

dr inż. Tomasz Grudniewski

Akademia Bialska im. Jana Pawła II

ORCID: 0000-0003-3394-8992

dr Sławomir Żurawski

Państwowa Akademia Nauk Stosowanych w Chełmie

ORCID: 0000-0001-9527-3391

dr Iwona Lasek-Surowiec

Państwowa Akademia Nauk Stosowanych w Chełmie

ORCID: 0000-0002-7231-7993

mgr Zuzanna Jordan

ORCID: 0009-0009-2636-8501

https://doi.org/10.29316/9788368103205_2

WPŁYW CYBERATAKÓW NA SEKTOR FINANSOWY

THE IMPACT OF CYBERATTACKS ON THE FINANCIAL SECTOR

Streszczenie

Celem rozdziału jest przedstawienie charakteru i skutków cyberataków wymierzonych w sektor finansowy. W pierwszej części zaprezentowano charakterystykę sektora finansowego jako obszaru szczególnie narażonego na cyberzagrożenia, z uwzględnieniem rodzaju ataków oraz ich wpływu na bezpieczeństwo danych i stabilność gospodarki. Druga część koncentruje się na analizie konkretnych przypadków cyberataków – głównie

Summary

The aim of the chapter is to present the nature and effects of cyberattacks aimed at the financial sector. The first part presents the characteristics of the financial sector as an area particularly vulnerable to cyber threats, taking into account the type of attacks and their impact on data security and economic stability. The second part focuses on the analysis of specific cases of cyberattacks – mainly in the context of actions against the Polish

w kontekście działań przeciwko KNF – oraz ich bezpośrednich i pośrednich konsekwencji. W części trzeciej opisano aktualne strategie reagowania, obowiązujące regulacje prawne oraz wyzwania i kierunki rozwoju systemu cyberbezpieczeństwa w instytucjach finansowych. Problem badawczy sformułowano: Jakie są główne zagrożenia cybernetyczne dla sektora finansowego w Polsce i w jaki sposób instytucje finansowe, w tym KNF, reagują na te zagrożenia? W rozdziale zastosowano analizę literatury przedmiotu, dokumentów, w szczególności raportu rocznego CSIRT KNF 2024 oraz rzetelnych źródeł internetowych. Rosnące zagrożenie cyberatakami wobec sektora finansowego wymaga systemowego podejścia, które łączy działania techniczne, prawne i edukacyjne, a także rozwój odporności instytucjonalnej opartej na współpracy i ciągłej adaptacji do zmieniających się realiów cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, sektor finansowy, KNF, cyberatak, fałszywe inwestycje

Financial Supervision Authority – and their direct and indirect consequences. The third part describes current response strategies, applicable legal regulations as well as challenges and directions of development of the cybersecurity system in financial institutions. The research problem was formulated: What are the main cyber threats to the financial sector in Poland and how do financial institutions, including the Polish Financial Supervision Authority, respond to these threats? The chapter uses an analysis of the literature on the subject, documents, in particular the annual report of the CSIRT KNF 2024 and reliable online sources. The growing threat of cyberattacks against the financial sector requires a systemic approach that combines technical, legal, and educational activities, as well as the development of institutional resilience based on cooperation and continuous adaptation to the changing realities of cyberspace.

Keywords: cybersecurity, financial sector, Polish Financial Supervision Authority, cyberattack, fake investments

Wstęp

W dobie postępującej cyfryzacji i rosnącej zależności od technologii informatycznych, sektor finansowy staje się jednym z głównych celów cyberprzestępców. Instytucje takie jak banki, domy maklerskie, giełdy, towarzystwa ubezpieczeniowe, a także organy nadzorcze – w tym Komisja Nadzoru Finansowego – przetwarzają i przechowują ogromne ilości danych wrażliwych oraz zarządzają infrastrukturą krytyczną dla funkcjonowania całej gospodarki. W konsekwencji każda luka w zabezpieczeniach może prowadzić do poważnych konsekwencji, zarówno dla pojedynczych podmiotów, jak i dla stabilności całego systemu finansowego.

Cyberataki na sektor finansowy przybierają coraz bardziej wyrafinowane formy. Złośliwe oprogramowanie, ataki typu phishing, ransomware, a także zaawansowane techniki inżynierii społecznej są wykorzystywane do uzyskania

dostępu do systemów informatycznych i danych klientów. Dodatkowo rośnie zagrożenie ze strony podmiotów państwowych i zorganizowanych grup cyberprzestępczych, które działają w sposób skoordynowany i często trudny do wykrycia. Z uwagi na skalę ryzyka, jak również potencjalne skutki społeczne i ekonomiczne, kwestia ochrony przed cyberatakami stała się jednym z priorytetów strategii bezpieczeństwa finansowego w Polsce i na świecie.

