Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215905

Analysis of the ENISA report ‘Finance Threat Landscape 2024’ and implications for the Polish financial sector

Analiza raportu ENISA „Finance Threat Landscape 2024” i implikacje dla polskiego sektora finansowego

Jolanta Turczynowicz-Kieryłło
Akademia Sztuki Wojennej
ORCID: 0009-0009-7075-8638
E-mail: j.turczynowicz-kieryllo@akademia.mil.pl

Abstract

This article presents a comprehensive analysis of the European Network and Information Security Agency (ENISA) report entitled ‘Threat Landscape: Finance Sector’ (January 2023 – June 2024). The report analyses 488 incidents related to cybersecurity in the broad sense. The incidents discussed in the report had a clear impact on financial institutions in Europe. The main threats were identified, including distributed attacks such as a) denial of service, b) data breaches, c) social engineering attacks, d) ransomware, and e) attacks on the so-called supply chain.

The article analyses the impact on European credit institutions of the approximately 46% of all cyber incidents they experienced and which had the greatest impact on them. ENISA's research has shown that operational disruptions and data disclosures were decisive for the assessment due to their far-reaching consequences and threats. A comparative analysis assesses the possibility and impact of applying ENISA's findings to the Polish financial sector, taking into account Poland's unique geopolitical vulnerabilities, emerging external and internal cyber threats, and the DORA and NIS2 compliance frameworks.

Research indicates that cyber threat statistics for the financial sector will continue to rise to the detriment of the system. Currently, increased cyber attacks on Polish critical infrastructure, partly due to geopolitical issues, explicitly demonstrate and justify the urgent need to increase cyber resilience. Security can and should be improved by introducing advanced threat detection techniques and strategies, education, and, in particular, holistic training for management and employees in the financial sector in the field of cyber risk management. The need for synergy and precise coordination between the activities of financial institutions and national cybersecurity authorities is clearly highlighted.

Keywords

ENISA; investment fraud, cyber resilience; DORA, NIS 2

Streszczenie

Niniejszy artykuł przedstawia wszechstronną analizę raportu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) pt. „Threat Landscape: Finance Sector" (styczeń 2023 r. – czerwiec 2024 r.). W Raporcie tym zostało przeanalizowanych 488 incydentów powiązanych z tematem rozumianego sensu largo cyberbezpieczeństwa. Omawiane w Raporcie incydenty miały wyraźny wpływ na instytucje finansowe w Europie. Zidentyfikowano główne zagrożenia, w tym rozproszone ataki takie jak a) „odmowa usługi", b) naruszenia bezpieczeństwa danych, c) ataki oparte o socjotechnikę, d) oprogramowanie ransomware oraz e) ataki na tzw. łańcuch dostaw. Artykuł analizuje, jaki wpływ na europejskie instytucje kredytowe miało doświadczenie przez nie ok. 46% z wszystkich zaistniałych cyberincydentów i które miały na nie największy wpływ. Badania ENISA dowiodły, iż decydujące znaczenie dla oceny miały zakłócenia operacyjne i ujawnienia danych z uwagi na daleko idące konsekwencje oraz zagrożenia. Dokonując analizy porównawczej poddaje się ocenie możliwość i wpływ zastosowania ustaleń ENISA do polskiego sektora finansowego, biorąc pod uwagę wyjątkowe słabości geopolityczne Polski, pojawiające się cyberzagrożenia zewnętrzne i wewnętrzne oraz ramy zgodności z przepisami DORA i NIS2.

Badania wskazują, że statystyka cyberzagrożeń sektora finansowego będzie jeszcze rosła na niekorzyść systemu. Obecnie wzmożone cyberataki na polską infrastrukturę krytyczną m.in. z uwagi na kwestie geopolityczne *explicite* pokazują i uzasadniają wymóg pilnego zwiększenia cyberodporności. Wzrost bezpieczeństwa można i powinno się osiągać poprzez wprowadzanie zaawansowanych technik i strategii wykrywania zagrożeń, edukację, w szczególności holistyczne szkolenia kadry zarządczej oraz pracowników sektora finansowego w dziedzinie zarządzania cyberryzykiem. Wyraźnie eksponuje sie przy tym potrzeba synergii i precyzyjnej koordynacji między działaniami instytucji finansowych a krajowymi organami zajmującymi się cyberbezpieczeństwem.

Słowa kluczowe

ENISA; oszustwa inwestycyjne, cyberodporność; DORA, NIS 2

Wprowadzenie

Do *facta notoria* należy zaliczyć stwierdzenie, że sektor finansowy jest jednym z najważniejszych filarów współczesnej gospodarki, zaś zrozumienie zjawisk dotychczas nieobecnych na taką skalę, jak narażenie systemu na cyberryzyko, zagrożenia cyberbezpieczeństwa na rynkach finansowych, jest kluczowe nie tylko dla rozwoju i wzrostu gospodarczego, ale przede wszystkim dla stabilności rynku. W tym znaczeniu to co dzieje sie na rynkach finansowych ma zawsze krytyczne znaczenia dla państwa, a co za tym idzie, jak każda cenna rzecz, staje się *per se* atrakcyjnym celem dla cyberprzestępców, ale także konkurencyjnych gospodarek czy nawet tzw. hakerów-aktywistów, którzy poprzez wykorzystywanie słabych punktow i luk w zabezpieczeniach dążą do osiągnięcia korzyści finansowych lub szpiegostwa, czasem zaś działają z pobudek określanych jako ideologiczne[1] .

Publikacja zawiera rekomendacje oparte na wynikach przeprowadzonych przez ENISA badań i statystyk dotyczące wdrażania w opisanje rzeczywistości koniecznych i skutecznych regulacji prawnych, a tym samym poprawy bezpieczeństwa instytucjonalnego.

[1] Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Zagrożenia: sektor finansowy (styczeń 2023 – czerwiec 2024), Heraklion 2024, https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf [dostęp na 01.12.2025].

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, mając na wzgledzie strategiczne znaczenie analizy cyberryzyk i zagrożeń dla bezpieczenstwa rynku finansowego, przeprowadziła wszechstronne badania, których wynik publikowany został w Raporcie poświęconym wyłącznie sektorowi finansowemu. Raport obejmuje okres styczeń 2023 - czerwiec 2024 r. Dostrzeżenie przez ENISĘ konieczności powstania dedykowanej analizy zbiega się w czasie z wprowadzaniem przepisów regulujących kwestie bezpieczeństwa sektora finansowego[2]. Na zmieniający się krajobraz cyberzagrożeń wskazują dane statystyczne poddane badaniom w Raporcie. Analiza obejmje 488 zgłosoznycch incydentów cybernetycznych, które miały wpływ na podmioty finansowe w państwach członkowskich UE i krajach sąsiednich. Szczególnie interesujące analizy dotyczące podatności, ryzyk i wpływu na rynek niebezpieczeństw związanych z cyberprzestepczością można przeprowadzić na polskim sektorze finansowym. Narodowy system bankowy i związana z nim infrastruktura płatnicza oraz platformy inwestycyjne to znaczący rynek finansowy z perspektywy Europy Środkowej i Wschodniej. Natomiast transgraniczne transakcje o wartości setek miliardów euro rocznie, ogromny kapitał ludzki, rozwinięty jeszcze po inwazji Rosji na Ukrainę i bezpośrednio związanej z tym migracją ludności uciekającej przed wojną oraz lokującej swój kapitał w polskim systemie bankowym przesądza o zasadności poszukiwania mechanizmów ochrony wobec oczywistego dodatkowego czynnika ryzyka jakim są działania odwetowe przeciwników zaangażowania Polski w pomoc Ukranie.

Nie można nie zauważyć, iż strategiczne położenie geopolityczne Polski, w tym aktywne wsparcie Ukrainy przed agresją rosyjską, niezmiennie naraża polskie instytucje finansowe na bezprecedensowe zagrożenia cybernetyczne. Daje to dodatkowo asumpt do konluzji, iż ryzyka ataków cybernetyczych zwłaszcza na infrstrukturę krytyczną, w tym sektor finansowy mogą być cześcią militarnej strategii przeciwników politycznych zaangazowanych w działania wojenne po innej stronie.

Powagę cyberzagrożeń dla polskich instytucji finansowych ukazują najnowsze statystyki. I tak przytaczając *in extenso* dane raportu Check Point Software Technologies „Security Report 2025”[3] ,nie sposób nie obliczyć, że polskie instytucje finansowe doświadczają około 1750 cyberataków tygodniowo, co wydatnie przekracza nawet średnią światową cyberataków, która wynosi 1510 ataków tygodniowo oraz średnią europejską[4] . Ten podwyższony profil zagrożeń

[2] Dyrektywa w sprawie bezpieczeństwa sieci i systemów informacyjnych 2 (dyrektywa NIS2), Dyrektywa 2022/2555, Bruksela 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555., Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa cybernetycznego w całej Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Dyrektywa NIS weszła w życie w Polsce 28 sierpnia 2018 r. na mocy ustawy o krajowym systemie cyberbezpieczeństwa. Dyrektywa NIS2 weszła w życie na poziomie UE 16 stycznia 2023 r., a termin jej wdrożenia upłynął 17 października 2024 r. Rada Ministrów przyjęła projekt ustawy 22 października 2025 r., a dokument został przedłożony Sejmowi w listopadzie 2025 r. Planuje się, że Sejm i Senat przyjmą go przed końcem 2025 r. Wejście w życie nowelizacji przewiduje się na początek 2026 r., z okresem przejściowym do 6 miesięcy dla podmiotów o znaczeniu istotnym i ważnym. Nowe przepisy rozszerzą zakres podmiotowy o sektory takie jak usługi pocztowe i produkcja chemiczna, wprowadzając m.in. obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa.

[3] https://www.checkpoint.com/resources/items/report-cyber-security-report-2025, [dostęp na 2.12.2025].

[4] Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, ibid.,s.3-5

na pewno wymaga kompleksowego zrozumienia współczesnych cyberzagrożeń oraz stworzenia i wdrażania strategii obronnych.

Niewątpliwie próbą systemowej odpowiedzi na zagrożenia dotyczące cyberbezpieczeństwa finansowego w Polsce są Ustawa o odporności operacyjnej w środowisku cyfrowym (DORA)[5] , obowiązująca od 17 stycznia 2025 r., a także dyrektywa w sprawie bezpieczeństwa sieci i informacji 2 (NIS2)[6] . Akty te należy interpretować wraz z pełnymi wymogami wdrożeniowymi, gdyż łącznie ustanawiają one komplementarne i współzależne ramy zarządzania ryzykiem i reagowania na incydenty, a co za tym idzie *in pleno* zarządzania cyberbezpieczeństwem w instytucjach finansowych o zasiegu europejskim.

