**Polski sektor finansowy i bank centralny w stanie gotowości cybernetycznej**

**Europejski sektor finansowy pozostaje głównym celem ataków cybernetycznych. Raport „Threat Landscape 2024” Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) ostrzega przed nasilającymi się atakami na banki, firmy ubezpieczeniowe i dostawców usług finansowych. Według danych Check Point Research, organizacje finansowe odnotowały w 2024 roku 30% wzrost cyberataków i średnio na świecie były atakowane 1 500 razy tygodniowo. Banki w Polsce znajdują się na czołowej liście celów cybernetycznych z przeciętną liczbą 1 850 ataków w 2025 roku.**

Według Wojciecha Głażewskiego, dyrektora zarządzającego izraelskiej firmy specjalizującej się w bezpieczeństwie sieciowym Check Point Software Technologies w Polsce, sektor finansowy stanowi kręgosłup światowej gospodarki, co czyni go jednym z najbardziej narażonych na ataki cybernetyczne.

- *W miarę jak bankowość internetowa, transakcje mobilne i innowacje fintechowe czy AI się rozwijają, zagrożenia cybernetyczne również się ewoluują. Cyberprzestępcy nieustannie wykorzystują luki w aplikacjach finansowych, co sprawia, że silne środki bezpieczeństwa są niezbędne do ochrony wrażliwych danych klientów, transakcji i operacji biznesowych –* ostrzega Wojciech Głażewski z Check Point Software Technologies.

Dowodem na to jest analiza raportu Check Point Security Report 2025, która wskazuje na 30% wzrost liczby cyberataków na sektor finansowy w 2024 roku, z średnią liczbą 1 510 ataków tygodniowo na całym świecie*. - Polska odnotowała ostatnio liczbę incydentów wyższą niż średnia światowa, z ponad 1 850 atakami tygodniowo na ten sektor* – dodaje Głażewski.

W 2024 roku Polska doświadczyła największej liczby cyberataków na świecie. Według Ministerstwa Cyfryzacji, Polska odnotowała ponad 1 000 cyberataków tygodniowo w 2024 roku. Raport firmy Check Point Research wskazuje na wyższą ilość ataków…. Polska doświadcza średnio ponad 1 500 ataków na organizację tygodniowo, a sektory strategiczne ponad 2 000. **Sektor finansowy w Polsce jest celem 1 859 ataków co tydzień – wynika z danych Check Point Research.**

W ciągu ostatnich dwóch dekad organizacje z sektora finansowego padły ofiarą ponad 20 000 cyberataków, które spowodowały straty przekraczające 12 miliardów USD, jak podaje SecurityWeek, powołując się na dane Międzynarodowego Funduszu Walutowego. Te incydenty wiążą się również z pośrednimi stratami, takimi jak uszczerbki na reputacji czy dodatkowe koszty związane z wzmocnieniem środków bezpieczeństwa. Szacuje się, że organizacje finansowe są celem około jednej piątej wszystkich cyberataków. Jeśli skutki ataku dotkną lub mogą dotknąć klientów, ujawnienie tych informacji jest wymagane przez prawo.

Od ataków typu Distributed Denial-of-Service (DDoS), nasilenie których wywołane zostało konfliktami geopolitycznymi, po oszustwa internetowe i ataki na łańcuchy dostaw, zagrożenia cybernetyczne stają się coraz bardziej wyrafinowane. Przestępcy wykorzystują luki w zabezpieczeniach, aby uzyskać dostęp i sprzedać wrażliwe dane, podczas gdy schematy oszustw internetowych stają się coraz bardziej zaawansowane. Poza widocznymi atakami, takimi jak ransomware, które blokuje dostęp do danych w zamian za okupy, coraz częściej wykorzystywane są subtelniejsze metody, takie jak phishing i inżynieria społeczna. Kampanie smishing i vishing wprowadzają użytkowników w błąd, nakłaniając ich do podania krytycznych informacji finansowych, podczas gdy oszustwa związane z kryptowalutami stają się coraz powszechniejsze.

**W obliczu rosnących wyzwań związanych z cyberbezpieczeństwem, Unia Europejska nasila wysiłki na rzecz poprawy koordynacji wśród swoich państw członkowskich, aby chronić krytyczną infrastrukturę i wzmocnić suwerenność technologiczną**. W tym kontekście polska prezydencja w Radzie UE zwołała na 5 marca br. spotkanie europejskich ministrów ds. cyfryzacji, aby ocenić odporność cybernetyczną Unii. Nieformalne spotkanie, które odbyło się w Warszawie, zakończyło się ogłoszeniem „*Warszawskiego Apelu”,*wzywającego państwa członkowskie do wzmocnienia współpracy w zarządzaniu kryzysami cybernetycznymi i finalizacji *„Planów UE dotyczących zarządzania kryzysowego w zakresie cyberbezpieczeństwa*”. Ministrowie podkreślili potrzebę stworzenia strategii walki z cyberatakami. Podkreślili również znaczenie wzmocnienia współpracy UE-NATO, szczególnie w kontekście zagrożeń bezpieczeństwa zaostrzonych przez inwazję Rosji na Ukrainę.