Przykłady incydentów z ostatnich lat, w tym cyberataków wymierzonych w Komisję Nadzoru Finansowego, pokazują, że nawet instytucje odpowiedzialne za nadzór i bezpieczeństwo nie są odporne na tego rodzaju zagrożenia. Naruszenia integralności danych, utrata dostępności do systemów czy upublicznienie poufnych informacji mogą prowadzić do spadku zaufania do całego rynku finansowego, a w skrajnych przypadkach – do destabilizacji jego funkcjonowania.

Celem niniejszego rozdziału jest analiza wpływu cyberataków na sektor finansowy w Polsce, ze szczególnym uwzględnieniem incydentów dotyczących Komisji Nadzoru Finansowego. W rozdziale omówione zostaną zarówno mechanizmy i techniki wykorzystywane przez cyberprzestępców, jak i działania podejmowane przez instytucje w odpowiedzi na rosnące zagrożenia. Podjęta zostanie również refleksja nad aktualnym stanem bezpieczeństwa cyfrowego w sektorze finansowym oraz nad potrzebą dalszego wzmacniania odporności instytucji na ataki w cyberprzestrzeni.

Sektor finansowy jako cel cyberataków

W ramach systemu finansowego funkcjonują różnorodne instytucje finansowe, które zajmują się szeroko pojętym zarządzaniem zasobami pieniężnymi państwa i obywateli¹, dlatego od lat znajduje się w centrum zainteresowania cyberprzestępców. Jest to obszar gospodarki o wyjątkowym znaczeniu systemowym, który nie tylko odpowiada za obrót kapitałem, ale także stanowi fundament zaufania społecznego i stabilności ekonomicznej. W związku z tym każdy incydent bezpieczeństwa w tym sektorze może mieć daleko idące konsekwencje – od strat finansowych po kryzysy zaufania i zaburzenia płynności rynkowej. RCB jako główne wskazało następujące segmenty systemu:

¹ R. Hennig, *Cyberterroryzm vs infrastruktura krytyczna. Cz. V. System finansowy*, Kwartalnik Bellona, Nr 2, Wydawnictwo MON, Warszawa 2017, s. 184.

- budżetowy, związany z funkcjonowaniem finansowych struktur państwowych;
- bankowy, odnoszący się do funkcjonowania banków i instytucji kredytowych;
- ubezpieczeniowy, związany z ubezpieczeniami społecznymi oraz na życie, osobowymi i majątkowymi;
- kapitałowy, poświęcony obrotowi średnio i długoterminowych instrumentów finansowych².

Instytucje finansowe, takie jak banki, domy maklerskie, firmy ubezpieczeniowe, fundusze inwestycyjne oraz operatorzy systemów płatniczych, gromadzą i przetwarzają ogromne ilości danych osobowych, finansowych i handlowych. Są to dane o wysokiej wartości, zarówno dla cyberprzestępców działających w celach finansowych, jak i dla podmiotów zainteresowanych działalnością wywiadowczą lub destabilizacją systemu gospodarczego. Co więcej, cyfryzacja usług finansowych – bankowości internetowej, aplikacji mobilnych, e-płatności – poszerzyła powierzchnię potencjalnych ataków, a także zwiększyła zależność od infrastruktury IT³. Do najczęstszych form ataków skierowanych przeciwko sektorowi finansowemu należą:

- Phishing – technika polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych logowania, numerów kart płatniczych lub innych poufnych informacji.
- Malware – złośliwe oprogramowanie wprowadzane do systemów w celu kradzieży danych, przejęcia kontroli nad systemem lub wywołania szkód w infrastrukturze IT.
- Ransomware – oprogramowanie szyfrujące dane i żądające okupu za ich odszyfrowanie. Tego rodzaju ataki często paraliżują działalność operacyjną instytucji finansowych.
- DDoS (Distributed Denial of Service) – ataki polegające na przeciążeniu systemów sieciowych, prowadzące do niedostępności usług online, np. bankowości elektronicznej.

² Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1. Charakterystyka systemów infrastruktury krytycznej, Warszawa 2013, s. 37-41.

³ D. Skoczylas, *Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych*, Acta Iuris Stetinensis, 43 (2), 2023, s. 109.

- Manipulacje rynkowe i ataki na algorytmy transakcyjne – cyberprzestępcy coraz częściej próbują ingerować w działanie systemów handlu elektronicznego, automatycznych mechanizmów decyzyjnych czy nawet manipulować kursami instrumentów finansowych.