Trzeba podkreślić, że wdrożenie ww. Dyrektyw w Polsce nastąpiło poprzez komplementarne działania jakimi były zmiany w ustawie o Krajowym Systemie Cyberbezpieczeństwa (UKSC) oraz odpowiednia koordynacja działań przez Komisję Nadzoru Finansowego (KNF). Nie bez znaczenia była równiez w tej kwestii rola sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT KNF). Wszystkie wyżej wymienione podmioty tworzą złożone otoczenie regulacyjne, które bezwzględnie wymaga dostosowania instytucjonalnego[7].

Niniejszy artykuł ma trzy główne cele badawcze: (1) przedstawienie kompleksowej analizy wyników raportu ENISA „Threat Landscape: Finance Sector" (Krajobraz zagrożeń: sektor finansowy), (2) ocena stosowalności i znaczenia ustaleń ENISA w kontekście konkretnego sektora finansowego w Polsce, (3) sformułowanie opartych na dowodach zaleceń dla polskich instytucji finansowych, organów regulacyjnych oraz przestawicieli władzy wykonwaczej i parlamentarzystów.

Analiza Raportu ENISA to przede wszystkim zidentyfikowanie kluczowych zagrożeń, podmiotów potencjalnie wrażliwych na zagrożenia, ale też z drugiej strony podmiotów, które same stanowią zagrożenie. Badanie to skupia się również na krytycznej ocenie wzorców oddziaływania poddanych obserwacji w okresie badawczym, to jest od stycznia 2023 r. aż do czerwca 2024 r.; Ocena polskiego sektora finansowego i jego cyberoodporności musi natomiast nastąpić z uwzględnieniem czynników geopolitycznych, krajowych ram regulacyjnych oraz tzw. lokalnych słabości instytucjonalnych**;**

Zalecenia ochronne dla sektora finansowego będą wskazane przede wszystkim w celu uporządkowania zakresow odpowiedzialności oraz zwiększenia cyberodporności zgodnie z europejskimi standardami regulacyjnymi, ale także w aktywnej reakcji na pojawiające sie nowe zagrożenia.

Metodologia badań łączy systematyczną analizę dokumentów zawartych w oficjalnym raporcie ENISA dotyczącym zagrożeń z oceną porównawczą danych dotyczących zagrożeń o charakterze *signum specificum* dla polskiego sektora

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie odporności operacyjnej cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

[6] M. Nowikowska , Mechanizmy współpracy w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS , [w] Rola cyberbezpieczeństwa w sferze publicznej: wymiar europejski, red. K. Chałubińska-Jentkiewicz (IP), Istvan Hoffman – Maribor, Słowenia: Instytut Samorządu Lokalnego Maribor, 2022, s. 79-92.

[7] Komisja Nadzoru Finansowego, CSIRT KNF, Raport roczny 2024, Warszawa 2025, https://www.knf.gov.pl/en/?articleId=93273&p_id=19, [dostęp 15.11.2025].

finansowego, krajowych wymogów regulacyjnych oraz tzw. punktów newralgicznych o podwyższonej czułości na cyberzagrożenia.
Analiza oparta jest na oficjalnych statystykach polskich organów ds. Cyberbezpieczeństwa takich jak CSIRT GOV (Computer Security Incident Response Team) CSIRT NASK, CSIRT KNF, komunikatach regulacyjnych Komisji Nadzoru Finansowego (KNF). Badania zostały przeprowadzone w świetle międzynarodowych ocen cyberzagrożeń oraz recenzowanej literatury naukowej przedmiotu, w szczególności dotyczacej europejskiego zarządzania cyberbezpieczeństwem finansowym**.** Szef Agencji Bezpieczeństwa Wewnętrznego prowadzi Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV na poziomie krajowym i odpowiada za koordynację wszelkich procesów reagowania na tzw. incydenty cybernetyczne w sektorach opisanych w art. 26 ust. 7 ustawy z dnia 5 lipca 2018r. o Krajowym systemie cyberbezpieczeństwa (Dz.U.2018, poz.1560).
Zasady działania CSIRT są w krajach europejskich ujednolicone i do głównych obowiązków takich zespołów należy rozpoznawanie, zapobieganie oraz wykrywanie zagrożeń dla obiektów, instalacji, urządzeń, usług oraz systemów należących do infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007r.o zarządzaniu kryzysowym (Dz.U. 2007nr 89 poz. 590).
Artykuł jest podzielony na sześć części. Część pierwsza zawiera kompleksowy przegląd metodologii ENISA oraz zakresu analizy zagrożeń. W części drugiej systematycznie przeanalizowano główne zagrożenia zidentyfikowane w raporcie ENISA, w tym ataki DDoS, naruszenia danych, socjotechnikę, oszustwa, oprogramowanie ransomware, złośliwe oprogramowanie i ataki na łańcuchy dostaw. Część trzecia zawiera analizę podmiotów stanowiących zagrożenie zidentyfikowane w okresie sprawozdawczym - głównie podmiotów powiązanych z państwem, cyberprzestępców i haktywistów – oraz ocenę ich możliwości, celów oraz wzorców działania. W cześci czwartej oceniono wpływ zaobserwowanych cyberincydentów na europejskie instytucje finansowe, zwłaszcza dotknięte nimi aktywa oraz implikacje sektorowe. W części piątej omówiono zastosowanie ustaleń ENISA do kontekstu polskiego sektora finansowego, zaś w części szóstej poddano badaniu nie tylko kryminologiczne ale i geopolityczne kierunki zagrożeń, wymogi zgodności z przepisami a także słabe punkty instytucjonalne. Artykuł kończy się zaleceniami dotyczącymi wzmocnienia polskiego sektora finansowego opartymi na zebranych w raporcie dowodach, zwłaszcza podkresleniu znaczenia cyberodporności systemów krytycznych poprzez stosowanie środków technicznych, organizacyjnych i przede wszystkim strategicznych zgodnie z DORA, NIS2 i międzynarodowymi najlepszymi praktykami**.**

1. Metodologia i zakres raportu ENISA dotyczącego zagrożeń

W pierwszym rzędzie należy podkreslić, że metodologia wykorzystana w Raporcie ENISA „Threat Landscape: Finance Sector” dla sektora finansowego oparta jest o zweryfikowane na przestrzeni lat metody analityczne zastosowane do badania innych sektorów gospodarki i oceny zagrożeń dla cyberbezpieczeństwa[8].
Raport ENISA „Threat Landscape: Finance Sector” wykorzystuje rygorystyczną, sprawdzoną metodologię opracowaną i udoskonaloną w ramach programów

[8] Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape: Finance sector, op.cit.s.4-5

ENISA dotyczących oceny zagrożeń dla cyberbezpieczeństwa[9] . Metodologia ta stanowi przestrzeń analityczną dla wielu strumieni danych, w tym informacji z tzw. otwartych źródeł (OSINT). W związku ze swoimi kompetencjami oraz doświadczeniem *de facto* ENISA posiada już niezależną instytucjonalną zdolność w zakresie rozpoznawania sytuacji krytycznych, poddawania ich analizom, a także ma narzędzia badawcze do analiz medialnych oraz dysponuje bazą raportów z badań dotyczących bezpieczeństwa. W ramach założeń metodologicznych uwzględniane są oficjalnie zgłoszone incydenty zgodnie z dyrektywą NIS.

Gromadzenie przez ENISA danych do raportu w szczegoności koncentrowało się na incydentach cybernetycznych mających rzeczywisty wpływ na podmioty sektora finansowego UE i krajów sąsiednich (Albania, Islandia, Liechtenstein, Mołdawia, Norwegia, Szwajcaria, Wielka Brytania i Ukraina)[10] . Zakres badań obejmował bowiem podmioty podlegające ramom regulacyjnym dyrektywy NIS i Rozporządzenia DORA, w tym instytucje kredytowe (banki), instytucje płatnicze, instytucje pieniądza elektronicznego, firmy inwestycyjne, dostawców usług związanych z kryptowalutami, centralne depozyty papierów wartościowych, kontrahentów centralnych, platformy obrotu, organizacje ubezpieczeniowe, agencje ratingowe i dostawców usług cyfrowych wspierających sektor finansowy[11] .

Z udostępnionych w raporcie danych wynika, że w okresie sprawozdawczym (styczeń 2023 r. – czerwiec 2024 r.) ENISA przeanalizowała 488 zgłoszonych publicznie incydentów mających wpływ na europejskie podmioty finansowe, w tym 432 cyberataki, 30 zorganizowanych kampanii i 26 ostrzeżeń dotyczących potencjalnych zagrożeń oraz luk pojawiających się w zabezpieczeniach. W wyniku przeprowadzonych analizy w istocie zidentyfikowano 414 incydentów w sposób wyraźny oddziaływujących na infrastructurę państw członkowskich UE oraz 74 incydenty mające wpływ na kraje sąsiednie. Niezwykle istotne jest zastrzeżenie ENISA, iż zbiór poddanych analizie danych obejmuje wyłącznie incydenty zgłoszone publicznie i nie odzwierciedla pełnego zakresu cyberincydentów mających wpływ na europejski sektor finansowy.

To ograniczenie metodologiczne odzwierciedla zjawisko niedostatecznego zgłaszania incydentów cybernetycznych przez instytucje finansowe, zwłaszcza w sprawach oszustw, gdyż ujawnienie informacji o atakach mogłoby pociągać za soba poważne ryzyka reputacyjne reputacyjne lub presję regulacyjną[12]. Dlatego zwiększone obowiązki sprawozdawcze wynikające z dyrektywy NIS i wymogów DORA mogą przyczynić się do wzrostu tzw. widoczności incydentów cybernetycznych. Należy zwrocić jednak uwagę, że ww. wzrost może w pierwszej kolejności odzwierciedlać ulepszone mechanizmy sprawozdawczości niż oznaczać bezwzględny wzrost częstotliwości ataków.

Co istotne, zgodnie z dyrektywą NIS, ENISA uzupełniła publiczne dane dotyczące incydentów o oficjalnie zgłoszone incydenty przez operatorów sektorowych usług kluczowych . Raport wskazuje, że w 2023 r. instytucje kredytowe, operatorzy systemów obrotu i kontrahenci zgłosili oficjalnie właściwym organom krajowym 155 incydentów o znaczącym wpływie,co umożliwiło uzupełnienie danych oraz

[9] Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape: Finance sector, op.cit.s.4-5

[10] Ibid.s.6

[11] IBM, Cost of a Data Breach Report 2025, Ponemon Institute, https://www.ibm.com/reports/data-breach [Dostęp: 15.11.2025].

