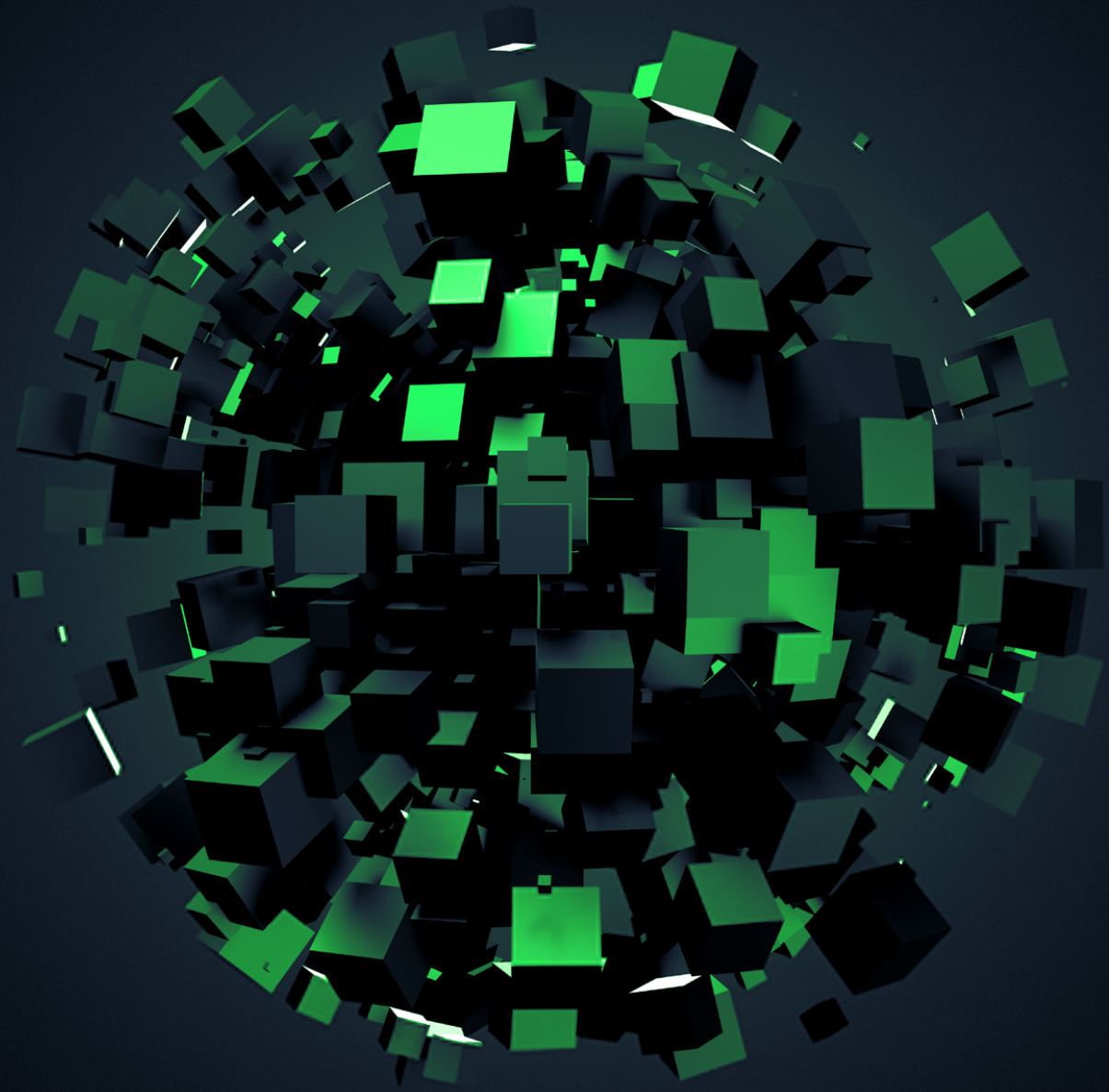
RAPORT ROCZNY 2025

z działalności CERT Polska

Krajobraz bezpieczeństwa
polskiego internetu



30 LAT | CERT.PL NASK

RAPORT ROCZNY 2025

z działalności CERT Polska

Krajobraz bezpieczeństwa polskiego internetu

CERT.PL NASK | NASK | Ministerstwo Cyfryzacji

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TYTUŁ: Raport roczny 2025 z działalności CERT Polska.
Krajobraz bezpieczeństwa polskiego internetu

AUTOR: zespół CERT Polska

Warszawa 2026

ISBN: 978-83-68356-51-9

Państwowy Instytut Badawczy NASK
ul. Kolska 12
01–045 Warszawa

Spis treści

Wstęp

Za nami kolejny rok działania zespołu CERT Polska. Był on wyjątkowy, ponieważ wieńczył trzecią dekadę naszej działalności – świętujemy właśnie 30. urodziny! Rok 2025 to czas pełen wyzwań, rozwoju i kształtowania cyberbezpieczeństwa w kompleksowy sposób – od proaktywnych działań na rzecz wykrywania zagrożeń, poprzez obsługę zgłoszeń i reagowanie na incydenty aż po dzielenie się wiedzą i budowanie świadomości społecznej.