Warto również zwrócić uwagę, że zagrożenie nie zawsze pochodzi z zewnątrz. Równie niebezpieczne są działania osób z wewnątrz organizacji (tzw. insider threats), które mają dostęp do krytycznych systemów i danych⁴. Takie przypadki są trudniejsze do wykrycia i często wiążą się z nadużyciem zaufania oraz lukami w polityce bezpieczeństwa. Oto kilka przykładów największych cyberataków na sektor finansowy:

- Equifax: w 2017 r. hakerzy zaatakowali Equifax, jedną z największych agencji oceny zdolności kredytowej. Ujawniono dane osobowe około 147 milionów klientów, w tym numery ubezpieczenia społecznego i dane finansowe⁵.
- Banco de Chile: w 2018 r. chilijski Banco de Chile został zaatakowany przez hakerów, którzy zablokowali systemy banku i skradli dane klientów. Diagram ataku na infrastrukturę ofiary. Pomimo, że wszystkie wskazane przykłady dotyczą rynków zagranicznych, w Polsce sektor finansowy również jest jednym z najczęściej atakowanych przez cyberprzestępców⁶.
- Atak na Evolve Bank & Trust: w lipcu 2024 r. Evolve Bank & Trust z siedzibą w Memphis, Tennessee, doświadczył poważnego naruszenia danych, które dotknęło 7,6 miliona osób. Atak został powiązany z grupą ransomware LockBit, która ujawniła wrażliwe dane klientów po tym, jak bank odmówił zapłacenia okupu. Skradzione informacje obejmowały nazwiska, numery ubezpieczenia społecznego, numery kont bankowych oraz dane kontaktowe⁷.
- Atak na LoanDepot: LoanDepot, czołowy pożyczkodawca hipoteczny z siedzibą w Irvine w Kalifornii, padł ofiarą ataku, w wyniku którego

⁴ L. Liu, O. De Vel, Q.-L. Han, J. Zhang, Y. Xiang, *Detecting and Preventing Cyber Insider Threats: A Survey*, IEEE Communications Surveys & Tutorials, vol. 20, no. 2, 2018, s. 1400.

⁵ Equifax zapłaci za wyciek danych klientów. Uгода z FTC, <https://businessinsider.com.pl/firmy/zarzadzanie/equifax-zaplaci-za-wyciek-danych-klientow-ugoda-z-ftc/l8hdwqd>, [dostęp: 05.04.2025].

⁶ Ransomware sparaliżował bank w Chile – Bankier.pl, <https://www.bankier.pl/wiadomosc/Ransomware-sparalizowal-bank-w-Chile-7958860.html>, [dostęp: 05.04.2025].

⁷ Major Cyber Attacks Targeting the Finance Industry - SOCRadar® Cyber Intelligence Inc., <https://socradar.io/major-cyber-attacks-targeting-the-finance-industry>, [dostęp: 05.04.2025].

naruszono dane 16,9 miliona klientów. Atak miał miejsce między 3 a 5 stycznia 2024 r. i został przypisany grupie Alphv, znanej również jako Blackcat. Skradzione dane obejmowały nazwiska, adresy, numery kont finansowych, numery telefonów oraz daty urodzenia klientów⁸.

- Atak na ByBit: w lutym 2025 r. FBI zidentyfikowało Koreę Północną jako odpowiedzialną za kradzież wirtualnych aktywów o wartości 1,5 miliarda dolarów z giełdy kryptowalut ByBit. Jest to największa tego typu kradzież w historii. Skradzione środki zostały początkowo prze-transferowane na wiele adresów bitcoin i innych wirtualnych aktywów, a następnie prawdopodobnie wyprane i zamienione na walutę fiducyjną⁹.

Cyberzagrożenia w sektorze finansowym to nie tylko problem instytucji komercyjnych, takich jak banki czy firmy ubezpieczeniowe, ale również organów nadzoru, które pełnią kluczową rolę w zapewnieniu stabilności i transparentności rynku. Jednym z najgłośniejszych przykładów w ostatnich latach był cyberatak wymierzony w Komisję Nadzoru Finansowego (KNF), który unaoczniał skalę i powagę ryzyk związanych z bezpieczeństwem cyfrowym w instytucjach publicznych¹⁰.

