# 5 największych problemów firm z sektora bankowego, o których jeszcze nie wiedzą

**Systemy bankowe są nieustannie wystawione na ryzyko związane z atakami cybernetycznymi. Cyberprzestępcy wykorzystują nowoczesne technologie do próby uzyskania dostępu do zasobów finansowych instytucji. Wiele informacji na temat największych zagrożeń dla sektora bankowego dostarcza raport Cyfrowa Twierdza[[1]](#footnote-1) przygotowany przez Centrum Procesów Bankowych i Informacji oraz raport Cyberzagrożenia w sektorze finansowym 2022[[2]](#footnote-2) przygotowany przez Komisję Nadzoru Finansowego. Czego mogą się spodziewać przedstawiciele sektora bankowego i jak mogą chronić się przez zautomatyzowanymi atakami? Oto 5 największych problemów, z jakimi przyjdzie się zmierzyć.**

## **Ataki hakerskie na klientów banków**

Według raportu Cyberzagrożenia w sektorze finansowym 2022 w 2022 roku najczęściej stosowaną metodą kradzieży środków finansowych użytkowników był phishing realizowany przy użyciu SMS-ów. Oszuści podszywali się pod znane banki w celu wyłudzenia loginów i haseł użytkowników oraz danych do ich kart płatniczych. W tym przypadku na celownik cyberprzestępcy wzięli pojedynczych użytkowników. Nierzadko jednak ich metody mają na celu sparaliżowanie pracy całego systemu bankowego.

Cyberprzestępcy polują także na słabe punkty mniejszych dostawców usług IT, próbując w ten sposób zyskać dostęp do sieci dużych banków. Aby temu zapobiec, Unia Europejska uchwaliła rozporządzenie DORA akcentujące problem ryzyka podmiotów trzecich współpracujących z instytucjami finansowymi.

## **Żądanie okupu w sieci**

Za najniebezpieczniejszy rodzaj cyberataków uznaje się ransomware czyli rodzaj złośliwego oprogramowania blokującego dostęp do danych lub systemu komputerowego. Cyberprzestępcy szyfrują dane, a następnie żądają okupu w zamian za przywrócenie dostępu do plików. Według firmy badawczej Gartner w ciągu ostatnich 2 lat 73% firm doświadczyło prób ataku tego typu, a aż 63% z tych firm stwierdziło, że napastnicy mieli dostęp do ich zasobów co najmniej 6 miesięcy przed wykryciem ataku.

– *W takich przypadkach istotne jest posiadanie rozwiązań umożliwiających automatyzację reagowania na incydenty bezpieczeństwa. W Simplicity implementujemy u naszych klientów zestaw zróżnicowanych mechanizmów, urządzeń i praktyk, których zadaniem jest minimalizowanie ryzyka oraz ochrona wrażliwych zasobów. Przykładem takiego rozwiązania jest Next Generation Firewall (NGFW) łączący tradycyjne funkcje firewalla z dodatkowymi funkcjami takimi jak filtracja treści, głęboka inspekcja (deep packet inspection) , detekcja i zapobieganie intruzom (IDS/IPS), kontrola aplikacji oraz analiza ruchu sieciowego. Zapewnia to skuteczną ochronę sieci przed współczesnymi zagrożeniami* – wyjaśnia Magda Frątczak, Director of Sales & Presales w Simplicity sp. z o.o.

## **Luki w zabezpieczeniach chmury**

Raport Cyfrowa Twierdza podaje luki w zabezpieczeniach chmury jako jedno z największych zagrożeń bezpieczeństwa cyfrowego banków. Rozwiązania chmurowe znacznie usprawniają procesy operacyjne, jednak migracja danych wiąże się z ryzykiem, zwłaszcza w przypadku nieprawidłowej konfiguracji narzędzi bezpieczeństwa. Szczególnie wrażliwymi obszarami w zakresie bezpieczeństwa usług chmurowych jest ochrona danych, profesjonalne zarządzanie środowiskiem chmurowym oraz zgodność z przepisami i regulacjami.

– *W Simplicity dbamy o dane przechowywanie zarówno lokalnie, jak i w chmurze publicznej czy hybrydowej. Projektujemy i wdrażamy kompleksowe systemy bezpieczeństwa usług i danych w chmurze wykorzystując Cloud Access Security Broker – nowoczesny broker zabezpieczeń uzupełniający funkcjonujące już zapory bezpieczeństwa, takie jak wspomniane wcześniej NGFW, systemy ochrony przed wyciekami informacji DLP, systemy kontroli tożsamości jako usługi IDaaS, zapory sieciowe aplikacji i inne. Uwagi wymagają również tak popularne rozwiązania jak Microsoft Office 365, dlatego wielokrotnie pomagaliśmy zabezpieczać takie usługi, a także tworzyć adekwatne polityki bezpieczeństwa oraz konfigurować płatne plany usługi Microsoft Defender* – wyjaśnia ekspertka Simplicity sp. z o.o.

## **Zbyt niski budżet na działania związane z cyberbezpieczeństwem**

Raport Cyfrowa Twierdza za jedno z potencjalnych w sektorze bankowym zagrożeń wymienia nieadekwatny do potrzeb i ekspozycji na ryzyko budżet na cyberbezpieczeństwo. Wiele wskazuje na to, że przedstawiciele sektora bankowego muszą poszerzyć swoją świadomość na temat budowania bezpiecznego ekosystemu bankowego odpornego na zagrożenia cybernetyczne.

## **Utrata reputacji instytucji finansowych**

Nawet najdrobniejsze działania prowadzone przez cyberprzestępców sukcesywnie obniżają reputację banków. Raport Cyberzagrożenia w sektorze finansowym 2022 omawia fałszywe reklamy inwestycyjne wykorzystujące wizerunek wiarygodnych instytucji finansowych do wykradania danych użytkowników. Ważnym działaniem ze strony banków powinno więc być stałe prowadzenie kampanii uświadamiających klientów na temat manipulacji, jakich dopuszczają się cyberprzestępcy oraz środków bezpieczeństwa, które można podjąć w przypadku podejrzenia oszustwa.

Kontakt dla mediów:

Małgorzata Knapik-Klata

PR Manager

tel. 509 986 984

e-mail: m.knapik-klata@commplace.com.pl

1. https://bank.pl/wp-content/uploads/2023/12/Raport-Cyfrowa-Twierdza.pdf [↑](#footnote-ref-1)
2. https://cebrf.knf.gov.pl/images/Cyberzagroenia\_w\_sektorze\_finansowym\_2022.pdf [↑](#footnote-ref-2)