[12] Ibid.s.14

analiz w zakresie incydentów o dużym wpływie, w stosunku do których nastapiła weryfikacja cyberodporności struktury organizacyjnej[13] .

2. Główne zagrożenia dla europejskich instytucji finansowych

W okresie sprawozdawczym ataki typu distributed denial-of-service (DDoS) stanowiły jedną z najpoważniejszych kategorii zagrożeń wpływających na europejskie instytucje finansowe. Ataki te polegały na zamierzonym przeciążaniu systemów określanych jako docelowe przez zwielokrotnioną liczbę wygenerownych sztucznie poleceń, co skutkowało niemożliwością udzielania odpowiedzi poprzez przewidywalną w danym czasie reakcję i w konsekwencji doprowadzało do wyczerpania zasobów obliczeniowych systemu oraz uniemożliwiało dostęp do usług finansowych legalnym użytkownikom.

Ataki DDoS odczuwalnie były koordynowane z wydarzeniami o charakterze geopolitycznym, w szczególności z inwazją Rosji na Ukrainę. Były też powiązane z datami oświadczeń państw członkowskich UE wspierających Ukrainę, co nadawało im określony kontekst deliktowy. Przeprowadzana comiesięczna analiza incydentów wykazała szczyty aktywności ataków DDoS w latach 2023 i 2024, zbiegające się w czasie z nasileniem w Europie retoryki antywojennej a także wydarzeniami militarnymi na Ukrainie i na Bliskim Wschodzie[14].

Dokonana przez ENISA naliza podmiotów, które były celem tychże ataków, wykazała, że około 58 % zaobserwowanych ataków DDoS było *explicite* skierowanych przeciwko europejskim instytucjom kredytowym (bankom), 21 % przeciwko oficjalnym rządowym stronom internetowym a także instytucjom zajmującym się usługami związanymi z finansami krajowymi. Ataki skierowane były zwłaszcza w kierunku stron internetowym krajowych ministerstw finansów, organów podatkowych, służb skarbowych i organów celnych[15] . Chociaż ENISA oceniła, że skutki ataków DDoS były często ograniczone ze względu na prawidłowe działania obronne to minimalizacja ich skutków odbywała się poprzez korzytsanie z komercyjnych usług naprawczych, co z kolei pociągało dla zaatakowanych instytucji znaczne obciążenie finansowe. Ataki te wymagały natychmiastowej synchronizacji pomiędzy publicznymi i prywatnymi zasobami w zakresie cyberbezpieczeństwa a to związane było z koniecznością ponoszenia dodatkowych kosztów wynikających z zakłóceń w działalności operacyjnej[16] .

Jedną z najbardziej znaczących kategorii zagrożeń wpływających na europejskie instytucje finansowe były wycieki danych ze względu na ich kwalifikowaną jako prioryetową - wysoką wartość strategiczna oraz pieniężną.

Wykryte naruszenia bezpieczeństwa danych były najcześciej konsekwencją błędnej konfiguracji systemowej, luk w zabezpieczeniach, ale także błędów oraz słabości ludzkich. Analiza ENISA wykazała, że 39% zaobserwowanych naruszeń bezpieczeństwa danych dotyczyło instytucji kredytowych, w mniejszym zakresie, aczkolwike też znaczącym innych dostawców usług finansowych (10%), jak również organizacji ubezpieczeniowych (8%), firm inwestycyjnych (8%), instytucji płatniczych (7%). Interesująca w kontekście dalszych pogłębionych badań przez pryzmat podmiotowy i przedmiotowy jest znajdująca się w raporcie informacja, że naruszenia bezpieczeństwa danych miały miejsce również wśrod dostawców usług związanych z kryptowalutami (6%).

[13] Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape: Finance sector, op.cit.

[14] Ibid.s.12

[15] Ibid.s.12

[16] Ibid.s.12

W znacznym stopniu na skutek wyżej wymienionych nieprawidłowości poszkodowani zostali klienci indywidualni. Ich dane osobowe i finansowe po bezprawnym ujawnieniu, potegowały ryzyko kradzieży tożsamości celem dokonania potencjalnych oszustw. W konsekwencji brak szczelność system i wyciek danych finansowych w sposób oczywisty wpływał na utratę zaufania do instytucji, z ktorej zostały wykradzione[17]. Znamienne jest, że sprawcy często wykorzystywali luki w zabezpieczeniach dokonując tzw. symultanicznych ataków utrudniających zlokalizowanie źródła wycieku. Były to na przykład ukierunkowane kampanie socjotechniczne takie jak kompromitacja biznesowej poczty elektronicznej, naruszenie jednego z ogniw łańcucha dostaw umożliwiające dostęp do niego stronom trzecim i dezorganizację, ale także bezpośrednie wykorzystanie luk w zabezpieczeniach oprogramowania. Istotnym przykładem takich działań było wykorzystanie krytycznej luki (CVE-2023-34362) w oprogramowaniu do przesyłania plików MOVEit przez grupę ransomware Cl0p -, które doprowadziło do jednoczesnego naruszenia bezpieczeństwa finansowego czterech dużych europejskich banków (Deutsche Bank, ING Bank, Postbank I Comdirect) za pośrednictwem ich wspólnego zewnętrznego dostawcy usług[18] .

Do niezwykle niebezpiecznych ataków socjotechnicznych – obejmujących phising, smishing (phising za pośrednictwem sms), vishing (phishing głosowy) dochodziło celem kompromitacji biznesowej poczty elektronicznej (BEC),ale także celem dokonania dyspozycji przelewów I innych zleceń o charakterze finansowym.

Ataki te wykorzystujące cechy lub słabości ludzkiego charakteru w powiązaniu z lukami w zabezpieczeniach nadal są dominującym *modus operandi* do początkowego przejęcia kontroli nad systemem i kradzieży danych uwierzytelniających. Ataki te następowały w wyniku dokonywanych przez sprawców profesjonalnych analiz ludzkich zachowań i proceców decyzyjnych celem uzyskania nieautoryzowanego dostępu lub ujawnienia poufnych informacji[19]. Phishing w okresie sprawozdawczym pozostał najpopularniejszą techniką socjotechniczną, a analiza ENISA wykazała, że 38% incydentów socjotechnicznych było skierowanych przeciwko osóbom fizycznym. Były to kampanie polegajace na podszywaniu się pod inne podmioty (głównie instytucje kredytowe), Aż w 36% ataków przy użyciu tych narzędzi było wymierzonych przeciwko organizacjom bankowym i finansowym.

Poważną, dostrzeżoną przez ENISA ewolucją taktyczną sprawcow było pojawienie się phishingu typu „adversary-in-the-middle” (AiTM), w którym atakujący umieszczali się pomiędzy legalnymi użytkownikami a systemami docelowymi w ten sposób utrudniając ich wykrycie. Działając jak bufor przechwytywali dane uwierzytelniające i kody uwierzytelniania wieloskładnikowego użytkowników, co ułatwiało im późniejsze popłenianie przestępstw. W czerwcu 2023 r. firma Microsoft zidentyfikowała precyzyjnie przygotownay, wyrafinowany, podzielony na kilka etapów atak phishingowy AiTM

[17]IBM, Raport dotyczący kosztów naruszenia bezpieczeństwa danych 2024, op.cit.

[18]E. Kovacs, Dowody wskazują, że grupa ransomware wiedziała o luce zero-day w MOVEit od 2021 r., SecurityWeek, 2023, [online], https://www.securityweek.com/evidence-suggests-ransomware-group-knew-about-moveit-zero-day-since-2021/ (Dostęp: 1.12. 2025).

[19]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Zagrożenia, op.cit.s.13

i BEC, ktorego źródłem okazał się zhakowany zaufany dostawca, co umożliwiło bezproblemowe dotarcie do wielu organizacji świadczących usługi bankowe i finansowe. Z uwagi na długoletnią współpracę I zweryfikowane źródła sprawcy obnizyli próg ryzyka I poziomy weryfikacji.
Według dnaych przedstawionychw raporcie ENISA konsekwencja ujawnionych i zgłoszonych i ujawnionych ataków socjotechnicznych były straty finansowe (50% przypadków), oszustwa i przestępstwa finansowe na dużą skalę (28%), ujawnienie i sprzedaż danych wrażliwych (19%). Warto w tym miejscu przytoczyć ocenę IOCTA z 2024, w której wskazuje, że w 2023 r. dominującą metodą phishingu stał się smishing, szybki wzrost odnotowano w przypadku quishingu (phishing z wykorzystaniem kodów QR)[20] .
Generalnie należy przypomnieć, że sektor finansowy jest sferą gospodarki o wysokich zagrożeniach reputacyjnych, podatną na informacje bezpośrednio przekładające się na sprzedaż usług i produktów finansowych, stąd walor bezpieczeństwa instytucjonalnego jest dla klientów kluczową wartością. Natomiast ujawnianie incydentów zawsze wiąże się z analizami pod kątem możliwych strat wizerunkowych a w konsekwencji spadku zaufania i wyników. Być może to stało się przyczyną stosunkowo niskiego procentowo odsetku ujawnionych oszustw na skutek cyberincydentów. Oszustwa w raporcie stanowią 6% wszystkich zaobserwowanych incydentów.
Co prawda ENISA przyznaje, że statystyka ta prawdopodobnie nie odzwierciedla w pełni rzeczywistej sytuacji ze względu na wspomniane wyżej ryzyko utraty reputacji i presję regulacyjną wywieraną na instytucje finansowe, jednak rzeczywiście udział procentowy kardynalnego z punktu widzenia sprawców przestępstwa przeciwko mieniu wymaga rzetelnych analiz, być może wspartych badaniami socjologicznymi. Niewątpliwie bowiem przyjmowano dotychczas, że cyberincydenty są dla większości sprawców narzędziem zdobywania środków pieniężnych a nie testowania ich mozliwości hakerskich czy dezorganizacji systemu finansowego z innych pobudek np.politycznych.
W nawiązaniu do danych z raportu ENISA trzeba wskazać, że incydenty skutkujące oszustwami dotknęły przede wszystkim osoby fizyczne (40%) oraz instytucje kredytowe (35%). Celem dokonania oszustw było pozyskanie danych osobowych (77%) i w mniejszym zakresie danych przedsiębiorstw (21%)[21] . Pokazuje to jak wielką wagę mają dane osobowe i właściwa ich ochrona w kontekście profilaktyki anty fraudowej. Oszustwa dokonane po użyciu danych procentowo powodowały straty finansowe (60%), zaś przestępstwa finansowe na dużą skalę (24%). Na poziomie (13%) mieściło się ujawnienie przez sprawców i sprzedaż danych wrażliwych[22] . Do istotnych typów oszustw należały podszywanie się pod pracowników pomocy technicznej banku, na co wplyw ma cały czas niewystarczająca edukacja legaltech i fintech klientów sektora finansowego oraz oszustwa inwestycyjne. W tym ostatnim przypadku szczególnie podatni na oszustwa byli klienci będący uczestnikami programów inwestycyjnych związanych z kryptowalutami. Raport też odnotował jako