Znajdziecie tu historie o popularnych kampaniach oszustw, relacje z obserwacji grup APT czy informacje z pierwszej ręki o przełomach w wykrywaniu zagrożeń. Opowiemy o testach bezpieczeństwa, upublicznianiu podatności, złośliwym oprogramowaniu i atakach ransomware.

Będzie też tradycyjnie o współpracy krajowej i międzynarodowej, ćwiczeniach i zawodach, projektach, w których biorą udział zespoły z całego świata, o polskiej prezydencji w Radzie Unii Europejskiej, o nowych inicjatywach łączących bezpieczników z różnych instytucji i sektorów gospodarki.

Nie zabraknie zagadnień dla fanów solidnych technicznych rozwiązań. Na kartach raportu poruszymy tematy usług i oprogramowania, które współtworzymy lub budujemy sami – AIPITCH, DNS4EU, FETTA, PERUN, Artemis, Lista Ostrzeżeń, MWDB, n6 i nasze flagowe przedsięwzięcie – moje.cert.pl.

Powyższe wyliczenie pokazuje, jak bardzo złożone i zróżnicowane są zadania, z którymi na co dzień mierzy się nasz zespół. Jednak u podstaw każdego z tych działań leży potrzeba uszczelniania i usprawniania systemu, który czyni polską cyberprzestrzeń bezpieczniejszą. Drugim filarem jest wiedza – świadomość zagrożeń i znajomość metod zapobiegania im to najskuteczniejsza broń w walce z cyberoszustami.

CERT Polska to ludzie i chcemy, żeby nasz raport też był ludzki. Merytoryczny, pełen rzetelnej wiedzy, liczb i wykresów, a jednocześnie ciekawy i angażujący. Przeczytacie dziś o wielu ważnych i trudnych tematach, ale są to sprawy, z których możemy być po prostu dumni – my jako CERT, ale też my jako Polacy.

Miłej lektury!

O CERT Polska

Dbamy o bezpieczeństwo polskiego internetu. To hasło, które bardzo dobrze oddaje sens i cel naszej pracy.

CERT Polska to historycznie pierwszy w Polsce zespół reagowania na incydenty. Dzięki skutecznej działalności od 1996 roku staliśmy się wiarygodnym i rozpoznawalnym partnerem w środowisku eksperckim oraz w sektorze publicznym. Dziś rzetelną obsługą zgłoszeń oraz działalnością edukacyjną podobną pozycję budujemy wśród obywateli.

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego i realizuje część zadań zespołu CSIRT NASK zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa. Jesteśmy zespołem odpowiedzialnym za obsługę incydentów bezpieczeństwa i współpracę z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej.

Od wejścia w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC) zespół realizuje wiele zadań CSIRT NASK, zgodnie z art. 26 tej ustawy.

Jako CSIRT NASK, zgodnie z art. 26 przywołanej ustawy, odpowiadamy m.in. za:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym,
- reagowanie na zgłoszone incydenty,
- koordynację obsługi incydentów,
- prowadzenie zaawansowanych analiz złośliwego oprogramowania oraz analiz podatności,
- rozwijanie narzędzi i metod do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,
- prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa.

Zajmujemy się także koordynacją incydentów zgłaszanych przez:

