aut. Andrzej Kozłowski 31.01.2017

WICEPREZES ZWIĄZKU BANKÓW POLSKICH: CYBERBEZPIECZEŃSTWO JEST WBUDOWANE W DNA BIZNESU BANKOWEGO

O atakach cyfrowych na sektor bankowy, działaniach Związku Banków Polskich, Bankowym Centrum Cyberbezpieczeństwa oraz wyzwaniach w przyszłości mówi dla Cyberdefence24.pl Mieczysław Groszek, wiceprezes Związku Banków Polskich.

Andrzej Kozłowski: Sektor bankowy na całym świecie uważany jest za jeden z najbardziej podatnych na cyberataki. Czy w Polsce jest podobnie?

Dr Mieczysław Groszek: Nie zgodzę się ze słowem „podatny". Podatny to znaczy łatwy do zaatakowania. Sektor bankowy jest atrakcyjnym celem ataków. Po pierwsze, w szerszym zakresie niż inne używa instrumentów elektronicznych. Po drugie, są tam duże pieniądze. Rożnego rodzaju oszustwa elektroniczne zmierzają do osiągnięcia jakiejś konkretnej korzyści, nie tylko bankowej, ale czasem mają również doprowadzić do zniszczenia. Najkrócej mówiąc, jest to kradzież pieniędzy przy wykorzystaniu różnych technik. Porównajmy to ze starą epoką – napadami na dyliżans czy konwojami. Kradzione w ten sposób banknoty były posortowane, z zapisanymi numerami i dlatego trudno było je wprowadzić do obiegu. W przypadku pieniądza elektronicznego ta sytuacja nie występuje. Dlatego jest to z punktu widzenia przestępcy tzw. bezpieczny pieniądz.

A.K.: Czy są prowadzone w Polsce badania na temat szacunkowych strat sektora bankowego z powodu działalności cyberprzestępców?

M.G.: Komisja Nadzoru Finansowego sporządza raporty, w których są bardzo precyzyjne zapisy. W ubiegłym roku było około 95 mln zł strat banków z tytułu przestępstw elektronicznych. Związek Banków Polskich robi rachunek netto i brutto. 95 mln to jest rachunek netto, czyli tyle, ile straciły banki, natomiast nie ma precyzyjnego określenia, ile mogłyby stracić, gdyby sukcesem zakończyły się udaremnione ataki. Tutaj pojawia się jednak problem wynikający z użycia różnej metodologii. Przykładowo bank blokuje przelew, wyjaśnia, okazuje się, że są spełnione wszystkie przesłanki, że jest to przestępstwo, i zatrzymuje proces. Sytuacja ta nie jest jednak wliczana w przytaczaną sumę. Gdyby nie system bezpieczeństwa, filtry, firewalle i tak dalej to byłoby tego więcej, ale tej drugiej liczby nie znamy.

A.K.: W takim razie jakie są największe zagrożenia, jakich technik najczęściej używają cyberprzestępcy w Polsce przeciwko bankom?

M.G.: Zacznijmy od najpoważniejszych zagrożeń. Są to ataki na operacyjny system bankowy. Półtora roku temu otrzymaliśmy sygnał, że taki atak nastąpi. Informacja została przekazana do jednego z banków. Sprawdzono sieci, ale nie znaleziono żadnego złośliwego oprogramowania, metodami operacyjnymi CERT.gov.pl także nie stwierdził symptomów przygotowywania „dużego” ataku na

system - zarówno w kraju, jak i z zagranicy. Mimo to podjęliśmy działania do uszczelnienia systemu. Wtedy powołaliśmy nasze wewnętrzne bankowe centrum bezpieczeństwa oraz nawiązaliśmy bliższą współpracę z organami odpowiedzialnymi za bezpieczeństwo. W szczególności bardzo dobrze przebiegała współpraca z ABW, która dysponuje instrumentami i informacjami, do których sektor prywatny nie ma dojścia. Odbyliśmy również trzy spotkania z CERT.GOV, który jest głównym organem odpowiedzialnym za bezpieczeństwo domen państwowych. W czasie podwyższonego zagrożenia cyberatakiem CERT.GOV wzmocniło obsadę.