[20]Europol, Ocena zagrożeń związanych z przestępczością zorganizowaną w Internecie (IOCTA), 2024. Urząd Unii Europejskiej, Luksemburg. doi:10.2813/442713 https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 [Dostęp: 11.11. 2025]

[21]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, op.cit.s.14
[22]Ibid.s.14

konsekwencję skutecznych kampanii phisingowych oraz smishingowych dużą skalę kradzieży danych kart kredytowych lub danych osobowych klientów.
Wymaga podkreślenia, że w raporcie IOCTA 2024 oszustwa, zwłaszcza o podłożu inwestycyjnym, zostały uznane za najczęściej identyfikowane przestępstwa źródłowe związane z nielegalnym wykorzystaniem kryptowalut[23].
Cyberprzestępcy coraz częściej żądają bitcoinów jako okupu, przestępcze wykorzystanie altcoinów wykazuje rosnącą tendencję. Szacuje się, że udział altcoinów w calkowitej kapitalizacji kryptowalut przekracza 37%. Usługi wymiany kryptowalut umożliwiające konwersję między środkami prywatnymi a stablecoinami stały się znaczącym czynnikiem ułatwiającym przestępstwa finansowe ze względu na ryzyka prania pieniędzy[24] .
Z raportu ENISA wynika, że przedsiębiorstwa wykazujące niższy poziom dojrzałości w zakresie cyberbezpieczeństwa doświadczały nieproporcjonalnie większego wpływu oprogramowania ransomware na swoją działalność. Wyjaśnia to stosunkowo mniejszą częstotliwość cyberincydentów wśród dojrzałych instytucji kredytowych o solidnych zdolnościach obronnych. Według raportu ataki ransomware były skierowane głównie przeciwko dostawcom usług finansowych, organizacjom ubezpieczeniowym (17 %) I instytucjom kredytowym (16 %)[25].
Analiza skutków ataków ransomware wykazała, że ich dominującymi konsekwencjami były straty finansowe (38 %), ujawnienie oraz sprzedaż danych wrażliwych (35 %), a także zakłócenia w działalności operacyjnej (20 %)[26].
Oprogramowanie ransomware, definiowane są jako forma cyberataku, w ramach którego podmioty stanowiące zagrożenie przejmują kontrolę nad aktywami osob trzecich i żądają zapłaty okupu w zamian za przywrócenie im dostępu do tych aktywów.
Nieujawnianie przez instytucje i podmiotuy sektora finansowego faktu oraz skali skradzionych danych, stanowiło główne zagrożenie dla statystyk i wniosków. Trzeba jednak odnotować w raporcie względnie mniejszą częstotliwość występowania tego zjawiska w porównaniu do ataków na inne sektory[27].
ENISA wskazuje na istotne warianty oprogramowania ransomware wykorzystane w okresie sprawozdawczym. Należały do nich: Akira (oprogramowanie pojawiające się w marcu 2023 r., generujące do stycznia 2024 r. około 42 mln USD z tytułu okupów). Cl0p/FIN11 (oprogranmowanie działające w modelu ransomware-as-a-service) i zlikwidowany w lutym 2024 r. w wyniku interwencji organów ścigania w ramach operacji Cronos[28] LockBit (najczęściej wykorzystywany wariant w 2022 r.
Według danych przedstawionych w raporcie Incydenty związane ze złośliwym oprogramowaniem, z wyłączeniem kategorii oprogramowania ransomware, stanowiły 6% wszystkich incydentów (21 przypadków). Często dotykały one duże

[23]Europol, Ocena zagrożeń związanych z przestępczością zorganizowaną w Internecie (IOCTA), op.cit.s.13
[24]Ibid.s.13

[25]Ibid.s.13-14
[26]Tamże.
[27]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Zagrożenia, op.cit.
[28]Europol, Organy ścigania rozbijają największą na świecie operację ransomware, komunikat prasowy, luty 2024 r., https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation, [dostęp 04.11.2025]

grupy osób ze względu na ataki na urządzenia bankowości osobistej[29] . Oszustwa dokonywane na skutek infekcji złośliwego oprogramowania na aplikacjach mobilnych stały się istotnym podtypem zagrożeń, zwłaszcza wobec wzrostu tendencji korzystania z aplikacji mobilych przez klientów detalicznych I rosnącej tendencji do dokonywania tą drogą transakcji finansowych.

Warto zwrócić uwagę na znaczny wzrost zaawansowania trojanów w bankowości mobilnej jaki nastąpił w okresie objętym raportem. Badania wykazały 200-procentowy wzrost liczby rodzin złośliwego oprogramowania atakujących aplikacje bankowe w ujęciu rok do roku. Progres w tej kwestii pokazuje statystyka, gdzie dotychczas globalnie 10 różnych grup hakerskich miało zdolność do ataku i atakowało 600 aplikacji zaś obecnie 29 grup jest w stanie w sposób nieprzerwany atakować 1800 aplikacji[30].

Modus operandi sprawcow jest dosyć klasyczny. Atakujący przejmują kontrolę nad urządzeniami, umożliwiając kradzież danych uwierzytelniających, następnie wykonywanie fałszywych transakcji oraz całkowite przejmowanie kontroli nad urządzeniami. Raport zidentyfikował w europejskich incydentach oraz określił jako istotne trojany bankowości mobilnej następujące trojany: Anatsa (atakujący Czechy), Mispadu (atakujący Włochy, Polskę i Szwecję), Godfather (atakujący aplikacje bankowe UE), Medusa/TangleBot (atakujący Hiszpanię, Turcję, Włochy, Francję), Hydra (atakujący urządzenia z systemem Android w Polsce), Copybara (atakujący Wielką Brytanię, Hiszpanię i Włochy), Bizarro (atakujący klientów europejskich banków). Analiza danych, które zostały zebrane *post factum* ujawniła w tej części sektora finansowego oszustwa i przestępstwa finansowe na dużą skalę (59%), straty finansowe (21%), ujawnienie i sprzedaż poufnych informacji (14%) oraz zakłócenia operacyjne (7%)[31] .

W okresie sprawozdawczym ENISA zidentyfikowała również 29 incydentów związanych z atakami na łańcuch dostaw. Dotyczyły one głównie naruszeń bezpieczeństwa danych przez oprogramowania ransomware skierowane przeciwko dostawcom usług, dostawcom infrastruktury cyfrowej, dostawcom usług w chmurze i dostawcom usług płatniczych

Ataki na łańcuch dostaw skierowane przeciwko dostawcom usług, umożliwiały naruszenie bezpieczeństwa, następnie rozprzestrzeniały się na wiele instytucji finansowych, stając się niepokojącą kategorią zagrożeń. Ataki te wykorzystywały zaufane relacje i wzajemne zależności w sektorze finansowym, tym samym umożliwiając atakującym ominięcie bezpośrednich zabezpieczeń instytucjonalnych poprzez naruszenie bezpieczeństwa dostawców[32]. Analiza skutków takich ataków wykazała ujawnienie i sprzedaż danych wrażliwych (63%), zakłócenia operacyjne (26%) oraz straty finansowe (11%). Ataki te często narażały jednocześnie wiele instytucji finansowych wykorzystując wielopoziomowo wspólne relacje z dostawcami usług I brak odpowiednich zapór, czego przykładem jest wykorzystanie luki w zabezpieczeniach MOVEit, które dotknęło Deutsche Bank, ING, Postbank i Comdirect.

3. Analiza podmiotów stanowiących zagrożenie i ich celów

[29]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, op.cit.
[30]Tamże.
[31]Tamże.

[32]Tamże.

Raport zwrócił uwagę na niedostrzeżone dotychczas na taką skalę motywy działania sprawców cyberincydentów *prima facie* nie dotyczące bezpośredniego uzyskania korzyści majątkowych. Rynek finansowy poza oczywistą funkcją gospodarczą ma niebagatelne znaczenie dla zapewnienia stabilności i bezpieczeństwa państwa. To z kolei implikuje założenie, że może być atrakcyjną przestrzenią do ataków o charakterze politycznym.

Podmioty powiązane z państwami realizowały dotyczas swoje cele skupiając się głównie na szpiegostwie gospodarczym i gromadzeniu informacji strategicznych. Jednak w ostatnim czasie widać dywersyfikację działań i kierunków cyberprzestępczości, których celem jest osiągnięcia przy pomocy wehikułów politycznych określonych korzyści finansowych lub uniknięcia sankcji.

Grupy powiązane z państwami, które atakują europejskie instytucje finansowe, zazwyczaj stosują zaawansowane techniki zrównoważonych zagrożeń. Charakteryzują się one specjalistrycznym rozpoznaniem, wydłużonymi ramami czasowymi operacji oraz zaawansowanymi możliwościami technicznymi. Wszystkie te czynniki łącznie mają za zadanie zminimalizowanie ryzyka wykrycia.

Do istotnych pejoratywnych działań powiązanych z państwami a oddziaływujacymi na sektor finansowy w cyberprzestrzeni należą działania grup z Korei Północnej (w szczególności Lazarus Group[33]) prowadzących operacje kradzieży kryptowalut i wdrażania oprogramowania ransomware. Przykładowo FBI zidentyfikowało Lazarus Group jako odpowiedzialną za kradzież 41 mln USD z giełdy kryptowalut Stake.com we wrześniu 2023 r., co niezbicie świadczy o wykorzystywaniu infrastruktury technologii finansowej przez atakujące grupy powiązane z państwem[34].

W tym kontekście konieczne jest wskazanie rownież na chińskie grupy wyspecjalizowane w zaawansowanych technologiach, w tym APT10 (Stone Panda), które atakowały tajwańskie instytucje finansowe za pomocą ataków typu zero-day. Ataki odbywały się w ten sposob, iż grupy penetrowały łańcuchy dostaw a na celu miały pozyskanie poufnych danych i własności intelektualnej. W sposób oczywisty niebezpieczne sa powiązane z państwem rosyjskie grupy APT, w tym APT29 (niezaprzeczanie związana z rosyjskimi służbami wywiadowczymi), które atakowały europejskie instytucje finansowe w ramach operacji cyber-szpiegostwa i pozyskiwania informacji.

Należy wyraźnie podkreslić, że podmioty powiązane z państwem coraz częściej wykorzystują znane strategie i zero-day luki w zabezpieczeniach, aby ułatwić sobie nieautoryzowany dostęp do systemów. Aspektem interesującym z kryminologcznego punktu widzenia jest wykorzystanie tych luk często wiele miesięcy lub lat po ich wykryciu[35] .