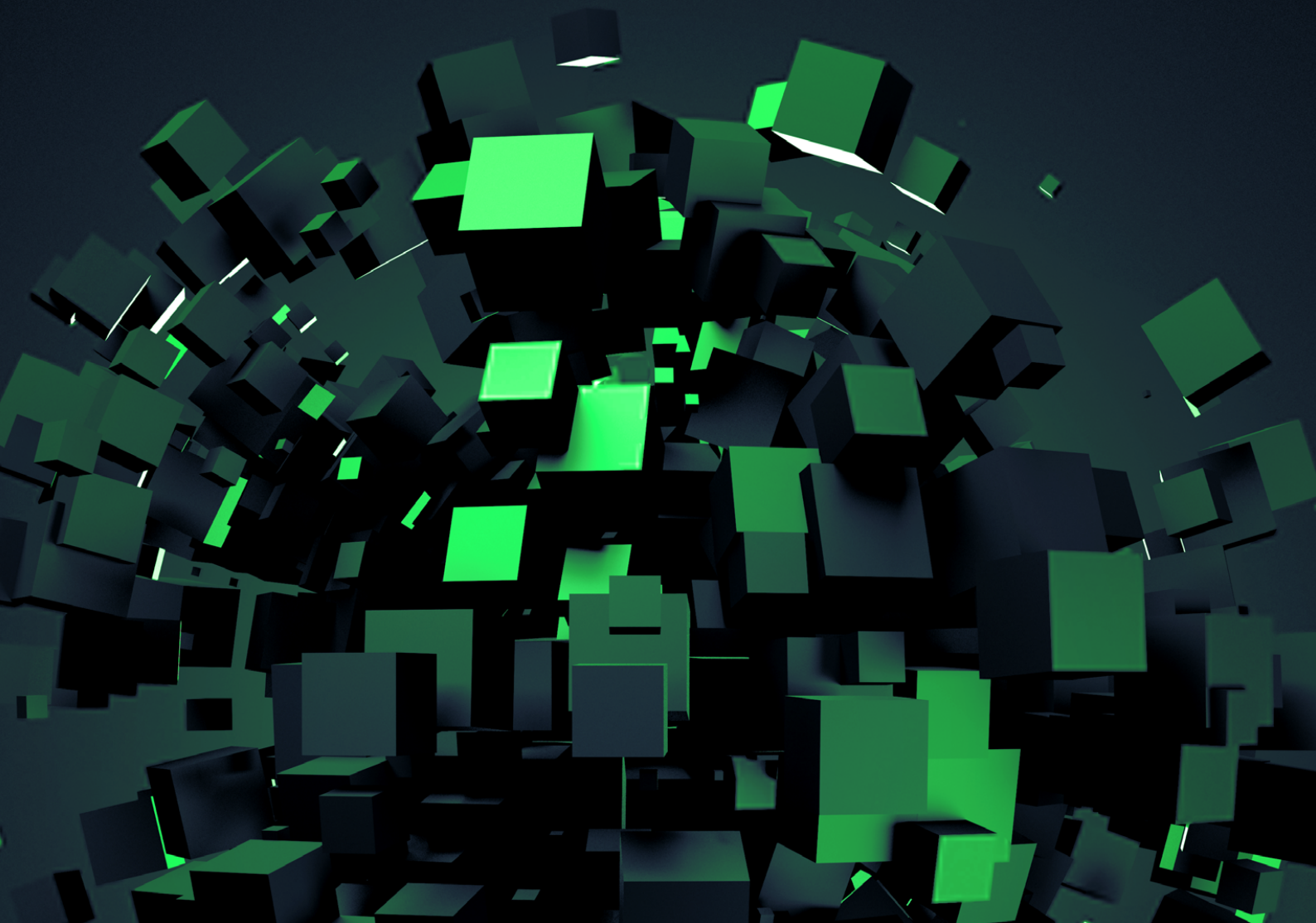
- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,

- jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2 ustawy o KSC,
- instytuty badawcze,
- Urząd Dozoru Technicznego,
- Polskie Centrum Akredytacji,
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,
- dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 5 ustawy o KSC,
- operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7 ustawy o KSC,
- inne podmioty niż wymienione powyżej oraz ust. 5 i 7 ustawy o KSC,
- osoby fizyczne.

Ważnym aspektem naszej pracy jest też budowanie świadomości w obszarze cyberbezpieczeństwa oraz proaktywne poszukiwanie rozwiązań na wyzwania, które stoją przed instytucjami, o których mowa wyżej. Do każdego zgłoszenia podchodzimy indywidualnie. Oferujemy wsparcie i pomoc merytoryczną. Obserwujemy trendy w cyberprzestrzeni i prowadzimy statystyki. Skutecznie ostrzegamy i informujemy. Więcej o naszej codziennej pracy przeczytacie w raporcie.

Zapraszamy do lektury!

