aut. Andrzej Kozłowski 02.04.2019

BEZPIECZEŃSTWO JEST INTEGRALNĄ CZĘŚCIĄ REVOLUT [WYWIAD]

„Naszym atutem jest to, że jesteśmy młodą firmą i bezpieczeństwo od samego początku było integralną częścią kultury naszej organizacji" – mówi w rozmowie z CyberDefence24.pl Paul Heffernan, szef cyberbezpieczeństwa w Revolut.

Z jakimi zagrożeniami musi się obecnie mierzyć sektor finansowy?

Prezentowane co roku na Forum Ekonomicznym w Davos badanie Global Risk Report wskazuje kluczowe wyzwania w obszarze bezpieczeństwa. Za jedno z najważniejszych w tegorocznej i zeszłorocznej edycji uznano cyberataki. Znalazły się one, obok kradzieży danych, w piątce ryzyk o największym prawdopodobieństwie wystąpienia. Jest to poważne wyzwanie dla firm i rządów. Sektor bankowy zawsze był narażony na cyberataki, ponieważ tutaj są pieniądze.

Prawda, ale banki posiadają również najlepsze zabezpieczenia.

Branża finansowa dba o bezpieczeństwo. Dla tradycyjnych usługodawców jest to jednak wyzwanie, ponieważ posiadają skomplikowaną, monolityczną strukturę. Sytuacja z Revolut wygląda inaczej. Narodziliśmy się w chmurze. Wiele organizacji rozważa dziś przeniesienie się do chmury. My byliśmy w niej od pierwszego dnia funkcjonowania firmy. Tradycyjne instytucje finansowe muszą zabezpieczyć własną infrastrukturę informatyczną. My tego problemu nie mamy, bo operujemy w chmurze. Warto dodać, że dane przechowujemy na terenie UE i podlegamy pod GDPR.

Jakie są specyficzne zagrożenia, z którymi Wy musicie sobie poradzić?

Powiedziałbym, że obecnie nie występują jakieś zagrożenia specyficzne dla Revolut. Inwestujemy wiele czasu i pieniędzy aby nasza aplikacja mobilna była jak najbardziej bezpieczna. Realizujemy też testy penetracyjne, żeby upewnić się, że nasze systemy są właściwie chronione.

Wiąże się to jednak z ingerencją w smartfony użytkowników?

Testy penetracyjne robimy tylko na naszych systemach. O bezpieczeństwo smartfona musi dbać również właściciel. Warto pamiętać, że poziom profesjonalizacji grup cyber-przestępczych cały czas rośnie. Jest coraz więcej kradzieży loginów i haseł, które następnie odsprzedawane są w Darknecie. Funkcjonuje to trochę jak ebay, gdzie sprzedawcy otrzymują oceny i feedback. Wielu ze sprzedających gwarantuje jakość usługi. Jeżeli kradzione loginy i hasła, którymi handlują nie zadziałają, można otrzymać zwrot pieniędzy.

To zagrożenia, z którymi musi się dzisiaj zmierzyć sektor finansowy. Niezależnie czy mówimy tutaj o Revolut, fintechach czy bankach. Dlatego współpracujemy z tzw. etycznymi hakerami, którzy pracują na wyłączność dla Revolut. Ich praca polega na testowaniu zabezpieczeń naszej aplikacji. Ponadto,

sprawdzają w Darknecie czy nie ma tam danych naszych klientów, by udaremnić ich wykorzystanie w niecnym celu.

Jakie narzędzia wykorzystują etyczni hakerzy w celu przeszukiwania Darknetu?

To nie jest łatwe, bo nie ma gotowych narzędzi, które pozwalają na przeczesywanie Darknetu. Zatrudniamy ekspertów, którzy tworzą dla nas wyspecjalizowane narzędzia umożliwiające prowadzenie takich działań.

Jakie zagrożenia widzicie w coraz powszechniejszych fraudach?

W Darknecie można znaleźć, wiele skradzionych kont bankowych, które następnie okazują się fałszywe. Handlarze często sprzedają nieprawdziwe informacje, loginy i hasła. Staramy się to wyśledzić i dowiedzieć, czy dane, które sprzedają o rzekomych klientach Revolut są prawdziwe.

Przykładamy wagę do tego, by bezpieczeństwo towarzyszyło nam od projektowania nowej usługi do jej oferowania. By było pierwszym etapem procesu, nie końcowym. Ma to wpływ na zaufanie użytkowników. Klienci wybierają produkty i usługi ze źródeł, którym ufają.

W jaki sposób Revolut dba o bezpieczeństwo swoich klientów?

Konto Revolut umożliwia zmianę funkcji bezpieczeństwa karty w czasie rzeczywistym i pozwala zablokować możliwość, przykładowo, wypłacania pieniędzy z bankomatu. Kolejna funkcja bezpieczeństwa wiąże się z geolokalizacją. Umożliwia zlokalizowanie transakcji kartą i porównanie czy użytkownik faktycznie przebywa z telefonem w jej pobliżu. Jeśli tak nie jest transakcja jest blokowana.