Na podstawie raportu można stwierdzić, iż w odrożnieniu od podmiotów powiązanych z państwami głównym celem niepowiązanych grup

[33]Grupa Lazarus była zaangażowana w kampanie szpiegostwa wojskowego oraz sabotaż instytucji finansowych, mediów i fabryk. Większość ofiar pochodzi z Korei Południowej, Indii, Chin, Brazylii, Rosji i Turcji. Cyberprzestępcy stworzyli złośliwe oprogramowanie Hangman (2014–2015) oraz Wild Positron (znane również jako Duuzer, 2015).

[34]Federalne Biuro Śledcze, FBI identyfikuje cyberprzestępców z grupy Lazarus jako odpowiedzialnych za kradzież 41 milionów dolarów ze strony Stake.com, komunikat prasowy, 2023. https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-responsible-for-theft-of-41-million-from-stakecom [Dostęp: 4 grudnia 2025].

[35]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, op.cit.

cyberprzestępczych jest osiągnięcie korzyści finansowych poprzez bezpośrednią kradzież, wymuszenia lub monetyzację skradzionych danych. W okresie objętym sprawozdaniem cyberprzestępcy coraz częściej wykorzystywali luki typu zero day oraz techniki inżynierii społecznej oparte na sztucznej inteligencji. Dostrzeżono również zastosowanie modelu ransomware-as-a-service (RaaS).
Mając na względzie mniej zaawansowane narzędzia do prowokowania incydentów cybernetycznych grupy takie prowadziły operacje cyberprzestępczości finansowej o niższych barierach wejścia[36].
Na pewno należy zwrocić uwagę na coraz większą dostępnośc technologii AI I jej wpływ na narzędzia stosowane przez grupy cyberprzestępcze w sektorze finansowym. Z ustaleń raportu można wywieść, że sztuczna inteligencja coraz częściej wykorzystywana jest do zwiększania skuteczności kampanii socjotechnicznych. Sprawcy wykorzystują generowanie skryptów phishingowych opartych na sztucznej inteligencji, technologię deepfake do podszywania się pod inne osoby za pomocą głosu i wideo. Przed zdemaskowaniem używają zaś broni w postaci zautomatyzowanych cyfrowych technik kamuflujących służacych do omijania wykrywania oszustw.
Warto też zwrócić uwagę na inne podmioty działające w sferze sektora finansowego to jest haktywistów. Grupy te dążąc do zmian społecznych lub politycznych, głównie z powodów ideologicznych i politycznych wykorzystują cyberataki dla osiągania swoich celów.[37] Jedną z najbardziej znanych grup haktywistycznych o pozytywnych konotacjach jest grupa Anonymous, jednak nie każda ideologia będzie korzystnym lub neutralnym czynnikiem, zawsze będzie to czynnik podwyższonego ryzyka, gdyż abstrahując od rzeczywistych motywów działalności, skutkiem jest nieuprawniona ingerencja w system.
Dlatego pomimo, że podstawowym motywem działania haktywistów jest zwrócenie uwagi na problemy, które eksponują w ramach swojej działalności, często z uwagi na posiadanie wysokich umiejętności mogą stać się narzędziem w rękach cyberprzestępców. W okresie objętym raportem podmioty stanowiące zagrożenie haktywistyczne coraz częściej koordynowały swoje działania z podmiotami powiązanymi z państwem. Działały pod potencjalnym patronatem państwa, zwiększając stopień zaawansowania operacyjnego[38] .

---

[36]Ibid. Do znanych grup cyberprzestępczych zajmujących się oprogramowaniem ransomware należą: Akira – grupa oferująca oprogramowanie ransomware jako usługę, która pojawiła się w marcu 2023 r. i atakuje różne branże na całym świecie, ze szczególnym uwzględnieniem sektora finansowego i ubezpieczeniowego, generując do stycznia 2024 r. 42 mln USD z tytułu okupów, wykorzystując taktykę podwójnego wymuszenia, łączącą szyfrowanie danych z groźbą ich ujawnienia. Cl0p (FIN11) – grupa przestępcza działająca od lutego 2019 r. w celach finansowych, wykorzystująca model ransomware-as-a-service do rekrutacji partnerów, szczególnie aktywna w wykorzystywaniu luk w łańcuchu dostaw i exploitów typu zero-day. Grupa wykorzystała lukę CVE-2023-34362 w oprogramowaniu MOVEit, atakując wiele europejskich instytucji finansowych. LockBit – pojawiła się w 2019 r., prawdopodobnie pochodzi z Europy Wschodniej, działa w modelu ransomware-as-a-service, atakując różne sektory przemysłowe na całym świecie, w tym usługi finansowe. Była najczęściej stosowaną odmianą oprogramowania ransomware w 2022 r., zanim została zlikwidowana w wyniku interwencji organów ścigania w ramach operacji Chronos (luty 2024 r.).

[37] Zob.szerzej: Raport o stanie bezpieczeństwa cyberprzestrzeni RP,s. 53-79 file:///C:/Users/User/Downloads/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2024.pdf

[38]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, op.cit.

4. Ocena wpływu i konsekwencje sektorowe

Analiza obszarów, na które wywarły wpływ cyberataki, wykazała, że najczęściej atakowaną kategorią była infrastruktura informatyczna (31% incydentów). Oznacza to, iż krytyczną bazą o charakterze materialnym są serwery, routery, zapory sieciowe i inne komponenty sieciowe mające kluczowe znaczenie dla efektywnego prowadzenia działalności finansowej . Drugą najczęściej atakowaną kategorią były dane operacyjne i infrastruktura podporządkowana (28%), obejmująca dane handlowe, systemy płatnicze i infrastrukturę bankomatów[39] .

Analiza sektorowa na poziomie podmiotów wykazała, że najczęściej atakowanymi podmiotami były europejskie instytucje kredytowe (46% wszystkich incydentów, czyli 301 incydentów). Znacząco rzadziej atakowane były agencje rządowe i organizacje sektora publicznego związane z finansami (13%) oraz najsłabiej indywidualni klienci usług finansowych (10%). Procentowy podział nieuprawnionych ingerencji wskazuje profil instytucji bankowych jako celów o wysokiej wartości.

Główne obszary cyberincydentów to zakłócenia operacyjne, sprzedaż wrażliwych danych, oszustwa i przestępstwa finansowe na dużą skalę oraz związane z ww.czynnikami straty finansowe wielkich rozmiarów. Zakłócenia operacyjne uniemożliwiały przetwarzanie transakcji, opóźniały kluczowe działania finansowe w konsekwencji ograniczały klientom dostęp do środków bankowych. Wszystkie wymienione sytuacje niosą daleko idące konsekwencje dla reputacji i kondycji sektora finansów.[40] Ujawnienie danych i późniejsze pojawienie się ich na rynku dark web umożliwiało lub znacznie ułatwiało wtórną działalność przestępczą, kradzież tożsamości doprowadzały w konsekwencji do oszustw finansowych. Straty finansowe wynikały wprost z kradzieży, płatności okupów, kosztów reagowania na incydenty i napraw, kar regulacyjnych oraz podwyższonych składek ubezpieczeniowych.

Szczególnie poważną długoterminową konsekwencją cyberincydentów, wielokrotnie przenikającą dane raportu ENISA była utrata reputacji, ponieważ status instytucji finansowych w poważnym stopniu zależy od zaufania klientów.

Do znanych grup haktywistów należą -NoName057(16) – prorosyjskie ugrupowanie haktywistów, które pojawiło się na początku 2022 r. i wykorzystuje ataki DDoS oparte na crowdsourcingu za pośrednictwem Telegramu i projektu oprogramowania DDoSia. Cele ataków są ściśle powiązane z rosyjskimi interesami geopolitycznymi, co sugeruje potencjalną koordynację na szczeblu państwowym i dostęp do zaawansowanych technologii oraz możliwości nieskręoowanego działania. W okresie sprawozdawczym atakowała europejskie instytucje kredytowe i rządowe służby finansowe. Turk Hack Team (THT) – turecka grupa nacjonalistyczna przeprowadzająca ataki DDoS o podłożu politycznym na instytucje finansowe, w tym Bank Centralny Malty i grupę Crédit Agricole, wykazując motywacje geopolityczne. UserSec – prorosyjskie ugrupowanie cyberprzestępcze atakujące kraje NATO i zwolenników Ukrainy z pobudek politycznych. W grudniu 2023 r. rzekomo przeprowadziła ataki DDoS na banki centralne Łotwy i Polski. Anonymous Sudan – powstała na początku 2023 r., przeprowadziła głośne cyberataki na różne sektory, w tym instytucje finansowe. Atakowała Europejski Bank Inwestycyjny atakami DDoS (czerwiec 2023 r.) i koordynowała działania z prorosyjskimi grupami atakującymi organizacje wspierające Ukrainę.

[39]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape, op.cit

[40]Ibid.

ENISA przyznała, że skutki w postaci utraty reputacji były trudne do oszacowania w analizowanym zbiorze dotyczączym incydentów, ale oceniła je jako znaczące wtórne konsekwencje badanych naruszeń .

5. Zastosowanie ustaleń ENISA w polskim sektorze finansowym

Polski sektor finansowy działa w specyficznym kontekście geopolitycznym, w którym narażony jest na zagrożenia cyberbezpieczeństwa silniej niż dotychczas w historii nie tylko ze wzgkędu na położenie w pobliżu stref konfliktu zbrojnego, ale także jako państwo członkowskie NATO, udzielające aktywnego wsparcia zaatakowanej przez Rosję Ukrainie. Z uwagi na powyższe Polska stoi w obliczu podwyższonego ryzyka cyberzagrożeń ze strony podmiotów powiązanych z Rosją, cyberprzestępców umożliwiajacych omijanie sankcji oraz grup haktywistów sprzyjających interesom Rosji.

Podwyższony poziom zagrożeń potwierdzają [41] dane statystyczne. Według raportu Check Point Software Technologies „2025 Security Report" polskie instytucje finansowe doświadczają około 1750 cyberataków tygodniowo, co przekracza średnią światową wynoszącą 1510 ataków tygodniowo. Polskie Ministerstwo Cyfryzacji zgłosiło 113 600 poważnych cyberataków we wszystkich sektorach w 2024 r. NASK odnotowało ponad 130 000 incydentów cybernetycznych w tym okresie. Statystyki te plasują polskie instytucje finansowe wśród najczęściej atakowanych w Europie[42] . W listopadzie 2025 r. największy polski system płatności cyfrowych BLIK został zaatakowny rozproszonymi atakami typu denial-of-service. Spowodowały one powazne zakłócenia w transakcjach. Przypisano je tzw. źródłom „zewnętrznym", podkreślajac ich związek z trwającymi zagrożeniami hybrydowymi związanymi z konfliktem wojennym za wschodnią granicą. W październiku 2025 r. firma pożyczkowa SuperGrosz doświadczyła znacznego naruszenia bezpieczeństwa, gdyż zaatakowane zostały dane osobowe jej klientów i numery identyfikacyjne[43] .

