych zagrożeń i środków ich przeciwdziałania. Akceptacja proponowanych przez niższe szczeble struktur banków rozwiązań technicznych, dotyczących bezpieczeństwa infrastruktury teleinformatycznej (sieci i systemów) bez odpowiedniej wiedzy i kompetencji zarządu banku z zakresu nowoczesnych technologii, jest już niemożliwa w przypadku sprawnie i skutecznie działającej jednostki.

Dodatkowym czynnikiem jest konieczność weryfikacji, czy proponowane rozwiązania techniczne oraz infrastrukturalne nie rozmijają się z obmyśloną wizją i strategią banku. Kolejnym ważnym wątkiem jest umiejętność dostrzeżenia korelacji między rozwiązaniami technicznymi a możliwością wykorzystania ich w kontek-

[13] Źródło: https://cloud.gov [dostęp 12.02.2018 r.]

ście spełnienia wymogów regulacyjnych. Aby móc je dostrzec, osoba decyzyjna musi mieć umiejętność szerszego, bardziej technicznego spojrzenia.

6.5. Skuteczna walka z cyberzagrożeniami – współpraca ponad podziałami

Walka konkurencyjna między dostawcami usług finansowych może być pozytywnym zjawiskiem, ale nie może być ona stosowana, gdy w grę wchodzi bezpieczeństwo. W tym wyjątkowym przypadku wszystkie podmioty z danego sektora muszą współpracować razem dla wspólnej sprawy. Zaniedbanie jednego z obszarów bezpieczeństwa w przedmiotowym zakresie może zaszkodzić stabilności funkcjonowania całego rynku.

9 maja 2017 r. Prezes Rady Ministrów podpisała uchwałę nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Zgodnie z zapisami dokumentu:

> „Podstawą skutecznej reakcji na zagrożenia i ataki jest funkcjonowanie niezawodnych i bezpiecznych mechanizmów wymiany informacji pomiędzy interesariuszami krajowego systemu cyberbezpieczeństwa. Z drugiej strony powszechnie występującym problemem jest niechęć tych podmiotów do dzielenia się informacją na temat zauważonych zagrożeń, incydentów oraz szacowanych strat. Niezależnie od rozwiązań prawnych określających jednoznaczne mechanizmy wymiany informacji o cyberbezpieczeństwie, w pierwszym okresie konieczne jest utworzenie lub rozbudowa krajowej sieci CSIRT (narodowy, sektorowe, komercyjne i przedsiębiorców), które wymieniałyby kluczowe informacje o zagrożeniach bezpieczeństwa i incydentach w danym sektorze bądź dziale administracji rządowej”.

Dlatego wszystkie inicjatywy zarówno rządowe, jak i pozarządowe, mające na celu zwiększenie bezpieczeństwa teleinformatycznego Polski są bardzo ważne.

Bardzo istotną rolę w kontekście bezpieczeństwa teleinformatycznego pełni Naukowa i Akademicka Sieć Komputerowa (NASK) oraz działający w jej strukturach CERT.

NASK

W pierwotnej formie NASK był jednostką badawczo-rozwojową, natomiast od 30 kwietnia 2010 r. funkcjonuje jako instytut badawczy. Instytut prowadzi działalność naukową, krajowy rejestr domen.pl i jest dostawcą zaawansowanych usług teleinformatycznych. NASK oferuje nowoczesne rozwiązania teleinformatyczne dla klientów biznesowych, administracji i nauki.

CERT

Zespół CERT Polska to działający w strukturach NASK zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Od początku istnienia zespołu rdzeniem jego działalności jest obsługa incydentów bezpie-

czeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w sferze działalności operacyjnej, jak i badawczo-wdrożeniowej.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników,
- współpraca z innymi zespołami CERT w Polsce i na świecie,
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego,
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy szkodliwego oprogramowania i systemów wymiany informacji o zagrożeniach,
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń,
- regularne publikowanie raportu CERT Polska o bezpieczeństwie polskich zasobów Internetu,
- działania informacyjno-edukacyjne zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w serwisach społecznościowych Facebook i Twitter,
  - organizacja cyklicznej konferencji SECURE,
  - niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

NC Cyber – Narodowe Centrum Cyberbezpieczeństwa

Narodowe Centrum Cyberbezpieczeństwa[14] (NC Cyber) działa w strukturze NASK. Głównym zadaniem Centrum jest dbałość o bezpieczeństwo cyberprzestrzeni RP, m.in. poprzez opracowywanie narodowych planów ochrony. NC Cyber współpracuje w tym zakresie z administracją, biznesem oraz ze środowiskiem naukowym. Centrum funkcjonuje jako ośrodek wczesnego ostrzegania, który działając w systemie 24/7 monitoruje i zarządza trybem informowania o zagrożeniach sieciowych. Centrum zajmuje się również obsługą zgłoszeń szkodliwych i nielegalnych treści (Dyżurnet.pl).