**Ponadto, Polska zwróciła się (w ramach krajowej polityki odporności na cyberzagrożenia) do Europejskiego Banku Centralnego o opinię** **na temat projektu ustawy nowelizującej ustawę o krajowym systemie cyberbezpieczeństwa** (18.11.2024) oraz wytycznych bezpieczeństwa dla państwowego Narodowego Banku Polskiego (NBP), instytucji finansowych oraz systemów płatniczych i rozrachunkowych. **W odpowiedzi na prośbę Christine Lagarde, prezes EBC, napisała, że EBC sugeruje, aby odpowiednie umowy o współpracy i wymianie informacji zostały ustanowione pomiędzy Ministrem ds. Cyfryzacji a EBC, za pośrednictwem NBP, w celu zapewnienia ogólnej funkcjonalności krajowego systemu bezpieczeństwa.**

**Banki centralne na celowniku hakerów**

Zgodnie z raportem „*ENISA Threat Landscape 2024”* najbardziej atakowanymi sektorami gospodarki są administracja publiczna, transport oraz sektor bankowy/finansowy. W związku z tym, nie tylko instytucje finansowe, ale także **banki centralne są narażone na ataki.**Wynika to z różnych powodów.

Banki centralne pełnią kluczową rolę w gospodarce. Są one „kopalnią wiedzy” dla hakerów, ponieważ stanowią istotny element krytycznej infrastruktury finansowej. Są to unikalne instytucje publiczne, a większość ich funkcji nie może zostać zastąpiona. Posiadają monopol na emisję pieniędzy, odpowiadają za politykę monetarną, stabilność finansową, nadzór nad systemami płatniczymi i rozrachunkiem papierów wartościowych, prowadzą operacje wymiany walutowej, zarządzają rezerwami oficjalnymi i wspierają zarządzanie finansami państwa. Banki centralne są swoistymi „centralnymi węzłami” w sieci połączeń z bankami komercyjnymi. Posiadają również ogromne ilości poufnych danych finansowych, co czyni je atrakcyjnymi celami dla hakerów. Hakerzy mogą koncentrować się na konkretnych obszarach działalności banku centralnego, a znaczące zakłócenie jego codziennej działalności (i publiczne ujawnienie tego) może zostać uznane przez hakerów za miarę sukcesu ataku. Najczęściej wykorzystywanym narzędziem w tych atakach były dotychczas ataki DDoS, skierowane na strony internetowe i serwery banków centralnych poprzez zakłócanie usług sieciowych. Tego rodzaju ataki są stosunkowo mniej skomplikowane i łatwe do przeprowadzenia, chociaż nie powodują dużych strat. Warto wspomnieć, że ataki DDoS były przeprowadzane już na banki takie jak Riksbank, Bank Izraela, Bank Norwegii, Narodowy Bank Belgii, Czechy Narodowy Bank, Bank Słowenii oraz Centralny Bank Rosji.

**Cyberataki na europejskie banki – ENISA**

Między styczniem 2023 a czerwcem 2024 roku zagrożenia cybernetyczne skierowane w sektor finansowy Europy eskalowały, stanowiąc zagrożenie dla banków, dostawców usług finansowych i organów regulacyjnych. Zgodnie z raportem ENISA Threat Landscape: Finance Sector, sektor finansowy stanął w obliczu 488 publicznie zgłoszonych incydentów cybernetycznych, z bankami, publicznymi instytucjami finansowymi oraz indywidualnymi klientami wśród najbardziej dotkniętych. Raport wskazuje na ataki DDoS, wycieki danych, inżynierię społeczną, oszustwa, ransomware, ataki na łańcuch dostaw oraz złośliwe oprogramowanie jako główne zagrożenia dla instytucji finansowych. Sektor finansowy pozostaje głównym celem cyberprzestępców ze względu na swoje cenne zasoby i połączenia w ramach cyfrowej infrastruktury. Zgodnie z wynikami ENISA, 46% wszystkich zgłoszonych incydentów dotyczyło europejskich instytucji kredytowych (banków), co czyni je najczęściej atakowanymi podmiotami. Publiczne organizacje finansowe stanowiły 13% incydentów, a indywidualni klienci zostali dotknięci w 10% przypadków, często poprzez phishing i oszustwa.

**Instytucje finansowe balansujące między innowacją (AI) a środkami bezpieczeństwa**

*Sektor usług finansowych znajduje się na krytycznym momencie, stojąc przed rosnącą presją dostosowania swoich systemów do rozwoju najnowszych technologii, takich jak sztuczna inteligencja (AI), aby pozostać konkurencyjnym. Prognozy wskazują na gwałtowny wzrost wydatków związanych z AI w sektorze finansowym (wzrost o 30,7% rocznie między 2023 a 2024 rokiem). Wzrost ten osiągnie poziom ponad 1,4 miliarda USD do końca br. Jednakże z tymi możliwościami wiąże się ryzyko bezpieczeństwa i odporności systemów AI* – podkreślają analitycy Check Point. Zrozumienie, jak instytucje finansowe mogą balansować między potrzebą innowacji a ochroną swoich operacji poprzez solidne środki bezpieczeństwa cybernetycznego i strategie zarządzania ryzykiem AI, będzie jednym z najważniejszych wyzwań na drodze do skutecznego i bezpiecznego wdrożenia AI i Generative AI.

**Polska liderem w zakresie cyberbezpieczeństwa**

Są jednak pocieszające sygnały. Polska zajmuje (dane 03.24) drugie miejsce na świecie w [Indeksie Cyberbezpieczeństwa Narodowego](https://ncsi.ega.ee/country/pl/)(NCSI), co oznacza, że tylko jeden kraj był lepiej przygotowany na cyberataki niż Polska. Nasz kraj osiągnął prawie 100-procentową zgodność przygotowania i odpornośc systemów w prawie każdym aspekcie. Tylko w zakresie badań i rozwoju cyberbezpieczeństwa uzyskał mniej niż 67%. W pozostałych obszarach wynik wynosił co najmniej 67%. W sumie kraj uzyskał maksymalną liczbę punktów w 8 z 12 ocenianych kryteriów, co czyni go jednym z liderów międzynarodowych. Tylko Czechy były lepiej przygotowane według NCSI.