Kalendarium



STYCZEŃ

01.01–**30**.06 Okres polskiej prezydencji w Radzie Unii Europejskiej

https://www.gov.pl/web/cyfryzacja/polska-prezydencja-w-radzie-ue-bezpieczna-i-cyfrowa-europa-dzieki-dzialaniom-ministerstwa-cyfryzacji2

02.01 Zapowiedź wycofania pierwszej wersji Listy Ostrzeżeń

https://cert.pl/posts/2025/01/wycofanie-pierwszej-wersji-listy/

09.01 Artemis wykrył ponad 500 tys. błędów i podatności

https://x.com/CERT_Polska/status/1877314450845262010

13.01 Informowaliśmy o wycieku danych ze strony sklepbaterie.pl

https://x.com/CERT_Polska/status/1878786709510390037

17.01 Ostrzegaliśmy przed kampanią phishingową wymierzoną w użytkowników poczty Onet

https://x.com/CERT_Polska/status/1880315748419268641

LUTY

05.02 Ostrzegaliśmy przed stronami podszywającymi się pod gov.pl, na których rzekomo można było uzyskać informację o wsparciu finansowym

https://x.com/CERT_Polska/status/1887121450823188910

11.02 Informowaliśmy o kampanii, w której oszuści wysyłali wiadomości z informacją o rzekomo przysługującym zwrocie nadpłaconego podatku

https://x.com/CERT_Polska/status/1889269064234914191

12.02 Premiera serwisu moje.cert.pl

https://cert.pl/posts/2025/02/moje.cert.pl/

MARZEC

07.03 Dane z Genesis Market zostały udostępnione w moje.cert.pl

https://x.com/CERT_Polska/status/1898002700203147307

18.03 Skanowania zrealizowane w ramach moje.cert.pl pozwoliły nam wykryć ponad 100 tys. podatności i błędnych konfiguracji

https://x.com/CERT_Polska/status/1901918495685988657

24.03 Ostrzegaliśmy przed kampanią phishingową, w której oszuści podszywali się pod system e-TOLL

https://x.com/CERT_Polska/status/1904131427324555692

25.03 Opublikowaliśmy artykuł „Krytyczne podatności w kontrolerze Ingress-Nginx w Kubernetes”

https://cert.pl/posts/2025/03/krytyczne-podatnosci-w-kontrolerze-ingress-nginx-kubernetes/

28.03 Serwis moje.cert.pl ma ponad 10 tys. użytkowników

https://x.com/NASK_pl/status/1905514627188097523

28.03 Ostrzegaliśmy przed kampanią wykorzystującą wizerunek Urzędu Patentowego

https://x.com/CERT_Polska/status/1905612569374503160

31.03 Opublikowaliśmy artykuł „Meta niedostatecznie realizuje postulaty CERT Polska”

https://cert.pl/posts/2025/03/ewaluacja-oczekiwan-wobec-meta/

KWIECIEŃ

03–04.04 SECURE International Summit 2025 w Bydgoszczy

https://polish-presidency.consilium.europa.eu/en/news/europe-unites-in-the-face-of-cyber-attacks-end-of-the-secure-international-summit-2025/

03.04 Premiera „Raportu rocznego 2024 z działalności CERT Polska”

https://cert.pl/posts/2025/04/raport-roczny-2024/

18.04 Szkolenie CERT Polska dla pracowników Wodociągów Warszawskich

https://x.com/CERT_Polska/status/1913176503711379599

18.04 Nowe źródła wycieków dodane do moje.cert.pl

https://x.com/CERT_Polska/status/1913212995783532622

23.04 Ostrzegaliśmy przed kampanią, w której oszuści podszywali się pod usługę BLIK

https://x.com/CERT_Polska/status/1914993630323855666

24.04 Opublikowaliśmy artykuł o technikach deobfuskacji w Lumma Stealer

https://cert.pl/en/posts/2025/04/peephole-deobfuscation/

30.04 Zasilenie portalu bezpiecznedane.gov.pl kolejnymi zbiorami danych

https://x.com/CERT_Polska/status/1917602656853299642

MAJ

09.05 W ćwiczeniach NATO Locked Shields 2025 zespół polsko-francuski zajmuje 2. miejsce

https://x.com/CERT_Polska/status/1920832659820892167

12–16.05 CyberWeek w Krakowie – tydzień eksperckich spotkań i prac nad przyszłością cyberbezpieczeństwa w Europie