Polskie instytucje finansowe stoją przed trudnym wyzwaniem, monitoringu i egzekwowania zgodności z przepisami, ustawy o odporności operacyjnej w środowisku cyfrowym (DORA)[44] oraz dyrektywy o bezpieczeństwie sieci i informacji 2 (NIS2). Muszą również raportować wypełnianie równoległych obowiązków wynikających z ogólnego rozporządzenia o ochronie danych (RODO) i polskiej ustawy o krajowym systemie cyberbezpieczeństwa (UKSC).

Zgodnie z polską ustawą o krajowym systemie cyberbezpieczeństwa działalność podmiotów rynku finansowego sklasyfikowanych jako operatorzy usług kluczowych jest poddawana ocenie CSIRT KNF. Zespół CSIRT koordynuje reakcje na incydenty, analizuje i zbiera informacje o zagrożeniach, bada zgodność ich działań z przepisami dla banków, firm ubezpieczeniowych, instytucji

[41]Polska Agencja Inwestycji i Handlu (PAIH), Fintech. Cyber. Biometria. Twoje zaufane trio z Polski, Warszawa, 2025, (|20.05.2025), [dostęp 01.10.2025].

[42]Ministerstwo Cyfryzacji, Krajobraz cyberprzestrzeni: roczne sprawozdanie o cyberbezpieczeństwie za 2024 rok. Warszawa, 2025, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie [Dostęp 01.12.2025].

[43]Polska Agencja Prasowa, Client data leaked in hack on Polish online lender, 02.11.2025, https://www.pap.pl/en/news/client-data-leaked-hack-polish-online-lender, [dostęp 15.11. 2025].

[44]Zob. M.Lemonnier (red.) DORA. Operacyjna odporność cyfrowa sektora finansowego. Komentarz. Wolters Kluwer 2025, Bejm T., Gryber M., Kisiel S., Lemonnier M. (red.), Mariański M., Pałka P., Sowińska-Kobelak D., Turczynowicz-Kieryllo J.

płatniczych i dostawców usług związanych z kryptowalutami[45] . Obowiązki sprawozdawcze podmiotów finansowych w zakresie zgłaszania związanych z ICT incydentów I znaczących cyberzagrożeń sa realizowane poprzez udostępniony przez CSIRT KNF system do obsługi incydentów DORA pod adresem https://csirt.knf.gov.pl. Procedura zgłaszania incydentów jest zabezpieczona na wypadek niemożności zrealizowania sprawozdania poprzez system i opiera sie na formularzach wysyłanych na dedykowany adres mailowy: incydenty.dora@knf.gov.pl

Sektorowy zespół reagowania na incydenty związane z cyberbezpieczeństwem Komisji Nadzoru Finansowego (CSIRT KNF) udokumentował niepokojące trendy w obszarze zagrożeń charakterystycznych dla polskich instytucji finansowych. W 2024 r. wykryto bowiem ponad 51 000 domen phishingowych atakujących polski sektor finansowy, z czego przeważająca ilość, bo około 46 000 było ukierunkowanych na fałszywe programy inwestycyjne. Dane te są zgodne z tendecją ustaloną w raporcie ENISA. Rzeczywiście to phishing stanowi dominujący schemat ataków w przypadku oszustw finansowych i początkowego naruszenia bezpieczeństwa systemów[46] .

Reguły kształtowania odporności cyfrowej instytucji finansowych oraz zasady bezpieczeństwa klientów bankowości przede wszystkim zostały uregulowane przez dwie kluczowe regulacje UE wzmacniające cyberbezpieczenstwo. DORA ustanawia kompleksowe wymagania dotyczące odporności operacyjnej w obszarze cyfrowym. Mają one zastosowanie w instytucjach kredytowych, płatniczych, instytucji pieniądza elektronicznego, firmach inwestycyjnych, u dostawców usług związanych z kryptowalutami oraz kluczowych zewnętrznych dostawców usług ICT. DORA nakłada obowiązek wdrożenia ram zarządzania ryzykiem, zdolności reagowania na incydenty, audytów bezpieczeństwa przeprowadzanych przez podmioty zewnętrzne, testów penetracyjnych opartych na zagrożeniach oraz wymogów dotyczących zgłaszania incydentów związanych z cyberbezpieczeństwem. Polskie instytucje finansowe muszą zapewnić zgodność z DORA poprzez politykę organizacyjną, kontrolę bezpieczeństwa i protokoły zarządzania incydentami. Warto podkreslić, że Rozporządzenie realizuje istniejące wytyczne Europejskiego Urzędu Nadzoru Bankowego.

NIS2 rozszerza wymagania dotyczące zarządzania cyberbezpieczeństwem poza ograniczony zakres dyrektywy NIS, obejmując „ważne" podmioty w sektorach świadczenia usług cyfrowych, energetyki, transportu, bankowości opieki zdrowotnej i gospodarki wodnej oraz nnych usług publicznych.

W tym znaczeniu zakres Dyrektywy jest szerszy podmiotowo niż Rozporządzenia Dora, jednak to DORA będzie traktowana jako *lex specialis* w przypadku rozbieżności interpretacyjnych dla sektora finansowego, zwłaszcza w zakresie specyficznych wymagań dotyczących odporności operacyjnej i zarzadzania ryzykiem ICT. Zgodnie z polskim wdrożeniem NIS2 poprzez zmiany w ustawie o krajowym systemie cyberbezpieczeństwa określone zostały wymogi dotyczące zgłaszania incydentów oraz mechanizmy nadzoru i egzekwowania, w tym kary finansowe w wysokości do 10 mln euro lub 2% rocznego obrotu dla podmiotów krytycznych.

[45]Tamże.

[46]Komisja Nadzoru Finansowego, Raport roczny CSIRT KNF za rok 2024, Warszawa 2025, https://www.knf.gov.pl/en/?articleId=93273&p_id=19, [dostęp 15.11.2025].

Z uwagi na wage problematyki Komisja Nadzoru Finansowego wydała komunikaty sektorowe wymagające od instytucji finansowych samooceny zgodności z DORA, wdrożenia kontroli technicznych oraz zwiększenia odporności organizacyjnej. KNF ogłosiła planowane uchylenie wcześniejszych zaleceń dotyczących bezpieczeństwa IT, dokumentów zawierających wytyczne oraz „komunikatów dotyczących chmury", eliminując tym samym powielanie obowiązków wynikających z DORA i zmniejszając obciążenia regulacyjne. Działania te mają bezpośredni wpływ na wzmocnienie obowiązkowych ram zgodności[47] .

6. Analiza porównawcza: zagrożenia ENISA a słabe punkty w zakresie cyberbezpieczeństwa. Zalecenia dotyczące wzmocnienia odporności polskiego sektora finansowego.

Analiza porównawcza typologii zagrożeń udokumentowanych przez ENISA i udokumentowanych słabych punktów Polski wykazuje znaczną zbieżność i jednocześnie identyfikuje czynniki wzmacniające zagrożenia specyficzne dla Polski. Podczas gdy ENISA udokumentowała szczyty ataków DDoS skorelowane z wydarzeniami geopolitycznymi pośrednio związanymi z sytuacją w Ukrainie, polskie instytucje stanęły w obliczu podwyższonego i utrzymującego się ryzyka ataków DDoS ze względu na bezpośrednie zaangażowanie we wsparcie Ukrainy. Jest empirycznie potwierdzone, że grupy haktywistów, w tym NoName057(16), UserSec i Anonymous Sudan, atakują polskie instytucje finansowe i rządowe usługi finansowe. Wynikający z ataków poziom zagrożeń przekracza podstawowe poziomy ryzyka w Europie[48].

ENISA zidentyfikowała trojany bankowości mobilnej (Mispadu, Hydra) atakujące polskich klientów. Kampanie Mispadu koncentrowały się na Polsce, Włoszech i Szwecji. Hydra atakowała urządzenia z systemem Android w Polsce.

Koncentracja tej rodziny złośliwego oprogramowania odzwierciedla wysoki poziom adopcji technologii fintech i bankowości mobilnej w Polsce. Ważne w tym miejscu jest wskazanie, że polskie instytucje finansowe w dużym stopniu polegają na zewnętrznych dostawcach usług, w tym dostawcach infrastruktury chmurowej, dostawcach usług płatniczych i operatorach infrastruktury cyfrowej.

Dokumentacja ENISA na temat częstości występowania ataków na łańcuch dostaw poprzez wykorzystanie luki w zabezpieczeniach MOVEit (dotyczącej czterech dużych europejskich banków korzystających z usług tych samych dostawców) unaocznia skalę narażenie Polski na zagrożenia pochodzących od podmiotów zewnętrznych.

Podobnie ocena ENISA, że mniej dojrzali dostawcy usług finansowych ponoszą nieproporcjonalne koszty ataków ransomware, odzwierciedla strukturę polskiego sektora wobec cyberincydentów. Duże banki komercyjne co do zasady wykazują dojrzałą postawę w zakresie cyberbezpieczeństwa natomiast pośrednicy ubezpieczeniowi, firmy inwestycyjne i mikroprzedsiębiorstwa charakteryzują się podwyższonym poziomem podatności na cyberzagrożenia[49].

Zaobserwowane przez ENISA zaniżania liczby zgłoszeń oszustw ze względu na obawy o reputację i presję regulacyjną jest szczególnie istotne w kontekście

[47]Komisja Nadzoru Finansowego, Pismo sektorowe w sprawie wymogów zgodności z ustawą o odporności operacyjnej cyfrowej (DORA), Warszawa 2024, https://www.knf.gov.pl/en/MARKET/CSIRT_KNF.

[48]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape op.cit.