Następnym rodzajem zagrożeń są ataki na systemy konkretnych banków. Miało to miejsce wiosną 2015 roku. Wtedy najmniejszy bank w Polsce poniósł straty w wysokości około 5 mln. Badając ten incydent oraz inne podobne, bardzo ważne okazało się zarządzanie kryzysem i między innymi kontakt z klientami. Zaatakowany bank podjął w tym obszarze działania, zanim podały to media. Media zresztą miały o to pretensje, że o incydencie poinformowaliśmy zbyt późno. Jednak było to nasze celowe działanie na życzenie organów ścigania, które nie chciały wszczynać paniki dla dobra śledztwa. Był to naprawdę dobry test na współpracę z policją. Oceniam ją bardzo pozytywnie, a w szczególności z komórką do przeciwdziałania cyberprzestępczości.

Wcześniej pracowaliśmy razem z policją przy aresztowaniu Polsilvera, którego celowo nie nazywam hakerem, bo to był po prostu przestępcą. Najpierw pracował on dla firmy informatycznej, która robiła instalacje dla zaatakowanego banku. Motyw działania Polsilvera był czysto finansowy. Gdyby to był „tradycyjny" napad na bank, to pewnie nakręcono by na podstawie tego co najmniej dwa filmy. Natomiast my nie chcemy ujawnić za dużo informacji.

A.K.: A jakie są największe źródła niebezpieczeństwa dla klientów banków?

Kolejną metodą ataku jest kradzież tożsamości użytkownika. Polega ona na tym, że pod prawdziwymi danymi fałszywy osobnik wyciąga pieniądze. Jest to rodzaj bezpośredniego uderzenia w klienta, z tą metodą możemy się najczęściej spotkać. Mamy też do czynienia z kradzieżą danych w bankomatach. Bardzo często obserwujemy kombinację phishingu i *business email compromise*. Phishing polega tutaj na podłożeniu fałszywej strony, na którą klient się loguje, po czym podaje swoje dane. Natomiast *business email compromise* umożliwia wchodzenie w różnego rodzaju systemy niefinansowe, najczęściej pocztowe, i prowadzenie obserwacji, a następnie wymuszenie na właścicielu konta podjęcie niekorzystnej dla niego (a korzystnej dla przestępcy) decyzji. Bardzo popularne było włamanie na tzw. prezesa. Polegało ono na tym, że przestępcy, po wcześniejszym dokładnym rozpoznaniu firmy, jej zwyczajów, poprzez włamanie do poczty wewnętrznej, dzwonili od odpowiedniej osoby lub wysyłano informacje mailem z treścią, że dzwoni/pisze prezes i prosi o dokonanie szybkiego przelewu na dany rachunek. O tym, że czasem taką drogą prezes wydaje dyspozycje, przestępcy wiedzieli po spenetrowaniu poczty lub podsłuchu telefonów, o czym wcześniej wspomniałem.

Coraz popularniejsze są również tzw. złote strzały. Kiedyś cyberprzestępczość cechowała się masowymi działaniami i kradzieżą niewielkich sum pieniędzy. Obecnie wybiera się małą liczbę celów o dużej wartości, a przygotowanie do ataku zajmuje o wiele więcej czasu.

A.K.: Mówiliśmy o pewnym krajobrazie zagrożeń. Co związek robi, aby z nimi walczyć? Jakie są główne inicjatywy?

M.G.: Mówiąc kolokwialnie, cyberbezpieczeństwo jest wbudowane w DNA biznesu bankowego. Niedawno miałem spotkanie z najstarszym zespołem Polskiego Związku Banków, jakim jest Rada Bezpieczeństwa Banków. Wspominano, że na samym początku członkowie zespołu chodzili z bronią palną i pełnili rolę konwojentów. W tamtym czasie hasło bezpieczeństwo było kojarzone z napadami, z kamerą, z facetem, który chodzi i patrzy na wszystkich podejrzliwie.

Obecnie technologia spowodowała, że w kasach bankowych nie ma pieniędzy. Zasilenie gotówkowe, pomimo dużego obrotu, jest rozproszone. Teraz większość pieniędzy znajduje się w bankomatach, których na terenie Polski mamy ponad 25 tys. Również w oddziałach przechowywane są niewielkie zasoby gotówki. Jeśli chcemy wyjąć powyżej 5 tys zł, to musimy wcześniej o tym fakcie powiadomić, żeby przygotowano odpowiednią kwotę. Jest to przykład fizycznego bezpieczeństwa, które wciąż jest ważne. Następnie pojawiła się bankowość elektroniczna, do której ludzi bardzo zachęcaliśmy. Równolegle z tym skupiliśmy się na informacjach o rodzajach zagrożeń i instrukcjach jak ich unikać.