https://x.com/CYFRA_GOV_PL/status/1923389157931397380

19.05 Ostrzegaliśmy przed kampanią, w której oszuści podszywali się pod Tauron Polska Energia

https://x.com/CERT_Polska/status/1924464876774105293

22.05 Uruchomienie komunikatów o zagrożeniach w moje.cert.pl

https://cert.pl/posts/2025/05/moje.cert.pl-powiadomienia/

CZERWIEC

01.06 Wycofanie pierwszej wersji Listy Ostrzeżeń

https://cert.pl/posts/2025/01/wycofanie-pierwszej-wersji-listy/

04.06 Przestrzegaliśmy przed kampanią, w której oszuści podszywali się pod InPost i rozsyłali szkodliwe oprogramowanie

https://x.com/CERT_Polska/status/1930233080767291609

05.06 Opublikowaliśmy artykuł „Kampania UNC1151 wykorzystująca podatność w oprogramowaniu Roundcube do kradzieży poświadczeń”

https://cert.pl/posts/2025/06/unc1151-kampania-roundcube/

06.06 EU Cyber Blueprint przyjęty podczas formalnego posiedzenia Rady ds. Transportu, Telekomunikacji i Energii

https://x.com/CERT_Polska/status/1930988050647286042

11.06 Ostrzegaliśmy przed kampanią, w której oszuści podszywali się pod Urząd Statystyczny w Warszawie

https://x.com/CERT_Polska/status/1932757483920990329

16.06 Przestrzegaliśmy przed kolejną odsłoną fałszywych reklam informujących o możliwości wygrania biletu okresowego na komunikację miejską

https://x.com/CERT_Polska/status/1934612683996696683

23.06 Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca aktualizacji oprogramowania Roundcube

https://x.com/CERT_Polska/status/1937193939146068304

LIPIEC

04–06.07 Krajowe kwalifikacje do European Cybersecurity Challenge 2025

https://x.com/CERT_Polska/status/1941134908388233589

09.07 Na Liście Ostrzeżeń w 2025 roku umieściliśmy 100 tys. domen

https://x.com/CERT_Polska/status/1942961943574384785

17.07 Informowaliśmy o kampanii fałszywych SMS-ów o rzekomym przejęciu danych z komputerów użytkowników

https://x.com/CERT_Polska/status/1945785553296732293

21.07 Ogłoszenie listy reprezentantów Polski na European Cybersecurity Challenge 2025

https://x.com/CERT_Polska/status/1947250200629698847

24.07 Informowaliśmy o publikacji dekryptora grupy ransomware Phobos/8Base

https://moje.cert.pl/komunikaty/2025/19/publikacja-dekryptora-phobos/

SIERPIEŃ

01.08 Informowaliśmy o kampanii mailowej o rzekomych nagraniach kompromitujących adresata

https://x.com/CERT_Polska/status/1951236500508516363

06.08 Udostępniliśmy narzędzie DRAKVUF Sandbox v0.19.0

https://x.com/CERT_Polska/status/1953106389481509309

07.08 Opublikowaliśmy „Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT”

https://cert.pl/posts/2025/08/rekomendacje-csirt/

12.08 Po pół roku działania moje.cert.pl ma ponad 12,5 tys. użytkowników

https://x.com/NASK_pl/status/1955167359955529868

20.08 Przestrzegaliśmy przed kampanią SMS-ową o rzekomym „rządowym kuponie energetycznym”

https://x.com/CERT_Polska/status/1958159593718026362

WRZESIEŃ

03.09 Ostrzegaliśmy przed nowym wariantem wyłudzenia na „zwrot środków”, w którym oszuści podszywali się pod NFZ

https://x.com/CERT_Polska/status/1963225473900519803

05.09 Opublikowaliśmy poradnik „Bezpieczeństwo twojej kieszeni, czyli jak ochronić swój telefon”

https://cert.pl/bezpieczny-telefon/

16.09 Poprzez skanowania w ramach moje.cert.pl wykryliśmy milion podatności oraz błędnych konfiguracji

https://x.com/CERT_Polska/status/1967978056104206662

17.09 Opublikowaliśmy artykuł „Jak rozpoznać fałszywe strony internetowe i uniknąć phishingu”

https://cert.pl/posts/2025/09/analiza-adresow-stron/

19.09 Ostrzegaliśmy przed ofertami zdalnej pracy z podejrzanie wysokimi zarobkami

https://x.com/CERT_Polska/status/1968948175756214636

22.09 Informowaliśmy, że do serwisu bezpiecznedane.gov.pl dodano 1,8 mln rekordów zawierających dane logowania

https://x.com/CERT_Polska/status/1970090473533456432

PAŹDZIERNIK

06–09.10 Zawody finałowe European Cybersecurity Challenge 2025 w Warszawie

https://www.nask.pl/aktualnosci/cyberbitwa-rozstrzygnieta-wlosi-gora-polska-w-pierwszej-dziesiatce