Do incydentu doszło na przełomie grudnia 2023 i stycznia 2024 r. Atak został zakwalifikowany jako poważny incydent bezpieczeństwa, skutkujący czasowym unieruchomieniem niektórych systemów informatycznych Komisji. Choć oficjalne komunikaty KNF nie zawierały wielu szczegółów, wiadomo, że w ramach środków zaradczych instytucja natychmiast odłączyła swoje systemy od sieci zewnętrznych, co spowodowało zakłócenia w dostępie do usług elektronicznych, w tym do systemu ePUAP. W wyniku tego utrudniona została codzienna komunikacja z interesariuszami i nadzorowanymi podmiotami. Z informacji medialnych i raportów branżowych wynika, że za atakiem mogła stać zorganizowana grupa przestępcza, prawdopodobnie działająca z zagranicy, posługująca się znanymi schematami – w tym oprogramowaniem

⁸ *The biggest data breaches of 2024 in financial services*, American Banker, <https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services?>, [dostęp: 05.04.2025].

⁹ North Korea behind \$1.5bn hack of crypto exchange ByBit, says FBI, North Korea, The Guardian, <https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi?>, [dostęp: 05.04.2025].

¹⁰ *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa – Archiwum, <https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/>, [dostęp: 05.04.2025].

ransomware i kampanią phishingową. Choć nie doszło do potwierdzonego wycieku danych osobowych lub finansowych, eksperci ds. bezpieczeństwa ostrzegali, że nawet czasowa niedostępność systemów nadzorczych może mieć poważne implikacje dla ciągłości działania całego sektora. Bezpośrednie konsekwencje incydentu objęły:

- tymczasowy paraliż komunikacyjny w KNF,
- zakłócenia w procesach nadzoru i obsługi zgłoszeń,
- zwiększoną podatność na dezinformację i ataki wtórne.

Pośrednie skutki miały natomiast charakter reputacyjny i systemowy. Pojawiły się pytania o odporność infrastruktury IT kluczowych instytucji państwowych, a także o zdolność KNF do szybkiej reakcji w sytuacjach kryzysowych. Utrata zaufania do instytucji nadzorczej, nawet chwilowa, może rzutować na stabilność całego systemu finansowego – szczególnie w oczach inwestorów, klientów i międzynarodowych partnerów.

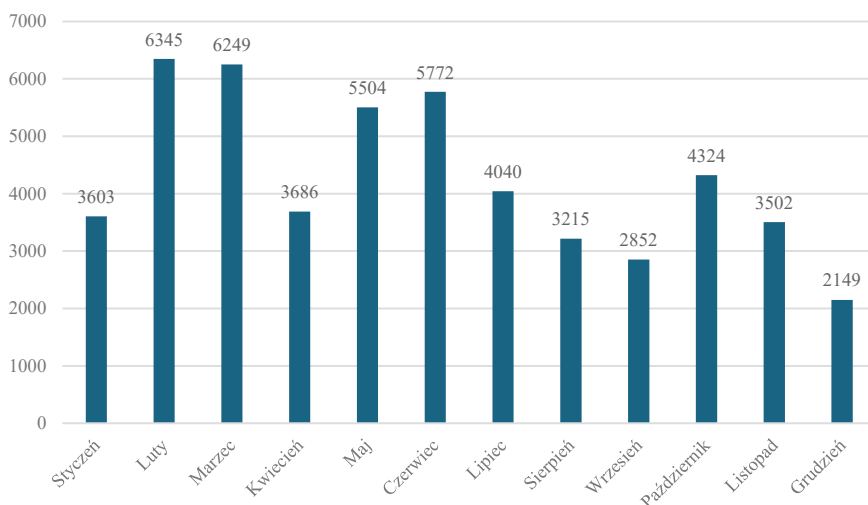
W odpowiedzi na atak, Komisja Nadzoru Finansowego we współpracy z zespołami CSIRT NASK i CERT Polska wdrożyła procedury zarządzania incydem, przeprowadziła szczegółowe analizy techniczne oraz podjęła działania prewencyjne, mające na celu podniesienie poziomu bezpieczeństwa swoich systemów informatycznych. Zdarzenie to stało się również impulsem do szerszej debaty o konieczności modernizacji infrastruktury cyfrowej w instytucjach publicznych i podjęcia dalszych działań legislacyjnych w zakresie cyberbezpieczeństwa.

Przypadek KNF potwierdza, że nawet najbardziej doświadczone i dobrze zorganizowane instytucje mogą stać się ofiarą cyberataków. Dlatego tak istotne jest ciągle doskonalenie mechanizmów obronnych, monitorowanie zagrożeń oraz budowanie kultury cyberodporności zarówno w sektorze prywatnym, jak i publicznym.

