aut. Ireneusz Piecuch 05.11.2018

CYFROWE PIENIĄDZE. (NIE)BEZPIECZNA PRZYSZŁOŚĆ? [ANALIZA]

Osoby zarządzające instytucjami finansowymi, a w zasadzie właściciele czy organy tych instytucji odpowiedzialne za ład korporacyjny, powinni przyzwyczajać się do myśli że cyberbezpieczeństwo dawno już przestało być wyłącznie domeną IT.

W połowie lat dziewięćdziesiątych, Bill Gates stwierdził, że usługi bankowe przetrwają, bo są niezbędne, ale ta sama zasada nie musi dotyczyć banków. Po upływie ponad dwudziestu lat banki dalej mają się nieźle i w dalszym ciągu tworzą fundament nowoczesnej gospodarki, jednakże rysy na ich pancerzu są coraz bardziej widoczne. Spośród ponad 3.5 miliarda użytkowników Internetu, coraz większa liczba dochodzi do wniosku, że tradycyjne usługi bankowe można w coraz łatwiejszy sposób zastąpić poprzez powstające jak grzyby po deszczu instytucje finansowe, realizujące wybrane funkcje bankowe za pomocą najnowszej technologii, ale bez zbędnych formalności, biurokracji i wizyt w oddziale. W jednym z przeprowadzonych badań wśród klientów młodego pokolenia dot. usług finansowych, ponad 70 procent respondentów odpowiedziało, że woleliby wizytę u dentysty niż odwiedziny w oddziale banku. Mimo to, wydaje się jednak, że Bill Gates nie miał do końca racji a oddział, coraz rzadziej jest synonimem banku. Aczkolwiek transformacja banków tradycyjnych do postaci czysto internetowej, nie jest ani łatwa, ani w niektórych przypadkach nawet możliwa. Na rynku powstają non stop nowe banki, działające wyłącznie w przestrzeni internetowej (niektóre z nich, jak Klarna, po przekształceniu z typowego fintechu) starając się łączyć w sobie łatwość i przystępność usług oferowanych przez fintech, bezpieczeństwo, jak również zaufanie będące domeną tradycyjnej bankowości. Zarówno jednak banki jak i nowi gracze na rynku usług finansowych muszą zmierzyć się z ciemną stroną lawinowo rosnącej penetracji Internetu – z cyberprzestępczością.

Czytaj też: KE zamierza utworzyć unijne laboratorium FinTech

Co ciekawe, wedle wielu zestawień, to nie banki (czy też szerzej instytucje finansowe), padają najczęściej ofiarą hackerów. Raport ERPScan obejmujący rok 2017 sytuuje sektor finansowy dopiero na trzeciej pozycji za branżą mediów i rozrywki, branżą informatyczną oraz administracją publiczną. Dziewięć procent wszystkich incydentów obejmuje banki (prawie połowa z tych incydentów), projekty związane z kryptowalutą (około 20%), firmy pożyczkowe (11%) oraz szereg innych podmiotów prowadzących działalność w innych obszarach tego sektora. Inne źródła, wskazują jednak na to, że to właśnie banki atakowane są kilkaset razy bardziej intensywnie niż inne podmioty. Nikt jednak nie jest zainteresowany upowszechnianiem tych danych. Spekuluje się, że nie więcej niż 15 procent incydentów jest ujawnianych publicznie, albowiem straty wizerunkowe mogą niejednokrotnie być równie bolesne jak straty finansowe. Niezależenie od tego, patrząc wyłącznie na rynek Wielkiej Brytanii, oraz biorąc pod uwagę tylko incydenty zgłoszone do Financial Conduct Authority (FCA), ostatnimi laty wyraźnie widać tendencję wzrostową. Jedynie w roku 2017, wzrost liczby incydentów wykrytych w sektorze kontrolowanym przez FCA, był o 80 procent większy niż w roku 2016.

Przyglądając się kilku największym, znanym przypadkom cyber-wpadek z udziałem instytucji finansowych warto zacząć od roku 2005 i CitiFinancial, firmy należącej do Citigroup. To właśnie w tej firmie, nośniki pamięci zawierające dane 3.9 miliona klientów ubiegających się o pożyczkę zniknęły po nadaniu ich ...jako przesyłki kurierskiej przez UPS.

Przejęcie strony serwisu CheckFree Corp. (2009) realizującego płatności on-line doprowadziło do tego, że ponad 5 milionów użytkowników tego serwisu zalogowało się na fałszywą stronę ujawniając dane pozwalające na dostęp do ich rachunków. Ponad 20 milionów klientów Korea Credit Bureau (2014) - czyli 40 procent mieszkańców Korei Południowej w tym czasie, zostało narażonych na utratę swoich danych po tym jak jeden z pracowników tej instytucji skopiował całą bazę danych i spokojnie wyniósł ja z biura. Warto dodać, że Korea Credit Bureau to spółka zajmująca się wykrywaniem nadużyć oraz pomocą w zarządzaniu ryzykiem.