15.10 Opublikowaliśmy pierwszy numer raportu miesięcznego o stanie cyberbezpieczeństwa w Polsce

https://cert.pl/posts/2025/10/raport-miesieczny-09/

24.10 Kampania fałszywych SMS-ów, w których oszuści podszywają się pod e-Urząd Skarbowy

https://x.com/CERT_Polska/status/1981707250596237406

LISTOPAD

03.11 Opublikowaliśmy artykuł „Analiza kampanii złośliwego oprogramowania NGate (NFC relay)"

https://cert.pl/posts/2025/11/analiza-ngate/

04.11 Ostrzegaliśmy przed kampanią fałszywych wiadomości wymierzoną w klientów banku PKO BP

https://x.com/CERT_Polska/status/1985738816670588973

14.11 Informowaliśmy o aktywnie wykorzystywanej podatności CVE-2025-64446 w oprogramowaniu FortiWeb

https://moje.cert.pl/komunikaty/2025/57/aktywnie-wykorzystywana-krytyczna-podatnosc-w-urzadzeniach-fortinet-fortiweb-manager/

GRUDZIEŃ

02.12 4 wystąpienia ekspertów z CERT Polska na konferencji Oh My Hack 2025

https://x.com/CERT_Polska/status/1995504567157481857

04.12 Informowaliśmy o krytycznej podatności CVE-2025-55182 React2Shell

https://moje.cert.pl/komunikaty/2025/61/krytyczna-podatnosc-w-react-server-components-oraz-innych-aplikacjach-z-tym-rozwiazaniem/

09.12 Informowaliśmy o kampanii phishingowej, w której oszuści podszywali się pod Spotify

https://x.com/CERT_Polska/status/1998361990641648061

13.12 Opublikowaliśmy artykuł „Publiczne sieci Wi-Fi – czy jest się czego bać?”

https://cert.pl/posts/2025/12/publiczne-sieci-wifi/

13.12–**24**.12 Publikowaliśmy posty w ramach świątecznej serii #CyberPrezent

https://x.com/CERT_Polska/status/2003858209610850480

19.12 Informowaliśmy, że w serwisie moje.cert.pl zarejestrowało się 15 tys. użytkowników

https://x.com/CERT_Polska/status/2002000973766484051

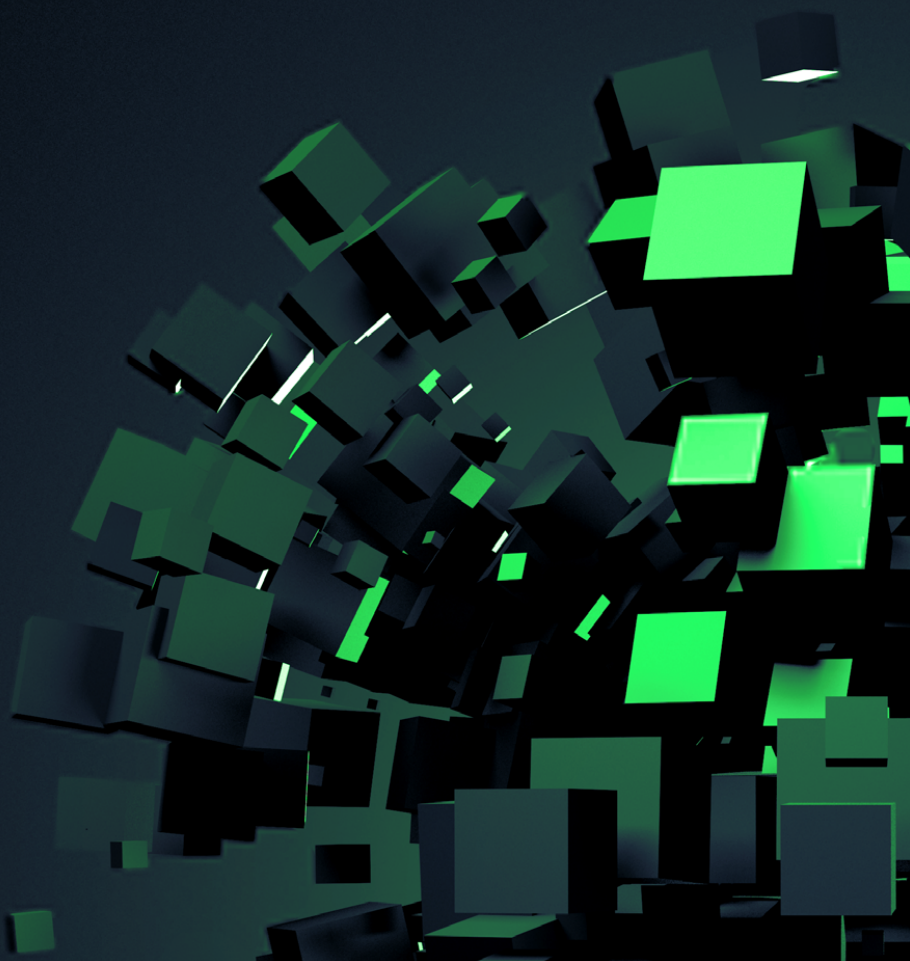
29.12 Skoordynowane ataki wymierzone w wiele podmiotów sektora energii