A.K.: Jak wygląda polityka informacyjna banku?

Bardzo ważne jest mówienie o zagrożeniach, ale nie ciągłe, ponieważ wtedy klient się męczy i jego odbiór zaczyna się blokować. W ramach naszych zespołów ocenialiśmy czasami krytyczne informacje, które banki podają na temat bezpieczeństwa na swoich stronach. Strony transakcyjne ostrzegają klientów przed zagrożeniami. Naszym zdaniem powinno to być odpowiednio uwydatnione. Trzeba sprawić, żeby klient się tym zainteresował wcześniej, a nie dopiero jak media napiszą o ataku.

Ponadto staramy się wyjść z informacjami na temat cyberbezpieczeństwa poza obszar banku, ponieważ nie chodzi tylko o pieniądze na koncie – jest to również sprawa ochrony tożsamości w internecie, niezależnie czy w kontekście bankowości elektronicznej, ale też w handlu internetowym, a nawet niewinnym prywatnym używaniu poczty i korzystaniu z różnych portali. Przykładowo, obserwuje się korespondencję mailową, bo w ten sposób poznaje się zwyczaje ludzkie. Ludzie są nieostrożni, wchodzą na niezabezpieczone strony albo nie korzystają z programów antywirusowych. Cyberbezpieczeństwo i cyberświadomość to jest dzisiaj część naszej postawy życiowej i zwyczaje w cyberprzestrzeni są bardzo ważne. Uważam, że to powinno stać się częścią edukacji.

A.K.: Sektor bankowy jest liderem działań informacyjno-edukacyjnych w zakresie cyberbezpieczeństwa. Wydaje się jednak, że to administracja powinna pełnić tutaj główną rolę.

M.G.: Dlatego uważamy, że powinien być to wspólny wysiłek wszystkich, którzy się tymi sprawami zajmują. Jako związek podjęliśmy się pewnego rodzaju misji i rozwinęliśmy akcję edukacyjną. Obecnie pełnimy rolę koordynatora rożnych inicjatyw edukacyjnych podejmowanych przez wiele instytucji. W Ministerstwie Cyfryzacji jeszcze za czasów ministra Boniego powstała inicjatywa koalicji na rzecz kształtowania cybertożsamości i cyberświadomości. Pozgłaszały się różne instytucje. Pomysł ten niestety upadł, ale była to doskonała inicjatywa. W ramach Bankowego Centrum Bezpieczeństwa zbudowaliśmy koncepcję opartą na trzech filarach i jednym z nich była właśnie edukacja. My, jako związek, dostarczamy ekspertów.

A.K.: Nawiązując do Bankowego Centrum Cyberbezpieczeństwa, co zadecydowało o jego stworzeniu?

M.G.: Było ono efektem naturalnego rozwoju. Z jednej strony wynikało z naszych doświadczeń, z drugiej z naszych potrzeb. Przede wszystkim należy zacząć od dynamicznego rozpowszechnia się instrumentów bankowości elektronicznej. Jeszcze 20 lat temu było nieco ponad 2 tys. kont, dzisiaj jest ich 35 mln, z czego połowa jest aktywnych. To już pokazuje skalę. Po drugie rachunków bankowych jest 36 mln. Są one przeróżne, często ludzie posiadają po kilka. Tylko 6 mln rachunków nie ma dostępu elektronicznego. I to prawdopodobnie tych nieaktywnych, należących do osób starszych.

Po drugie, oczywiście tak jak się rozprzestrzeniała bankowość, tak pojawiały się zagrożenia. Mają one charakter oszustw, ataków i włamań. Zawsze się tym zajmowaliśmy, pierwszą płaszczyzną współpracy była wymiana informacji. Jednym z naszych pierwszych systemów kodowanych był system wymiany informacji o zagrożeniach. Gromadzono w nim różnego rodzaju kategorie danych.