[14] https://www.nask.pl/pl/dzialalnosc/nc-cyber/142,NC-Cyber-Narodowe-Centrum-Cyberbezpieczenstwa.html [dostęp 12.02.2018 r.]

Narodowe Centrum Cyberbezpieczeństwa zostało oficjalnie otwarte 4 lipca 2016 roku.

Związek Banków Polskich

Jednym z zadań Związku Banków Polskich (ZBP) jest organizowanie współdziałania banków na rzecz rozwoju sektora bankowego i infrastruktury międzybankowej, w zakresie bezpieczeństwa banków i przeciwdziałania wykorzystywaniu banków w działalności przestępczej, w tym również cyberprzestępczej. ZBP przedstawił na swojej stronie internetowej praktyczny poradnik dotyczący bezpieczeństwa transakcji bankowych w internecie[15].

System Wymiany Ostrzeżeń o Zagrożeniach

Inicjatywą godną uwagi w kontekście bezpieczeństwa teleinformatycznego, realizowaną od lat przez Związek Banków Polskich, jest system SWOZ (System Wymiany Ostrzeżeń o Zagrożeniach). SWOZ to narzędzie służące do szybkiego ostrzegania o zagrożeniach w sektorze bankowym. Sektor bankowy jest szczególnie narażony na zagrożenia teleinformatyczne ze względu na bezpośredni dostęp do środków pieniężnych klientów.

Bankowe Centrum Bezpieczeństwa

Bankowe Centrum Bezpieczeństwa powstało ze względu na potrzebę mitygacji rosnącego ryzyka związanego z cyberprzestępczością sektora bankowego. Pierwotnie Bankowe Centrum Bezpieczeństwa funkcjonowało w ramach struktur ZBP, natomiast wraz z otwarciem Narodowego Centrum Cyberbezpieczeństwa zostało „wcielone" do jego struktur jako jedna z kluczowych platform. Celem Centrum jest wykrywanie cyberzagrożeń, ich analiza i operacyjne przeciwdziałanie skutkom ataków na systemy teleinformatyczne banków i innych instytucji publicznych.

Technologie teleinformatyczne rozwijają się w zawrotnym tempie. Świat technologii śmiało wchodzi w świat finansów. Płatności elektroniczne, bankowość internetowa i urządzenia mobilne to technologie, z których korzystamy codziennie, pojawiają się przedsiębiorstwa FinTech, które wprowadzą kolejne nowe produkty i usługi oparte na rozwiązaniach informatycznych.

Bezpieczeństwo teleinformatyczne usług w niedługim czasie może stanowić nie tylko o przewadze konkurencyjnej przedsiębiorstwa, ale również o jego istnieniu.

Dlatego w kontekście sektorowym, jak i międzynarodowym, współpraca stanowi klucz do bezpieczeństwa gospodarki, a wszystkie inicjatywy tworzące prawne i instytucjonalne ramy takiej współpracy, takie jak uchwalona przez Parlament Europejski Dyrektywa NIS przyczyniają się do wzrostu globalnego bezpieczeństwa.

[15] Źródło: http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=1

BIBLIOGRAFIA:

1. M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*, KNF, 2014 r.

   https://www.knf.gov.pl/?articleId=54745&p_id=18

2. M. Pachucki, *Piramidy i inne oszustwa na rynku finansowym - Poradnik klienta usług finansowych, wydanie III zaktualizowane*, KNF, 2016 r.

   https://www.knf.gov.pl/knf/pl/komponenty/img/piramidy%20finansowe%20calosc%20internet_48851.pdf

3. B. Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognozy,* KNF, 2013 r.

   https://www.knf.gov.pl/?articleId=53993&p_id=18

KNF

CEDUR
Centrum Edukacji dla Uczestników Rynku

Komisja Nadzoru Finansowego
Adres korespondencyjny:
Pl. Powstańców Warszawy 1
Skr. poczt. nr 419, 00-950 Warszawa 1
Tel. (+48) 22 262 50 00
Fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl

ISBN 978-83-63380-16-8