https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/

31.12 Opublikowaliśmy post, w którym poinformowaliśmy, że liczba szkodliwych domen dodanych przez nas na Listę Ostrzeżeń od początku jej istnienia przekroczyła 500 tys.

https://x.com/CERT_Polska/status/2006379829466177890

30 lat CERT Polska – perspektywa kierowników zespołu



Marcin Dudek

KIEROWNIK CERT POLSKA OD 2025 ROKU

W tym roku obchodzimy 30-lecie istnienia CERT Polska. Jest to ogromna praca wielu osób na przestrzeni tych lat. Zespół rósł, otoczenie i wyzwania się zmieniały, ale są elementy, które niezależnie od czasu zawsze stanowiły fundament. To, co dla mnie było niesamowite, gdy 6 lat temu dołączyłem do CERT Polska, to poziom zaangażowania ludzi tu pracujących i ich poczucie misji.

Gdy analizujemy incydent, to nie tak, żeby zgadzała się statystyka, ale tak, żeby faktycznie wyjaśnić, co się wydarzyło. Gdy wykrywamy stronę wyłudzającą dane według nowego schematu, to nie wystarczy jej zablokowanie, bo ciekawość zaprowadzi do wykrycia kolejnych stu i opracowania reguł do łapania nowych. Mnóstwo inicjatyw i pomysłów na rozwój powstaje oddolnie. Przykładowo portal moje.cert.pl nie był przez nikogo narzucony – grupa osób pewnego dnia uznała, że brakuje takiego miejsca, i w kilka miesięcy je stworzyła.

Jest to także zasługa kolejnych pokoleń kierowników, gdzie każdy był z wewnątrz organizacji, dzięki czemu rozumiał specyfikę tego zespołu i wiedział, że czasem wystarczy lekko akcentować kierunki, a niekoniecznie je narzucać. Krzysiek, Mirek, Piotrek, Przemek, Sebastian – dziękuję. Wkład każdego z Was był nieoceniony dla tego, czym obecnie jest CERT Polska.

Jestem ciekawy Waszej perspektywy z biegiem lat: jak „cyber” wyglądało w Waszych czasach? Jakie były wtedy wyzwania? Jakie decyzje były kluczowe? I najważniejsze – na co powinniśmy dalej się szykować?

Krzysztof Silicki

KIEROWNIK CERT POLSKA W LATACH 1996–2001

Jak wyglądał krajobraz cyberbezpieczeństwa w Polsce, kiedy obejmowałeś stanowisko kierownika CERT Polska? Jakiego rodzaju zagrożenia dominowały?

Początek historii CERT-u to rok 1996. To zaledwie kilka lat po tym, jak NASK dołączył Polskę do światowego internetu. Następował dynamiczny wzrost liczby hostów podłączonych do sieci i już wtedy można było zaobserwować wiele zagrożeń oraz incydentów. Mieliśmy na przykład do czynienia ze zjawiskiem masowych skanowań czy próbkowań w krajowej przestrzeni adresowej IP, w poszukiwaniu podatności w konfiguracji komputerów podłączonych do internetu – a znalezienie luk w systemach czy słabych haseł nie było trudne, bo niewiele podłączonych podmiotów miało świadomość, że należy stosować zapory sieciowe, a użytkownicy stosowali słabe hasła. Popularnym incydentem były na przykład tzw. website defacements, gdzie rozmaici hakerzy włamywali się do systemów komputerowych swych ofiar i podmieniali ich strony internetowe na swoje własne. Podmiot tracił wizerunkowo, a włamywacz zyskiwał uznanie w środowisku podobnych sobie osób. Znane też już były metody instalowania „koni trojańskich", podmieniania plików systemowych i penetrowanie kolejnych komputerów w zaatakowanej sieci lokalnej. Już wtedy problemem był też masowy spam. Co ciekawe, miały też miejsce pierwsze próby oszustw związanych z kartami płatniczymi, a instrukcje, jak to zrobić, były publikowane w internecie. Swoją drogą, od 1996 roku publikujemy roczne raporty CERT Polska, gdzie można prześledzić te kwestie.