Z czasem doszliśmy jednak do wniosku, że jest to niewystarczające i dlatego zdecydowaliśmy się powołać zespoły w ramach bankowości elektronicznej. Jednym z nich jest grupa robocza ds. bezpieczeństwa transakcji elektronicznych, działająca na styku bankowości (elektrocznej - przyp. red.) i kart. Potem powołaliśmy forum IT. Powodem tej decyzji były rekomendacje Komisji Nadzoru Finansowego (KNF), która jest centralnym organem administracji rządowej, sprawującym nadzór nad rynkiem finansowym. KNF stwierdziła, że podejście do bezpieczeństwa powinno mieć charakter całościowy, czyli że jest to cała organizacja, a nie skupianie się na zabezpieczaniu konkretnych ludzi lub procesów.

A.K.: Na czym polega to w praktyce?

W rekomendacji pojawiają się również zadania dla rady nadzorczej. Przykładowo polityka bezpieczeństwa ma być ustalana przez zarząd i polega na stworzeniu odpowiednich procedur. Bezpieczeństwo buduje się nie poprzez reakcje na incydenty, ale przez to, że system jest niepodatny albo mało podatny na zagrożenie. Dlatego bezpieczeństwo powinno polegać na zabezpieczeniu technologii hardware i software, tak żeby nie zostawiać włączonego komputera, kiedy się wychodzi czy nie stosować haseł i loginów jak np. admin1 czy 123456. Nie może również dochodzić do takiej sytuacji, że przy dowolnym zakłóceniu wyłącza się cały system.

Owocem naszej współpracy z KNF było powołanie zespołu ds. IT i systemów Bankowych Rejestrów Incydentów IT, czyli bazy danych o incydentach. Przeszliśmy w ten sposób do procedur zarządzania incydentem. Ministerstwo Cyfryzacji również interesuje się tym rozwiązaniem, ponieważ chcieliby zrobić coś bardzo podobnego, ale w układzie wielosektorowym.

A.K.: Jak wygląda struktura Bankowego Centrum Cyberbezpieczeństwa?

Ponad rok temu powołaliśmy Bankowe Centrum Cyberbezpieczeństwa składające się z trzech szczebli. Na szczycie jest komitet sterujący złożony z ludzi odpowiadających całościowo za bezpieczeństwo w bankach, szczebel niżej grupa analityczna, a na samym dole grupa operacyjna.

Kiedy wiosną 2016 roku pojawiła się informacja, że 217 banków będzie zaatakowanych, to wtedy postanowiliśmy przekształcić się w sztab antykryzysowy. Nawiązaliśmy również kontakt z bankami, dostarczając im odpowiednich informacji. Należy również pamiętać, jakie było tło całej sprawy: stwierdzono, że jeżeli banki mają skutecznie się zabezpieczyć przez malwarami, to powinny zakupić konkretny produkt. Wprowadziliśmy ponadto zasadę konsultacji z jednostkami posiadającymi systemy detekcyjne, aby omawiały z nami komunikaty ostrzegające o zagrożeniach, tak aby informowały propocjonalnie do skali ryzyka, i nie robiły medialnych sensacji, tam gdzie to ryzyko jest niewielkie.

W naszym zespole istnieje także zespół analityków, którzy pracują głównie na materiale historycznym i opracowują rekomendacje na przyszłość. Novum jest zespół operacyjny. Wcześniej działał on na zasadzie, tak że między bankami było porozumienie o systemie monitorowania sieci i co tydzień inny bank pełnił dyżur. Obecnie pracujemy nad powołaniem wspólnego poziomu operacyjnego w ramach Narodowego Centrum Cyberbezpieczeństwa, gdzie dysponujemy trzema stanowiskami „w ruchu ciągłym”. Naszym celem jest też to, żeby mieć dostęp do informacji, które będą przetwarzane w czasie realnym. Centrum swoim poziomem nie odbiega od światowych standardów. Przykładowo w Stanach Zjednoczonych w takim ośrodku dyżurują obok siebie nie tylko przedstawiciele różnych sektorów prywatnych, ale również FBI. Jak była potrzebna interwencja, to jedna jednostka namierzała, a druga szybko analizowała i następnie decydowano o zatrzymaniu przestępcy.

A.K.: Jakie będą główne zagrożenia i wyzwania dla sektora bankowego w 2017 roku?

M.G.: Musimy mieć świadomość, że zagrożenia zawsze będą. Wynika to z rozwijającej się technologii.