W lutym 2016 roku, Amerykański Bank Rezerw Federalnych otrzymał od centralnego Banku Bangladeszu polecenia dokonania przelewów na łączną kwotę miliarda dolarów. Pięć z łącznej ilości 55 poleceń, zostało zrealizowanych na łączna kwotę 101 milionów dolarów. Pozostałe przelewy zostały zablokowane z uwagi na... błędy w poleceniach dokonania przelewów. Atak, dokonany przy wykorzystaniu programu Dridex, obnażył nie tylko braki w systemach informatycznych Banku Bangladeszu, ale także brak w owym czasie systemu antyfraudowego w Banku Rezerw Federalnych, który działałby w czasie rzeczywistym (transakcje sprawdzane były losowo już po dokonaniu przelewów). Pikanterii całej sytuacji dodaje fakt, że rok przed całym wydarzeniem, gubernator banku z Bangladeszu, zdając sobie sprawę ze słabości posiadanej infrastruktury, zatrudnił jedną z firm amerykańskich w celu zwiększenia odporności tych systemów na ataki cybernetyczne. Z uwagi na biurokrację i przewlekłe procesy wewnętrzne, firma ta mogła przystąpić do prac...dopiero po całym zdarzeniu.

Czytaj też: Wiceszef NSA: Korea Północna stoi za cyberatakiem na bank w Bangladeszu

W końcu ostatnie głośne wydarzenie z roku 2017. Utrata przez firmę Equifax danych ponad 147 milionów klientów, połączona ze wszczęciem przez SEC postępowania przeciwko byłemu już CEO, po tym jak sprzedał on swoje udziały w Equifax, zanim fakt dokonania ataku i utraty danych został podany do publicznej wiadomości (warto dodać, że akcje tej firmy na zakończenie kwartału w którym informacja stała się publiczna straciły ponad 20 procent swojej wartości). Aby uzyskać dostęp do danych hackerzy wykorzystali słabość jednego z systemów, przed którą kilka dni wcześniej przestrzegał US-CERT. Włamywacze spędzili 76 dni w systemach Equifax, zanim fakt naruszenia został odkryty. Od tamtej pory Equifax wydał ponad 200 milionów dolarów na poprawę zabezpieczenia swoich systemów, został ukarany karą 500 milionów funtów przez brytyjski FCA, a w Stanach Zjednoczonych pojawiły się pomysły uchwalenia specjalnej ustawy nakładającej na Equifax karę 1.5 miliarda dolarów.

Czytaj też: Chińczycy stoją za atakiem na Equifax? [KOMENTARZ]

John Chambers – zwykł mawiać, że istnieją jedynie dwa rodzaje przedsiębiorstw. Te które już odkryły, że stały się przedmiotem ataku ze strony cyberprzestępców oraz takie, które co prawda zostały zaatakowane, ale jeszcze o tym nie wiedzą. Banki oraz inne instytucje nie stanowią tu wyjątku, choć regulatorzy tego sektora od dawna przykładali ogromną wagę do zarzadzania ryzykiem operacyjnym, którego częścią składową stał się obecnie narastający problem cyberprzestępczości.

Pierwsza rekomendacja dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa

środowiska teleinformatycznego w bankach została wydana w formie uchwały Komisji Nadzoru Bankowego już grudniu 2002 roku i zastąpiona obecnie obowiązującą uchwałą w styczniu 2013 roku. Wprowadzenie ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz obowiązków z tym związanych, a w szczególności obowiązku zarządzania ryzykiem związanym z systemami teleinformatycznymi nie powinno być zatem niczym nowym dla sektora poddanego nadzorowi KNF. Niedawny atak na systemy KNF pokazuje jednak, że regulacje i świadomość to jedno, a szybko zmieniająca się rzeczywistości oraz konieczność stałego, konsekwentnego inwestowania w systemy, edukację oraz odpowiednie zasoby eksperckie to już zupełnie inna bajka. Po jednej stronie mamy bowiem rosnący rynek usług i produktów związanych ze zwiększaniem odporności na ataki hackerskie oceniany na ponad 100 miliardów dolarów, a z drugiej zorganizowane grupy przestępcze wydające niemalże dziesięć razy więcej.

Czytaj też: Karol Okoński: Ustawa o krajowym systemie cyberbezpieczeństwa to znaczący krok naprzód [WYWIAD]

Willie Sutton, amerykański przestępca, który upodobał sobie sektor bankowy, co z jednej strony wzbogaciło go o 2 miliony dolarów, a z drugiej strony kosztowało niemal połowę dorosłego życia spędzoną za kratkami, na pytanie dlaczego napada na banki, miał ponoć odpowiedzieć, że dlatego, że to tam właśnie są pieniądze. Instytucje finansowe, w tym banki, są i będą jednym z ulubionych celów ataków nie tylko dlatego, że „tam są pieniądze“, ale także dlatego, że instytucje te dysponują walutą XXI wieku - danymi klientów. Zagrożenie ze strony cyberprzestępców jest niewątpliwie jednym z ryzyk operacyjnych, ale stawianie go na równi z innymi ryzykami może okazać się ryzykiem samym w sobie. Przypadek centralnego banku Bangladeszu czy też firmy Equifax pokazuje, że brak odpowiednich działań oraz inwestycji prowadzonych w tym zakresie może powodować skutki trudne do odwrócenia.

Wydaje się zatem, że osoby zarządzające instytucjami finansowymi, a w zasadzie właściciele czy organy tych instytucji odpowiedzialne za ład korporacyjny, powinni przyzwyczajać się do myśli że cyberbezpieczeństwo dawno już przestało być wyłącznie domeną IT. Rozwój nowych produktów i transformacja cyfrowa pozwalająca na konkurowanie z coraz szerszą masą pretendentów do schedy po tradycyjnym sektorze finansowym oraz inwestycje w budowanie odporności organizacji na cyberataki, to dwie strony tej samej monety, której szefowie banków oraz innych finansowych tuzów, nie powinni wypuszczać z rąk.