Rosnące zagrożenia cybernetyczne wobec sektora finansowego wymuszają na instytucjach konieczność inwestowania w nowoczesne systemy bezpieczeństwa, przeprowadzania regularnych audytów, testów penetracyjnych, a także budowania kultury cyberodporności wśród pracowników i klientów. W przeciwnym razie nawet najmniejszy błąd lub luka w zabezpieczeniach może zostać wykorzystana do przeprowadzenia skutecznego i kosztownego ataku.

Charakterystyka cyberataków na sektor finansowy w 2024 roku

Rok 2024 przyniósł bezprecedensowy wzrost liczby cyberataków wymierzonych w sektor finansowy w Polsce. Zgodnie z danymi zawartymi w raporcie CSIRT KNF, liczba zgłoszonych niebezpiecznych domen osiągnęła rekordowy poziom – 51 241 przypadków. W porównaniu z rokiem poprzednim oznacza to wzrost o ponad 70%. Największą grupę, stanowiącą aż 89,4% wszystkich incydentów, tworzyły fałszywe strony inwestycyjne. Ta forma oszustwa była nie tylko najczęściej występująca, ale również najbardziej szkodliwa, skutkując poważnymi stratami finansowymi i społecznymi. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 przedstawiono na rysunku poniżej.



Rysunek 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 roku w poszczególnych miesiącach

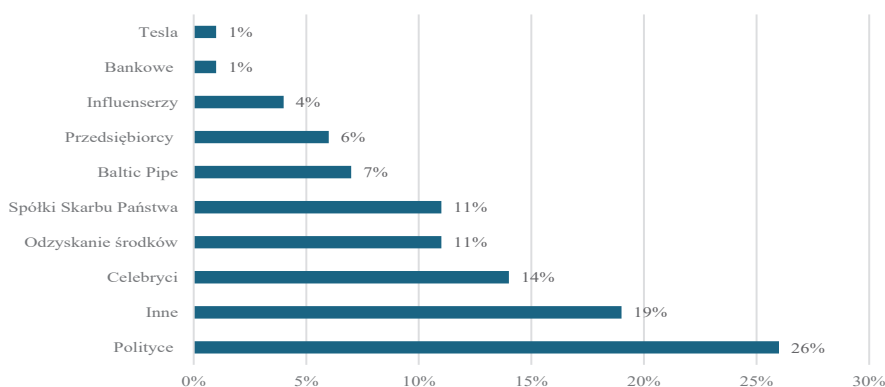
Źródło: Raport Roczny CISIRT KNF 2024, s. 9.

Fałszywe inwestycje polegały na tworzeniu profesjonalnie wyglądających, lecz całkowicie fikcyjnych platform inwestycyjnych. Cyberprzestępcy wykorzystywali zaawansowane techniki socjotechniczne, aby uwiarygodnić swoje działania – posługiwali się m.in. fałszywymi wykresami, sfałszowanymi opiniami, historiami rzekomych sukcesów oraz mechanizmami rekomendacyjnymi. W kampaniach tych szeroko wykorzystywano reklamy w mediach społecznościowych, które kierowały potencjalne ofiary na spreparowane

strony internetowe. Coraz częściej przestępcy sięgali po technologię deepfake, aby generować materiały wideo z udziałem znanych osób zachęcających do inwestycji, co dodatkowo potęgowało wrażenie autentyczności.

Oprócz fałszywych inwestycji, dużym zagrożeniem okazały się oszustwa ankietowe. CSIRT KNF zidentyfikował ponad cztery tysiące domen związanych z tego typu kampaniami. Ich mechanizm działania polegał na zachęcaniu użytkowników do wypełnienia krótkiej ankiety w zamian za rzekomą nagrodę. Użytkownik w trakcie wypełniania formularza był stopniowo skłaniany do podania danych osobowych oraz informacji o karcie płatniczej. Strony imitowały wygląd znanych marek i instytucji, co miało na celu zwiększenie wiarygodności przekazu. Kluczową rolę odgrywały tu emocje – przestępcy stosowali presję czasu i efekt „strachu przed utratą okazji” (FOMO), aby przyspieszyć reakcję użytkowników.