Obecnie pracujemy wraz z Ministerstwem Cyfryzacji nad bezpieczną przeglądarką. Mamy nadzieję, że pozwoli to na wyeliminowanie phishingu tak, żeby strona weryfikowała, czy łączymy się z pożądaną witryną, a nie podstawioną przez hakerów. Technologicznie to jest trudne do zrealizowania, ale możliwe. Musimy to zrobić, ponieważ obecny biznes elektroniczny jest masowy, mamy do czynienia z masowym klientem, a on bywa różny. I w związku z tym trzeba zorganizować nie tylko przyjazne rozwiązania, ale również przyjazne środki bezpieczeństwa. Gdy przeprowadziliśmy badanie, w którym dwustu dyrektorów banków wypowiedziało się o różnych sprawach, m.in. odpowiedzieli na pytanie, co bardziej cenią ich klienci - bezpieczeństwo czy wygodę, jak Pan myśli, co odpowiedzieli?

A.K.: Wygodę.

M.G.: Oczywiście. Klient wierzy, że coś jest bezpieczne, bo jest oferowane na rynku bankowym. Musimy jednak konstruować elementy bezpieczeństwa, które są przyjazne dla użytkownika. Czyli mają zabezpieczać przez jedno kliknięcie. Pamiętam taką sytuację, że jedna z firm produkujących systemy antywirusowe zaproponowała, że zainstaluje oprogramowanie ochronne. Jednak pojawiły się problemy, nie wszyscy chcieli się zgodzić, bo musieliby oddać komputery albo gdzieś z nimi się zgłosić. Większość nie skorzystała.

Musimy zagrożenia badać. Przykładowo na SGH jest osoba, która specjalizuje się w ekonomice przedsiębiorstwa przestępczego. Dzięki swojej pracy ma ona szerokie spojrzenie na ten niezwykle istotny temat. W przypadku darknetów nie wiemy ani co, ani kto się za nimi kryje, my je tylko identyfikujemy lub rekonstruujemy. Dzięki pracy analitycznej jesteśmy w stanie poznać, jak działają właśnie takie specyficzne przedsiębiorstwa i okazuje się, że to nie jest zabawa czy przypadkowa działalność, ale dobrze zorganizowane przestępcze przedsiębiorstwo. Na początku lat 90. społeczeństwa z sympatią traktowały hakerów. Ktoś, kto włamał się do Pentagonu, był uznawany z bohatera. Dzisiaj wszyscy się ich słusznie boją.

Kolejnym elementem, nad którym pracujemy, jest używanie odpowiednich definicji i komunikatów, żeby właściwe opisać zjawiska. Komunikaty muszą ludzi informować i edukować, a nie straszyć. Nie może mieć miejsca taka sytuacja, że ktoś ze strachu przed zagrożeniami nigdy nie otworzy konta. Ja konta internetowego używam od 20 lat i nigdy na tym nic nie straciłem. Pamiętam, że uczestniczyłem w konferencji na uczelni Akademii Leona Koźmińskiego, w której brało udział ponad 300 uczestników. Zapytałem, czy ktoś z nich padł ofiarą cyberprzestępstwa. Zgłosiło się 5 osób. Przykład ten pokazuje, że sytuacja wcale nie wygląda tak źle.

A.K.: Czyli jest Pan optymistą?

Jestem optymistą, jeśli chodzi o przyszłość cyberbezpieczeństwa. Prowadzimy obecnie rozwiniętą współpracę międzysektorową m.in. z telekomami czy Rządowym Centrum Bezpieczeństwa, którzy się zajmują infrastrukturą krytyczną. Uczestnicząc w konferencjach, widzę również zmianę języka, którym posługuje się rząd. Musimy zbudować podobny kontakt z wojskiem, tak jak zrobiliśmy to wcześniej z ABW, a jeszcze wcześniej z policją.

Duże nadzieje pokładałam również w przygotowywanej Ustawie o krajowym systemie cyberbezpieczeństwa. Pozytywnie oceniam w tym zakresie pracę Ministerstwa Cyfryzacji, które jest bardzo pragmatyczne w swoich działań i w swoich pracach podkreśla znaczenie międzysektorowości. W przyszłości spodziewam się również dynamicznych zmian w ofercie edukacyjnej. Związek Banków Polskich współpracuje ze 120 uczelniami, w obszarach zarządzania, prawnego bezpieczeństwa, korzystania z baz danych czy informacji gospodarczych. Powstają podręczniki na ten temat, przeprowadzamy specjalne wykłady. Teraz wprowadzamy nowy moduł czyli cyberbezpieczeństwo.

Dziękuję za rozmowę.