[49]Ibid.

polskim, gdzie kary regulacyjne i konsekwencje dla adekwatności kapitałowej stanowią silny czynnik zniechęcający do ujawniania oszustw[50] .
Polskie instytucje finansowe muszą priorytetowo traktować inwestycje w zaawansowane systemy wykrywania zagrożeń i reagowania na nie, obejmujące systemy wykrywania włamań, systemy zapobiegania włamaniom oraz rozwiązania służące do zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) oraz mieć zsynchronizowane i ujednolicone w zakresie podstawowych standardów podejście do kwestii testowania odporności cyfrowej oraz przeprowadzania testów penetracyjnych. Przede wszystkim zaś tworzyć zaawansowane komplekowe strategie zarządzania ryzykiem oraz informacją. Niezależnie od tego inwestowanie w systemy umożliwiające wykrywanie anomalii w czasie rzeczywistym pozwalać będzie na automatyczne reagowanie na incydenty[51] .
Konieczne analizy predykcyjne niewątpliwie może ułatwić integracja technologii sztucznej inteligencji i uczenia maszynowego. Dzieki temu instytucje finansowe mają szanse osiagnąć zdolność identyfikacji pojawiających się wzorców ataków i proaktywnie ograniczać zagrożenia.
Ze względu na dostrzeżoną w raporcie ENISA nieprawidłowość naruszenia DORA, NIS 2, RODO to jest poufności danych zasadne jest wdrożenie uwierzytelniania wieloskładnikowego (MFA) w dostępie pracowników i klientów do krytycznych systemów i danych. Taka podstawowa kontrola bezpieczeństwa ma szansę zapobiegać bezprawnemu wykorzystaniu danych uwierzytelniających.
Dokumentacja ENISA dotycząca technik phishingu typu „adversary-in-the-middle", omijających tradycyjne MFA poprzez przechwytywanie danych uwierzytelniających, wymagać będzie wdrożenia sprzętowych kluczy bezpieczeństwa i technologii powiązań urządzeń odpornych na zaawansowane ataki przechwytywania. Kompleksowe programy zarządzania ryzykiem stron trzecich muszą natomiast oceniać stan cyberbezpieczeństwa dostawców pamietając, iż sfera ta co wynika z raportu ENISA , ale także orzeczeń sądowych może być słabym punktem w zakresie cyberodporności. Instytucje finansowe wymagają mechanizmów ciągłego monitorowania praktyk bezpieczeństwa stron trzecich, zobowiązań umownych nakładających obowiązek zgłaszania incydentów i usuwania ich skutków oraz planów awaryjnych umożliwiających ciągłość usług w przypadku naruszenia bezpieczeństwa przez stronę trzecią. Systematyczne wzmacnianie bezpieczeństwa infrastruktury IT, zasobów przetwarzania w chmurze oraz procesów wdrażania oprogramowania/sprzętu zmniejsza narażenie na podatności, które mogą wykorzystać grupy stanowiące zagrożenie. Podkreśla się, że wdrożenie obejmuje wyłączenie zbędnych usług, wdrożenie restrykcyjnych kontroli dostępu, hostowego systemu wykrywania włamań oraz ustanowienie podstawowych zasad zarządzania konfiguracją[52] .
Ponieważ przeważająca część cyberincydentów następuje poprzez wykorzystanie socjotechniki stanowi ona stały czynnik ataku. Konieczne i rekomendowane są programy szkoleniowe dotyczące rozpoznawania phishingu, ochrony danych uwierzytelniających, taktyk socjotechnicznych i wymagań dotyczących zgłaszania incydentów oraz podstaw prawnych w zakresie

[50]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape op.cit .
[51]Ibid.

[52]Por. M. Lemonnier (red.) DORA. Operacyjna odporność cyfrowa sektora finansowego, op.cit.

rozumienia podstawowych znamion czynów zabronionych. Edukacja w tym względzie jest w stanie w sposób wydatny znacznie zmniejszyć skuteczność ataków socjotechnicznych.

Duże efekty profilaktyczne mogą przynieść również symulowane ćwiczenia phishingowe zapewniają praktyczne szkolenie umożliwiające w rzeczywistości pracownikom rozpoznawanie i zgłaszanie zaistniałych prób phishingu[53] . Dobrze zdefiniowane plany reagowania na incydenty, określające procedury wykrywania, powstrzymywania, eliminowania, odzyskiwania i komunikacji są wręcz niezbędne do zminimalizowania skutków naruszeń i kar regulacyjnych.

Odporność w zakresie cyberbezpieczeństwa wymaga wyraźnego zaangażowania zarządów, uświadomienia prawnej odpowiedzialności za zaniedbania, lekceważenie oraz niedopełnineie obowiązków szczególnego zaangażowania wobec nowych niespotykanych wcześniej zagrożeń. Naturalnie wymaga to również dedykowanych budżetów na bezpieczeństwo I odpowiedzialności kadry kierowniczej za wdrażanie programów bezpieczeństwa. Postuluje się, iż dyrektorzy ds. bezpieczeństwa informacji (CISO) powinni podlegać bezpośrednio kierownictwu wyższego szczebla i zarządom. Cyberodporność I cyberbezpieczeństwo od strony strategicznej winno być traktowane jako strategiczny priorytet równy zarządzaniu ryzykiem finansowym i operacyjnym[54] .

Polskie instytucje finansowe z całą pewnością muszą wdrożyć kompleksowe programy zgodności z DORA, obejmujące zarządzanie ryzykiem organizacyjnym. KNF wymaga dokumentacji samooceny wykazującej zgodność z wymogami DORA w obszarach zarządzania, zarządzania ryzykiem, kontroli ICT i zgłaszania incydentów. DORA przewiduje wysokie sankcje za nieprzestrzeganie przepisów[55] .

Wdrożenie wymogów NIS2 i polskiej ustawy o krajowym systemie cyberbezpieczeństwa w zakresie systemów zarządzania bezpieczeństwem informacji, protokołów zgłaszania incydentów, i odzyskiwania danych po awarii oraz audytu bezpieczeństwa wzmacni ich odporność instytucjonalną.

W związku z nowymi zagrożeniami w historii oraz brakiem długofalowych badań czy też doswiadczeń systemowych cenne okazać się mogą platformy wymiany informacji o zagrożeniach, sektorowe centra analizy i wymiany informacji (ISAC) oraz partnerstwa publiczno-prywatne. Uczestniczenie w tego typu forach umożliwi instytucjom finansowym dostęp do aktualnych informacji o zagrożeniach I pozwoli na cenne porównanie praktyk w zakresie bezpieczeństwa oraz koordynację wspólnych reakcji na pojawiające się zagrożenia. Wspólną identyfikację zagrożeń i zwiększanie zdolności reagowania wspiera i Koordynuje CSIRT KNF wraz z uczestnikami sektora bankowego [56] .

Należy podkreślić, że również polska judykatura potwierdza pilną potrzebę wzmocnienia środków bezpieczeństwa banków wobec cyberincydentów. W szczególności *per analogiam* można stosować linię orzeczniczą i doktrynalną w zakresie zaniedbań managementu instytucji finansowych co do zapewnienia odpowiednich zabezpieczeń I szkód powstałych w związku z zaniedbaniami w tym zakresie. Jedynie sygnalizacyjnie dla zobrazowania problematyki można

[53]Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA Threat landscape, op.cit.
[54]Por. M.Lemonnier (red.) DORA. Operacyjna odporność cyfrowa sektora finansowego,, op.cit.
[55]J.Turczynowicz- Kieryłło, Art. 50-55, (w) M.Lemonnier(red.), DORA. Operacyjna odporność cyfrowa sektora finansowego, op. cit.s.277-311.
[56]Komisja Nadzoru Finansowego, Raport roczny CSIRT KNF 2024, op.cit.

przytoczyć orzeczenie Sądu Najwyższego w sprawie II CSKP 1013/22 z dnia 15 września 2023 r. Powód, klient banku, doświadczył nieuprawnionego dostępu do swojego konta w dniu 15 marca 2018 r. Hakerzy przechwycili kod SMS wysłany przez bank, zalogowali się na konto powoda, a następnie, korzystając z drugiego przechwyconego kodu SMS, manipulowali systemem bankowości elektronicznej w celu dodania zaufanego odbiorcy krajowego, dla którego nie było wymagane dodatkowe upoważnienie. Z konta powoda wykonano trzy przelewy o łącznej wartości 118 464 PLN – o godz. 9:42:03 (38 788 PLN), o godz. 11:38:07 (39 988 PLN) oraz o godz. 14:49:22 (39 688 PLN). Sąd Najwyższy potwierdził, że bank ponosi odpowiedzialność za nieautoryzowane transakcje płatnicze zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych. Kluczowym ustaleniem Sądu była wrażliwość system. Sąd uznał, że „wymóg dodatkowej autoryzacji lub przynajmniej telefonu lub wiadomości tekstowej od banku do płatnika chroniłby posiadaczy rachunków bankowych przed oszustwami na tak dużą skalę". Powód nie dopuścił się rażącego niedbalstwa – nie podał świadomie kodów autoryzujących przelewy nowemu odbiorcy, a bank nie poinformował go wystarczająco jasno, że SMS o treści „Modyfikacja bazy odbiorców" oznacza dodanie zaufanego odbiorcy bez dodatkowej autoryzacji. Wcześniejszy wyrok wydany przez Sąd Okręgowy w Warszawie w sprawie o sygn.akt II C 334/16 z dnia 31 maja 2017 r. dotyczył sprawy klienta, którego komputer padł ofiarą ataku hakerskiego na początku października 2013 r. Mimo zainstalowanego oprogramowania antywirusowego po uzyskaniu dostępu do komputera hakerzy zalogowali się do systemu bankowości internetowej powoda. Następnie wysłali fałszywą wiadomość zalecającą zainstalowanie dodatkowego oprogramowania antywirusowego na telefonie komórkowym. Oprogramowanie to przekazywało wszystkie wiadomości tekstowe z kodami autoryzacyjnymi na numer telefonu hakerów w wyniku czego z rachunku powoda przelano 239 566 PLN w postaci 12 przelewów na rachunki osób trzecich. Ostatecznie zwrócono mu jedynie 40 932,45 PLN (pozostała część została wykorzystana do wypłaty gotówki przez osoby działające w imieniu oszustów) – tzw. „słupy"). Sąd Okręgowy w Warszawie jednoznacznie stwierdził, że za takie zdarzenia odpowiedzialność ponosi bank – powód nie naruszył bowiem swoich obowiązków wynikających z art. 42 ustawy o usługach płatniczych, ponieważ dane zostały uzyskane przez nieznanych sprawców w wyniku oszustwa, poprzez ataki na infrastrukturę informatyczną i fałszywą stronę logowania. Kluczowe ustalenie sądu dotyczyło statusu fałszywej wiadomości: powód widział zieloną kłódkę (oznaczającą połączenie SSL) i adres strony internetowej banku, jednak wiadomość pochodziła od hakera podszywającego się pod bank. W opinii sądu przekonanie, że wiadomość o pobraniu dodatkowego oprogramowania antywirusowego pochodziła od banku i miała na celu zwiększenie bezpieczeństwa, nie stanowiło rażącego niedbalstwa ze strony klienta. Trzecie orzeczenie obrazujące znaczenie cyberodporności oraz ryzyka odpowiedizlności kadry zarzadzającej banku zostało wydane przez Sąd Rejonowy dla Warszawy-Mokotowa, sygnatura akt XVI C 169/16, w dniu 3 lipca 2019 r. i dotyczyło ataku phishingowego w maju 2015 r. W sprawie tej powód padł ofiarą zaawansowanego ataku phishingowego, w wyniku którego pracownicy banku otrzymali fałszywe wiadomości e-mail podszywające się pod kuriera. Z konta powoda pobrano kwotę 44 183,65 PLN. Sąd orzekł, że oszukanie powoda w wyniku tak zaawansowanego ataku nie stanowiło z jego strony „rażącego niedbalstwa" a bank został zobowiązany do zwrotu pieniędzy. Sąd podkreślił, że „sposób działania sprawców był tożsamy z atakami phishingowymi na banki w maju 2015 r. Za rażące niedbalstwo nie