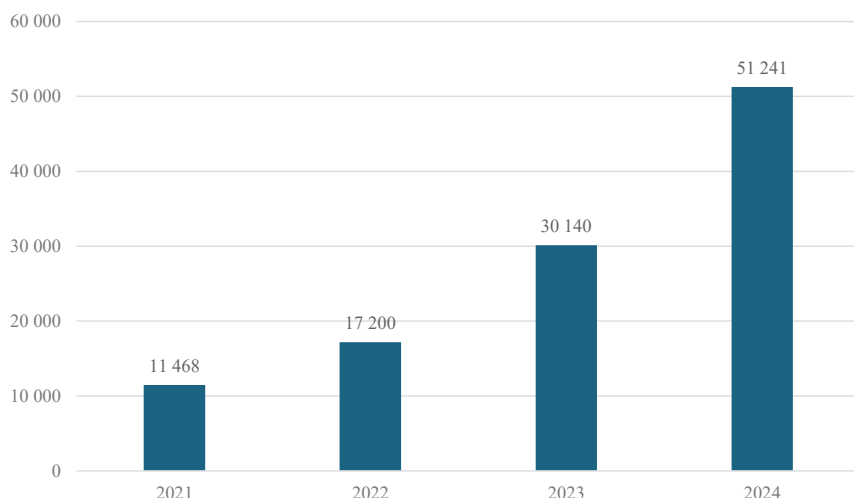
Kolejną kategorią były oszustwa bankowe, w których przestępcy podszywali się pod znane instytucje finansowe. Tworzyli fałszywe strony logowania do bankowości elektronicznej, często różniące się od oryginalnych jedynie minimalnymi szczegółami w adresie URL. Do ofiar trafiały reklamy w mediach społecznościowych, wiadomości SMS oraz e-maile, które przekierowywały na fałszywe witryny. Wykorzystywane wizerunki w reklamach fałszywych inwestycji w 2024 roku przedstawiono na poniższym rysunku.



Rysunek 2. Wykorzystywane wizerunki w reklamach fałszywych inwestycji w 2024 roku

Źródło: Raport Roczny CISIRT KNF 2024, s. 12.

Przestępcy potrafili wykorzystać zarówno techniki phishingowe, jak i manipulację wynikami wyszukiwania w Google, umieszczając swoje spreparowane strony w czołówce wyników. Poniżej na rysunku 3 przedstawiono liczbę zgłoszonych domen phishingowych w latach 2021-2024 przez CSIRT KNF.



Rysunek 3. Liczba zgłoszonych domen phishingowych w latach 2021-2024 przez CSIRT KNF

Źródło: Raport Roczny CISIRT KNF 2024, s. 10.

Z raportu wynika również, że rok 2024 był okresem intensywnych kampanii z użyciem złośliwego oprogramowania. Obserwowano aktywność wielu różnych typów malware, w tym programów typu stealer, takich jak Lumma Stealer czy AgentTesla, których celem było wykradanie danych logowania i poufnych informacji z komputerów użytkowników. Inne zagrożenia obejmowały oprogramowanie typu RAT (*Remote Access Trojan*), jak RemcosRAT czy Xworm, które pozwalało przestępcom na zdalne przejęcie kontroli nad zainfekowanym systemem. Szczególnie niepokojące były przypadki wykorzystania aplikacji mobilnych, dystrybuowanych np. przez fałszywe reklamy na Facebooku. Aplikacje te, często bazujące na technologiach WebAPK lub PWA, udawały oficjalne narzędzia bankowe, a w rzeczywistości wykradały dane osobowe i finansowe użytkowników.

Raport podkreśla także coraz większe zaawansowanie kampanii cyberprzestępczych. Przestępcy szybko dostosowują się do zmieniających się realiów i zabezpieczeń, korzystają z aktualnych wydarzeń społeczno-gospodarczych,

a także coraz częściej personalizują swoje działania w zależności od profilu ofiary. Widać także coraz częstsze wykorzystanie narzędzi opartych na sztucznej inteligencji, które umożliwiają tworzenie jeszcze bardziej przekonujących treści oszukańczych. W świetle powyższych danych, CSIRT KNF wskazuje na potrzebę stałego doskonalenia mechanizmów ochrony przez instytucje finansowe i regulatorów. Rok 2024 był kolejnym dowodem na to, że cyberprzestępczość staje się coraz bardziej profesjonalna i zorganizowana, a jej celem są zarówno dane, jak i bezpośrednie środki finansowe obywateli. Złożoność złośliwego oprogramowania, szybkość działania hakerów, doskonała znajomość wewnętrznych systemów transakcyjnych banków dowodzą wagi problemu, wobec którego stoją instytucje finansowe¹¹.

Reakcje, strategie i przyszłość cyberbezpieczeństwa w finansach

W obliczu rosnącej liczby i skali cyberzagrożeń sektor finansowy znajduje się dziś w punkcie zwrotnym, który wymaga nie tylko reagowania na incydenty, ale przede wszystkim strategicznego podejścia do budowania trwałej odporności cyfrowej. Odpowiedzią na nasilające się ataki są działania podejmowane na wielu poziomach – od pojedynczych instytucji finansowych, przez krajowe organy nadzoru, po inicjatywy międzynarodowe. Kluczowe znaczenie ma tu spójna i zintegrowana polityka bezpieczeństwa, która obejmuje zarówno aspekt technologiczny, jak i organizacyjny oraz edukacyjny.

