Wzmożona ostrożność nie powinna zaskakiwać. Jak wskazują dane Check Point Research, w zeszłym roku sektor bankowy doświadczył 50 proc. wzrostu ataków, natomiast w styczniu przeciętna polska organizacja z sektora finansowego przeżyła ok. 960 prób cyberataków w tygodniu!

Sektor bankowy już przed pandemią i wojną był znacznie lepiej niż inne branże przygotowany do wykrywania i odpierania cyberataków

BANKI W AWANGARDZIE

Nic dziwnego, że to właśnie sektor bankowy stał się dziś awangardą działań w dotyczących cyberbezpieczeństwa. Powód? Sektor bankowy już przed pandemią i wojną był znacznie lepiej niż inne sektory przygotowany do wykrywania i odpierania cyberataków. Polskie banki ściśle współpracują ze sobą w tym zakresie, a nad wszystkim czuwa zarówno Związek Banków Polskich, jak i KNF. Gdy tylko dochodzi do ataku na którąś z instytucji, reszta partnerów natychmiast dowiaduje się o tym i uruchamia procedury mające zablokować możliwość rozprzestrzeniania się zagrożenia.

– Jako instytucje zaufania publicznego łączymy siły, od kilku lat koordynując wspólne międzybankowe akcje, często z inicjatywy Związku Banków Polskich – przyznaje Daria Pawęda, dyrektor Departamentu Rozwoju Biznesu i Obsługi Klienta w Volkswagen Bank GmbH Oddział w Polsce. I dodaje, że edukacja na temat cyberbezpieczeństwa jest ukierunkowana na podnoszenie poziomu wiedzy o cyberprzestępczości i kształtowaniu właściwych postaw w kanałach cyfrowych. – Warto wspomnieć też o szerokiej aktywności instytucji europejskich. Październik był Europejskim Miesiącem Cyberbezpieczeństwa (European Cybersecurity Month – ECSM). To coroczna, ogólnoeuropejska kampania Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) z inicjatywy Komisji Europejskiej. W tegorocznej edycji hasłem przewodnim było „Pomyśl, zanim klikniesz" (Think Before You Click). Powinniśmy o tym pamiętać przy każdej okazji – apeluje Pawęda.

W ślad za wyzwaniami, jakie niosą trudne czasy, banki przygotowują ofertę, która wspiera przedsiębiorców w bezpiecznym prowadzeniu firmy. Przykładem jest Volkswagen Bank działający w ramach Volkswagen Financial Services. – Konsekwentnie wprowadzamy liczne innowacje – podkreśla Daria Pawęda. Jedną z nich jest digitalizacja rachunku. – Proces zakładania konta będzie odbywać się w pełni online, bez potrzeby oczekiwania na kuriera, co znacznie skróci czas realizacji – podkreśla Daria Pawęda. Podobny proces bank wdrożył w kredycie gotówkowym, gdzie identyfikacja tożsamości jest przeprowadzana automatycznie za pomocą algorytmów identyfikujących cechy biometryczne. – W procesie KYC wystarczy nagrać krótkie wideo przedstawiające twarz, aby porównać je automatycznie ze zdjęciem z dowodu tożsamości. Kolejnym etapem rozwoju oferty naszych kont detalicznych będzie wdrożenie tokenizacji, czyli usług typu Apple Pay, Google Pay czy Blik, które są powszechne na rynku i bardzo chętnie używane przez Polaków – zapowiada Daria Pawęda z Volkswagen Bank.

Ponadto bank proponuje przedsiębiorcom konto bieżące wraz z kartą Visa

EKSPERT

Grzegorz Waszkiewicz
broker ubezpieczeniowy, członek zarządu Krajowego Biura Obsługi Roszczeń Ubezpieczeniowych, twórca portalu: BezpieczenstwowBiznesie.pl

JAK OGRANICZYĆ KONSEKWENCJE CYBERATAKU

Czy można uniknąć ataku hakera? Nie sposób go wyeliminować, ale można sprawić, że możliwości „włamania" będą ograniczone, a ewentualne konsekwencje skutecznego ataku będą finansowo zminimalizowane.

Jak to zrobić? Pomyśleć o zarządzeniu ryzykiem poprzez zakup cyberubezpieczenia. To proces, a nie sam zakup. Przede wszystkim już sama analiza ofert towarzystw i ich wymagań pozwala wychwycić braki i niedociągnięcia w wewnętrznych regulaminach, sprzęcie i oprogramowaniu.

Trzeba sobie uświadomić, że dziś każda firma może być celem ataku hakerskiego prowadzącego w skutkach do usunięcia, pobrania, zmiany, zniszczenia, zmodyfikowania danych i informacji. Dzieje się to niestety najczęściej przez błąd ludzki, czyli niewłaściwe zachowanie pracownika lub błąd dostawcy oprogramowania.

Właściciele lub zarządzający powinni zatem nie tylko siebie zabezpieczyć przed cyberszantażem, ale też chronić dane swoich klientów i przewidzieć wynikające z tego roszczenia od osób trzecich lub państwowych regulatorów. A są to wysokie odszkodowania, zadośćuczynienia, kary administracyjne i grzywny.

Poza odpowiednimi zabezpieczeniami sieci informatycznej powinniśmy zatem wyposażyć się w odpowiednią tarczę finansową, czyli polisę ubezpieczeniową. W razie ewentualnego ataku ubezpieczyciel pokryje koszty ekspertów ds. informatyki śledczej, odzyskiwania danych, prawników oraz konsultantów PR, czyli specjalistów, którzy doradzą i opracują odpowiedni plan działania w sytuacji kryzysowej. Analizując atak na bieżąco, ubezpieczyciel może nawet podjąć szybko decyzję o zapłacie okupu, aby uniknąć znacznie kosztowniejszych skutków w postaci odszkodowań związanych np. z naruszeniem prywatności, utratą dokumentów, naruszeniem poufności informacji i bezpieczeństwa płatności czy wręcz zatrzymaniem działalności operacyjnej firmy w przypadku coraz częściej stosowanego internetu rzeczy *Internet of Things* – IoT).

FOT. MATERIAŁY PRASOWE