Mamy również opcję zabezpieczenia w postaci karty wirtualnej. Ludzie uwielbiają kupować produkty w Internecie. Wiemy jednak, że zdarzają się wycieki danych kart kredytowych klientów na masową skalę, jak w przypadku sieci hoteli Marriott czy linii lotniczych British Airways. Organizacje często nie wiedzą co dokładnie wyciekło. Gdy hakerzy instalują po cichu złośliwy kod przy bramkach płatności, aby w ten sposób wykraść dane, proceder często trwa niezauważony.

Bywa, że klienci nawet nie wiedzą, że padli ofiarą oszustów. Dlatego, dajemy naszym użytkownikom opcję wygenerowania jednorazowej karty wirtualnej osobno dla każdej transakcji, którą klient zamierza przeprowadzić. Na przykład, mam obecnie w aplikacji jedną z kart wirtualnych, której dane wpisuję do transakcji. Gdy transakcja przechodzi, stare dane karty są usuwane, a na ich miejsce generowane są nowe.

W jaki sposób przeciwdziałacie wyciekom danych, które mogą dotknąć klientów Revolut?

Monitorujemy informacje o wyciekach danych z innych firm. Wiele instytucji ucierpiało już z tego powodu. Staramy się monitorować te zdarzenia. Jednym z przykładów była kradzież informacji o klientach linii lotniczej Cathay Pacific. Udało nam się znaleźć wszystkich klientów, którzy używali karty Revolut do płatności w Cathay Pacific i poinformować ich, że dane dotyczące płatności (payment data) zostały skradzione w wyniku cyberataku. Zaproponowaliśmy im nasze jednorazowe karty wirtualne oraz dostarczenie nowych fizycznych kart Revolut.

Zastanawiamy się również nad możliwością wprowadzenia systemu monitorowania danych klientów, aby ostrzec ich na czas gdyby te dane pojawiły się w Darkwebie. Staramy się uczyć naszych programistów zasad bezpiecznego programowania i uczulać ich na cyberzagrożenia. Dążymy do tego, aby bezpieczeństwo towarzyszyło naszym produktom już na etapu projektowania, od pierwszej linijki kodu.

Jak przeprowadzane są audyty bezpieczeństwa?

Jesteśmy cyklicznie poddawani audytom bezpieczeństwa przeprowadzanym przez brytyjskiego regulatora, ale też naszych partnerów takich jak Visa czy MasterCard. W najbliższym czasie spodziewamy się kolejnego takiego audytu. Zewnętrzni partnerzy realizują ponadto testy penetracyjne naszych systemów. Odbywamy również wiele spotkań z deweloperami, staramy się dzielić naszą wiedzą o tym jak bezpiecznie pisać aplikacje i sprawdzać bezpieczeństwo kodu.

Zapewnienie bezpieczeństwa to również współpraca z innymi instytucjami.

Tak, dlatego m.in. organizujemy hackathon dla deweloperów. W przyszłości chcemy poszerzyć tę inicjatywę i skupić się nie tylko na bezpieczeństwie produktów Revolut, ale również na tym, żeby zwiększyć naszą wiedzę i dzielić się nią ze społecznością. Uważamy, że współpraca z innymi fintechami oraz bankami jest bardzo ważna, ponieważ zagrożenia z którymi walczymy są globalne. Budujemy nasze wspólne bezpieczeństwo wymieniając się wiedzą i informacjami.

Naszym atutem jest również to, że jesteśmy młodą instytucją, od samego początku bezpieczeństwo było integralną częścią kultury naszej organizacji. W tradycyjnych instytucjach zostało dodane później, przez co niekiedy wciąż traktowane jest jako element “na doczepkę” i spychane na koniec procesu.

W jaki sposób wykorzystujecie uczenie maszynowe i sztuczną inteligencję do walki z zagrożeniami?

Wykorzystujemy AI do oceny czy transakcje są uczciwe. Używamy systemu, który obserwuje transakcje i bada czy nie zachodzi żadne podejrzane zachowanie mogące wskazywać, że mamy do czynienia z fraudem. Jest wiele czynników, które mogą na to wskazywać jak np. dziwna lokalizacja, w której użytkownik karty nigdy wcześniej nie był. Szukamy wszystkich sygnałów zachowań, które wykraczają poza pewien schemat. Jeśli dostrzeżemy anomalię, wysyłamy użytkownikom zapytanie, czy dana transakcja miała miejsce i czy to on był jej autorem. Jeśli odpowiedź jest negatywna, automatycznie blokujemy transakcję i dokonujemy tzw. charge back. Używamy AI do ochrony klientów przed fraudami.

Czy zanotowaliście jakiś atak, który zakończył się sukcesem przeciwko Waszej firmie?