Jednym z najważniejszych elementów krajowej odpowiedzi na zagrożenia cybernetyczne jest działalność zespołu CSIRT KNF, pełniącego rolę sektorowego zespołu reagowania na incydenty komputerowe. W 2024 r. zespół ten nie tylko monitorował i analizował bieżące kampanie przestępcze, lecz także aktywnie uczestniczył w budowaniu systemu prewencji poprzez identyfikację niebezpiecznych domen, blokowanie oszukańczych treści i prowadzenie działań edukacyjnych. Współpraca z CSIRT NASK, CERT Polska oraz platformami społecznościowymi, takimi jak Facebook, umożliwiła szybkie reagowanie na nowe zagrożenia oraz ograniczanie ich zasięgu.

Istotnym krokiem w kierunku systemowego podejścia do bezpieczeństwa cyfrowego jest także wdrożenie regulacji europejskich, w tym aktu

¹¹ G. Strupczewski, *Zagrożenie cybernetyczne instytucji finansowych*, Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych, Nr 24, 2017, s. 80.

DORA (*Digital Operational Resilience Act*), który obowiązywać będzie od stycznia 2025 r. Rozporządzenie to nakłada nowe obowiązki w zakresie zarządzania ryzykiem ICT (technologii informacyjno-komunikacyjnych) na wszystkie instytucje finansowe działające na terenie Unii Europejskiej. DORA wprowadza jednolite standardy raportowania incydentów, testowania odporności cyfrowej, a także nadzoru nad dostawcami usług technologicznych. Jego celem jest wzmocnienie spójności i gotowości całego rynku finansowego na wypadek zakłóceń wywołanych cyberatakami. Na poziomie organizacyjnym wiele instytucji finansowych podejmuje działania mające na celu zwiększenie odporności swoich systemów¹². Wśród nich znajdują się inwestycje w nowoczesne technologie wykrywania zagrożeń, automatyzacja procesów bezpieczeństwa (np. poprzez SIEM czy SOAR), a także rozwój wewnętrznych zespołów reagowania i współpraca z zewnętrznymi partnerami w zakresie cyberbezpieczeństwa. Coraz większy nacisk kładzie się również na zarządzanie ryzykiem dostawców zewnętrznych, którzy odgrywają coraz istotniejszą rolę w działalności operacyjnej instytucji finansowych.

Nie można pominąć także roli edukacji i podnoszenia świadomości. Kampanie informacyjne, szkolenia dla pracowników, materiały dla klientów indywidualnych – to narzędzia, które pozwalają ograniczyć skuteczność ataków opartych na socjotechnice. CSIRT KNF w swoim raporcie wskazuje, że jednym z kluczowych czynników sukcesu cyberprzestępców jest właśnie nieświadomość użytkowników oraz ich skłonność do zaufania treściom publikowanym w Internecie. Dlatego też działania prewencyjne muszą być prowadzone równolegle z wdrażaniem zabezpieczeń technicznych.

W perspektywie najbliższych lat można spodziewać się dalszej ewolucji zagrożeń, związanej m.in. z wykorzystaniem sztucznej inteligencji do tworzenia treści oszukańczych, automatyzacją ataków oraz rosnącą liczbą podatności w systemach informatycznych. Nowe technologie przyniosą zarówno możliwości, jak i wyzwania, dlatego sektor finansowy musi nieustannie adaptować się do zmieniającego się krajobrazu zagrożeń.

Wnioski płynące z roku 2024 są jednoznaczne – cyberbezpieczeństwo nie jest już kwestią techniczną, lecz strategiczną. Tylko kompleksowe podejście, obejmujące zarówno rozwój technologii ochronnych, jak i działania

¹² A. Krawczyk-Jezińska, *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, tom LXXII, nr 8(854), 2019, s. 30.

legislacyjne, organizacyjne i edukacyjne, pozwoli na skuteczne przeciwdziałanie rosnącej fali zagrożeń w cyberprzestrzeni. Budowanie odporności sektora finansowego musi opierać się na współpracy wszystkich interesariuszy: instytucji publicznych, regulatorów, dostawców usług technologicznych oraz samych klientów. Tylko wtedy możliwe będzie utrzymanie zaufania do rynku finansowego jako stabilnego i bezpiecznego filaru gospodarki.