zostało uznane zachowanie bezpośredniej ofiary phishingu, czyli klienta, ale świadome ignorowanie zasad bezpieczeństwa przez bank.
Wdrożenie rozporządzenia DORA jest bezpośrednią odpowiedzią również na niedociągnięcia systemowe w zakresie cyberodporności ujawnione w orzeczeniach polskich sądów. Pierwszy filar DORA wymaga bowiem od zarządów instytucji finansowych wdrożenia solidnego systemu zarządzania ryzykiem ICT. Rozporządzenie to bezpośrednio odnosi się do problemu zidentyfikowanego w cytowanej powyżej sprawie o sygn.akt. II CSKP 1013/22 to jest niemożności wykrycia anomalii (trzy przelewy do nieznanego wcześniej odbiorcy w krótkim odstępie czasu). Drugi filar DORA nakłada obowiązek zgłaszania poważnych incydentów związanych z ICT właściwym organom nadzorczym. Norma ta co prawda nie istniała w momencie ataku w 2013 r. (sprawa II C 334/16) transakcje przeprowadzane na poszczególnych rachunkach nie były systematycznie zgłaszane, a sądy uzyskały informacje o istnieniu ataku dopiero w trakcie postępowania karnego i cywilnego, jednak nie stworzenie strategii zapobiegania takim naruszeniom stanoiwły już delict odpowiedizlanej osoby w banku. Trzeci filar DORA wymaga przeprowadzania testów penetracyjnych opartych na zagrożeniach (TLPT) w celu identyfikacji luk w zabezpieczeniach, zanim zostaną one wykorzystane. Istnienie takiego obowiązku mogłoby przyczynić się do wcześniejszego wykrywania luk w zabezpieczeniach. Przykład to brak obowiązkowej dwuetapowej autoryzacji przelewów do nowych odbiorców, co było sednem problemu w sprawie II CSKP 1013/22.

Wnioski

Raport ENISA „Threat Landscape: Finance Sector” dokumentuje cyberzagrożenia skierowane przeciwko europejskim instytucjom finansowym. Zawiera 488 udokumentowanych cyberincydentów ujawniających wyraźne wzorce zagrożeń, motywacje sprawców i słabe punkty sektora. Europejskie instytucje kredytowe były nieproporcjonalnie często atakowane (46% incydentów) wzgledem innych sektorow gospodarki, co nakazuje pilne i poważne działania naprawcze oraz aktywna obronę. Głównymi konsekwencjami cyberincydentów były zakłócenia w działalności operacyjnej i bezprawne ujawnienia danych. Główne zagrożenia – w tym ataki DDoS, naruszenia bezpieczeństwa danych, inżynieria społeczna, oszustwa, oprogramowanie ransomware, złośliwe oprogramowanie i ataki na łańcuch dostaw odzwierciedlają zarówno kategorie zagrożeń o charakterze trwałym, jak i rosnącą złożoność techniki ataków. Z drugiej strony pokazują ogromne możliwości podmiotów stanowiących realne zagrożenie dla sektora finansowego i *signum temporis,* w którym cyberprzestrzeń staje się najpoważniejszym wyzwaniem i najtrudniejszym terytorium do walki z cyberprzestepczością.

Analiza wyników badań ENISA wykazuje istotne znaczenie dla zagrożeń w polskim sektorze finansowym i jednocześnie pokazuje jego słabości instytucjonalne. Położenie Polski, wspierającej ukraiński opór wobec rosyjskiej inwazji, powoduje zwiększone narażenie na cyberzagrożenia ze strony podmiotów powiązanych z państwem, grupy cyberprzestępcze i haktywistów sterowanych politycznie. Udokumentowana liczba cyberataków na polskie instytucje finansowe znacznie przekracza średnią europejską i światową, co plasuje Polskę wśród najczęściej atakowanych europejskich sektorów finansowych. Polskie instytucje finansowe pilnie muszą wdrożyć kompleksowe

programy odporności cyberbezpieczeństwa, łącząc strategie cyberodporności, analizy prawne, środki kontroli technicznej, procedury organizacyjne, szkolenia pracowników i inne inicjatywy w zakresie zgodności z przepisami. Wdrożenie wymogów DORA i NIS2, poprzez instytucjonalne zarządzanie bezpieczeństwem, zaawansowane wykrywanie zagrożeń, uwierzytelnianie wieloskładnikowe, zarządzanie ryzykiem w łańcuchu dostaw, niewątpliwie wzmocni zdolności reagowania na cyberincydenty oraz umożliwi dostosowanie się do europejskich standardów regulacyjnych. Instytucje finansowe, organy regulacyjne muszą być świadomi pojawiających się nowych trendów i dostosowywać strategie obronne do dynamiki rozwoju zagrożeń.

Także linia orzecznicza polskich sądów zmierza w tym samym kierunku i stymuluje proces zmian. Przytoczone wyroki Sądu Najwyższego (II CSKP 1013/22), Sądu Okręgowego w Warszawie (II C 334/16) oraz Sądu Rejonowego dla Warszawy-Mokotowa (XVI C 169/16) pokazują, że standardy bezpieczeństwa obowiązujące przed wejściem w życie rozporządzenia DORA były niewystarczające. Rozporządzenie DORA i dyrektywa NIS2 stanowią spójną, opartą na faktach i doświadczeniach sektora finansowego odpowiedź regulacyjną na rosnące zagrożenia cybernetyczne. W połączeniu z polskim orzecznictwem historia ataków Carbanak, WannaCry, NotPetya i Bangladesh Bank wskazuje, że bez takich regulacji systemy finansowe pozostają nie tylko podatne na ataki mające globalne konsekwencje dla stabilności finansowej, ale wręcz bezbronne.

Podmioty sektora finansowego w Polsce, w tym instytucje kredytowe, dostawcy usług płatniczych, firmy ubezpieczeniowe, firmy inwestycyjne i operatorzy infrastruktury cyfrowej, muszą uznać cyberodporność za priorytet strategiczny wymagający zaangażowania kierownictwa, ciągłych inwestycji i ciągłego doskonalenia. Wdrożenie strategii ograniczania zagrożeń opracowanych przez ENISA pozwala polskim instytucjom bronić się przed znanymi kategoriami zagrożeń i przewidywać nieznane, jednocześnie zachowując ciągłość usług i zaufanie klientów do cyfrowego ekosystemu finansowego.

Bibliografia

Europejska Agencja Bezpieczeństwa Sieci i Informacji, ENISA, Threat landscape: Finance sector (styczeń 2023 – czerwiec 2024), Heraklion 2024, https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

Europol, Ocena zagrożeń związanych z przestępczością zorganizowaną w Internecie (IOCTA), 2024. Urząd ds. Bezpieczeństwa Sieci i Informacji Unii Europejskiej, Luksemburg. doi:10.2813/442713 https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

Europol, Organy ścigania rozbijają największą na świecie operację ransomware, komunikat prasowy, luty 2024 r., https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

Federalne Biuro Śledcze, FBI identyfikuje cyberprzestępców z grupy Lazarus jako odpowiedzialnych za kradzież 41 milionów dolarów ze strony Stake.com, komunikat prasowy, wrzesień 2023 r., https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-responsible-for-theft-of-41-million-from-stakecom.

IBM, Raport dotyczący kosztów naruszenia bezpieczeństwa danych 2024: Skutki finansowe cyberincydentów, Armonk 2024, https://www.ibm.com/reports/data-breach.

E. Kovacs, Dowody wskazują, że grupa ransomware wiedziała o luce zero-day w MOVEit od 2021 r., SecurityWeek, 2023, https://www.securityweek.com/evidence-suggests-ransomware-group-knew-about-moveit-zero-day-since-2021/.

Lemonnier M., (red.) DORA. Operacyjna odporność cyfrowa sektora finansowego. Komentarz Warszawa 2025, współautorzy: Bejm T., Gryber M., Kisiel S., Lemonnier M., Mariański M., Pałka P., Sowińska-Kobelak D., Turczynowicz-Kieryllo J.

Ministerstwo Cyfryzacji, Krajobraz cyberprzestrzeni: roczne sprawozdanie o cyberbezpieczeństwie za 2024 rok. Warszawa, 2025, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie

Nasarrouh S., Polski sektor finansowy pod ostrzałem: 1850 cyberataków tygodniowo wymierzonych w banki i fintechy, „Poland Insight" 2025, https://polandinsight.com/polish-financial-sector-under-siege-1850-cyberattacks-per-week-target-banks-and-fintechs-40804/.

Nowikowska M., Mechanizmy współpracy w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS, [w] Rola cyberbezpieczeństwa w sferze publicznej: wymiar europejski, red. K. Chałubińska-Jentkiewicz (IP), Istvan Hoffman – Maribor, Słowenia: Instytut Samorządu Lokalnego Maribor, 2022

Komisja Nadzoru Finansowego, Raport roczny CSIRT KNF 2024, Warszawa 2025, https://www.knf.gov.pl/en/?articleId=93273&p_id=19.

Komisja Nadzoru Finansowego, Pismo sektorowe w sprawie wymogów zgodności z ustawą o odporności operacyjnej w obszarze cyfrowym (DORA), Warszawa 2024, https://www.knf.gov.pl/en/MARKET/CSIRT_KNF.

Polska Agencja Inwestycji i Handlu (PAIH), Fintech. Cyber. Biometria. Twoje zaufane trio z Polski, Warszawa, 2025.

Polska Agencja Prasowa, Wyciek danych klientów w wyniku ataku hakerskiego na polskiego pożyczkodawcę internetowego, 02.11.2025 https://www.pap.pl/en/news/client-data-leaked-hack-polish-online-lender.

J.Turczynowicz- Kieryłło, Art. 50-55, (w) M.Lemonnier, DORA. Operacyjna odporność cyfrowa sektora finansowego, Warszawa 2025.