Nie odnotowaliśmy żadnego takiego incydentu, ale wychodzimy z założenia, że musimy być przygotowani na najgorsze. Uważamy, że w obecnym świecie zagrożeń w cyberprzestrzeni to raczej kwestia czasu kiedy do takiego ataku dojdzie, a nie czy do niego dojdzie. Dlatego, staramy się jak najlepiej do tych wyzwań przygotować. Szyfrujemy wszystkie dane. Są one chronione zgodnie z dyrektywą GDPR i nie są one przechowywane poza Unię Europejską. W ćwiczeniach symulujących cyberataki i reakcje na nie angażujemy wszystkich pracowników. Testujemy naszą reakcję na incydenty, uczymy się mitygować skutki ataków oraz komunikować o takich próbach klientom. Wszystkie te działania powodują, że szansę na kradzież informacji przez przestępców jest znacznie mniejsza.

W jaki sposób chronicie dane swoich klientów? Umieszczacie je w chmurze Google?

Tak. Są one przechowywane w zaszyfrowanej formie. Korzystając z chmury Google mamy pewność, że zawsze nasze usługi są dostępne. Wielu cyberprzestępców dąży do tego, żeby przerwać działalność biznesową. Przynosi to firmom ogromne straty. Google Cloud zapewnia ochronę przed takim zagrożeniem na poziomie globalnym, ale też oferuje wiele narzędzi bezpieczeństwa. Pamiętajmy, ile środków finansowych Google przeznacza na bezpieczeństwo.

Macie również rejestr transakcji w czasie rzeczywistym, który można zaobserwować na

Państwa stronie. Jak długo trzymacie informacje o nich?

Przechowujemy informacje o transakcjach zrealizowanych w Unii Europejskiej, oraz poza Europą. Dzięki mapie rejestrującej transakcje, widzimy, gdzie nasi użytkownicy podróżują i gdzie płacą. Na mapie dane są zanonimizowane. Dane przechowujemy zgodnie z wymaganiami brytyjskiego regulatora i europejskimi regulacjami GDPR.

Prawo pozwala również na dostęp do przechowywanych przez Was danych odpowiednim służbom, jeżeli wykryją one podejrzaną transakcję?

Muszą oczywiście złożyć odpowiedni wniosek o taki dostęp i to sąd decyduje czy im taki dostęp przyzna czy nie. W Londynie mamy zespół prawników, który zajmuje się takimi sprawami.

Revolut został założony w 2015 roku w stolicy Wielkiej Brytanii - Londynie. Jego założyciele jeździli po całym świecie, płacąc wysokie opłaty za konwersję walut zagranicznych i przesyłanie pieniędzy między państwami. Sytuacja ta doprowadziła do stworzenia koncepcji Revolut, który został wsparty m.in. przez MasterCard i Barclays. Revolut ma ambicję stać się usługą bankową o światowym zasięgu, która jest dostępna dla każdego zainteresowanego. Założenie konta zajmuje 3 minuty. Ściągnięcie aplikacji mobilnej wymaga rejestracji i zrobienia zdjęcia dowodu osobistego lub paszportu oraz uzupełnienia o dane karty debetowej.

Na aplikacji możesz zobaczyć liczbę pieniędzy na koncie, miejsce ostatniej transakcji oraz kategorię zrobionych zakupów. Te wszystkie informacje dostępne są w czasie rzeczywistym. Dodanie pieniędzy jest również banalnie proste, dzieje się to dzięki transferowi z karty bankowej. Revolut umożliwia posiadanie w swojej aplikacji 29 różnych walut, w tym 5 kryptowalut. Na całym świecie możesz wydawać pieniądze bez prowizji w ponad 150 walutach. Przykładowo posiadając polskie złote na koncie Revolut można zapłacić bez prowizji w 150 walutach na całym świecie. Konwersja przebiega na podstawie bieżącego kursu międzybankowego. Mając polskie złote można jechać np. do Turkmenistanu i robić zakupy przy pomocy karty Revolut lub wyciągnąć miejscową gotówkę bez konieczności ponoszenia wysokich opłat za przewalutowanie. Czasami jednak może się zdarzyć, że miejscowe bankomaty, banki lub terminale mogą pobrać prowizje.

Obecnie Revolut ma blisko 4,5 miliona użytkowników w Europie, w Polsce jest ich 370 tys. Polska jest trzecim największym państwem w Europie pod względem ilości klientów. Tylko we Francji i Wielkiej Brytanii jest ich więcej. Revolut współpracuje z kartami MasterCard i Visa. W Polsce jest już możliwość płacenia z Google Pay. Nie jest to oficjalne, ale można płacić z pomocą Garmin Pay. Pracujemy obecnie nad możliwością zapłaty za pomocą Apple Pay. W takich przypadkach nie potrzeba karty. W przypadku zakupów online, też nie ma potrzeby używania karty. Wystarczy tylko karta wirtualna w aplikacji standardowa lub jednorazowa ze zmiennym numerem.