Podsumowanie

Rok 2024 wyraźnie potwierdził, że sektor finansowy pozostaje jednym z najbardziej narażonych obszarów na cyberzagrożenia. Rosnąca skala i złożoność ataków, a także ich coraz bardziej zróżnicowane formy, wymusiły konieczność zintensyfikowania działań prewencyjnych i reagujących. Największym wyzwaniem okazały się kampanie fałszywych inwestycji, które zdominowały krajobraz cyberprzestępczy, prowadząc do poważnych strat finansowych wśród klientów indywidualnych. Ich skuteczność wynikała z umiejętnego łączenia technik socjotechnicznych z nowoczesnymi narzędziami, takimi jak deepfake czy personalizowane kampanie reklamowe.

Istotnym problemem pozostaje fakt, że cyberprzestępcy coraz częściej wykorzystują zaufanie społeczne – podszywają się pod znane osoby, instytucje publiczne czy duże firmy, co znacząco utrudnia wykrycie zagrożenia. Dodatkowo, rosnąca liczba oszustw ankietowych, ataków na bankowość elektroniczną oraz kampanii złośliwego oprogramowania pokazuje, że zagrożenie nie jest ograniczone do jednego typu działania, lecz przybiera wiele form jednocześnie. W związku z tym nie wystarczy już stosowanie klasycznych metod ochrony – potrzebne są rozwiązania kompleksowe, uwzględniające zarówno aspekty techniczne, jak i organizacyjne, a także edukacyjne.

Reakcja sektora finansowego, w tym działania podejmowane przez KNF i CSIRT KNF, wskazują na rosnącą świadomość w zakresie potrzeby budowania odporności cyfrowej. Przykładem tego jest coraz szersze wdrażanie regulacji europejskich, takich jak DORA, które mają na celu ujednolicenie standardów i wymogów dotyczących bezpieczeństwa w całej Unii Europejskiej. Jednocześnie rośnie znaczenie współpracy między instytucjami publicznymi, sektorem prywatnym oraz międzynarodowymi partnerami, co jest nieodzowne w kontekście globalnego charakteru zagrożeń.

Wnioski z analizy raportu CSIRT KNF są jasne – cyberbezpieczeństwo nie może być traktowane jako dodatek do działalności operacyjnej, lecz jako jej integralna część. Tylko wtedy możliwe będzie skuteczne przeciwdziałanie zagrożeniom i ograniczenie ich skutków. Niezbędna jest dalsza rozbudowa infrastruktury ochronnej, regularne testowanie mechanizmów bezpieczeństwa, a przede wszystkim – budowanie kultury świadomości cyfrowej wśród wszystkich uczestników rynku finansowego. Przyszłość cyberbezpieczeństwa w finansach zależy od tego, jak szybko i konsekwentnie sektor dostosuje się do nowych realiów, w których cyberprzestrzeń stała się nieodłącznym i coraz bardziej ryzykownym elementem funkcjonowania gospodarki.

Literatura

1. *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa – Archiwum, <https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/>.
2. *Equifax zapłaci za wyciek danych klientów. Uгода z FTC*, <https://businessinsider.com.pl/firmy/zarzadzanie/equifax-zaplaci-za-wyciek-danych-klientow-ugoda-z-ftc/l8hdwqd>.
3. Hennig R., *Cyberterroryzm vs infrastruktura krytyczna. Cz. V. System finansowy*, Kwartalnik Bellona, 2/2017.
4. Krawczyk-Jezińska A., *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, tom LXXII, nr 8(854), 2019.
5. Liu L., De Vel O., Han Q.-L., Zhang J., Xiang Y., *Detecting and Preventing Cyber Insider Threats: A Survey*, IEEE Communications Surveys & Tutorials, vol. 20, no. 2, 2018.
6. *Major Cyber Attacks Targeting the Finance Industry* – SOCRadar® Cyber Intelligence Inc., <https://socradar.io/major-cyber-attacks-targeting-the-finance-industry>.
7. Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Charakterystyka systemów infrastruktury krytycznej. Warszawa 2013, s. 37-41.
8. North Korea behind \$1.5bn hack of crypto exchange ByBit, says FBI, North Korea, The Guardian, <https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi?>
9. *Ransomware sparaliżował bank w Chile*, Bankier.pl, <https://www.bankier.pl/wiadomosc/Ransomware-sparalizowal-bank-w-Chile-7958860.html>.
10. Raport Roczny CISIRT KNF 2024.
11. Skoczylas D., *Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych*, Acta Iuris Stetinensis 43(2), 2023.
12. Strupczewski G., *Zagrożenie cybernetyczne instytucji finansowych*, Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych, 24, 2017, s. 80.
13. *The biggest data breaches of 2024 in financial services*, American Banker, <https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services?>