Jakie były największe wyzwania w okresie kierowania zespołem?

Po pierwsze – dotarcie z informacją do użytkowników, że CERT istnieje i po co jest oraz że warto mieć świadomość, iż internet to nie tylko fajne medium globalnej komunikacji, ale są też zagrożenia, czyli warto zadbać o swoje bezpieczeństwo. Dostawaliśmy wiele informacji od CERT-ów za granicą o próbach ataków na hosty w .pl i odzywaliśmy się do każdego, kto mógł być potencjalną ofiarą ataku. Już na początku naszej działalności były zdarzenia, kiedy kilkanaście tysięcy komputerów w Polsce było skanowanych i atakowanych przez automatyczne skrypty. Wtedy wiele podmiotów i użytkowników dowiadywało się, że istniejemy i oferujemy wiedzę i pomoc. Po drugie – chyba, w owym czasie, brak narzędzi, które sami musieliśmy tworzyć, adaptować i rozwijać, żeby chociażby zautomatyzować swoje działanie, bo skala zdarzeń rosła, a CERT liczył kilka, potem kilkanaście osób.

Po trzecie – brak świadomości u instytucjonalnych czy indywidualnych użytkowników, że bezpieczeństwo internetu to nie jest żaden temat niszowy i że każdy ma tu swój kawałek odpowiedzialności za bezpieczeństwo.

Z perspektywy czasu które decyzje, zmiany lub osiągnięcia były Twoim zdaniem kluczowe?

Oczywiście po pierwsze decyzja ówczesnego kierownictwa o powołaniu CERT-u w NASK. Ówczesna dyrekcja przychylnie potraktowała oddolną inicjatywę, aby zająć się kwestią bezpieczeństwa – to było kluczowe. Po drugie, postawienie na współpracę. Bardzo szybko staliśmy się członkiem organizacji FIRST zrzeszającej CERT-y na całym świecie. Działaliśmy w kraju, żeby promować ideę CERT-ową i wspierać powstawanie zespołów bezpieczeństwa np. u dużych operatorów (Telbank, TP SA) i współpracować z nimi. Powołaliśmy też sieć współpracy zespołów bezpieczeństwa – Abuse Forum, którą jeszcze kilka osób w środowisku pewnie pamięta... Po trzecie, prawie natychmiast powołaliśmy do życia konferencję SECURE. To jest pierwsza w kraju konferencja dotycząca bezpieczeństwa teleinformatycznego, która istnieje do dziś i jest dla nas i naszego constituency okazją do corocznego podsumowania, gdzie jesteśmy z cyberbezpieczeństwem, jakie są aktualne zagrożenia, ataki i wyzwania oraz jak się przed tym bronić.

Jednak za największe osiągnięcie uważam konsekwentne budowanie i hołdowanie określonemu systemowi wartości, który powodował, iż poczucie misji, poczucie realnego wpływu na rzeczywistość, odpowiedzialność, wysokie standardy etyczne i chęć dzielenia się wiedzą oraz efektami działań przyciągały kolejne, bardzo kompetentne osoby mające świetne pomysły na dalszy rozwój CERT-u.

Jakie Twoim zdaniem będą największe wyzwania w cyberbezpieczeństwie w ciągu najbliższych 5 lat? W szczególności w kontekście roli, jaką może odegrać CERT Polska.

CERT Polska przeszedł kilka faz rozwoju na swej drodze. Od podjęcia się „samozwańczo" misji działania na rzecz bezpieczeństwa internetu, poprzez budowanie topowych kompetencji, prowadzenie innowacyjnych projektów badawczych krajowych i międzynarodowych, współpracę z innymi, którzy potrzebowali pomocy lub działali na rzecz cyberbezpieczeństwa kraju aż po przyjęcie ustawowej roli jednego z trzech CSIRT-ów poziomu krajowego. Jestem przekonany, że CERT Polska czekają kolejne etapy rozwoju ze względu na takie czynniki, jak: rozwój sztucznej inteligencji i innych technologii o charakterze przełomowym, ewolucja krajowego systemu cyberbezpieczeństwa w obliczu nowych wyzwań oraz ustaw i prawa unijnego, zagrożenia o charakterze geopolitycznym, hybrydowym czy militarnym, czy też po prostu rosnąca dynamika oraz skala zagrożeń. Myślę, że w najbliższych latach kluczowe będzie wsparcie CERT Polska w rozwoju KSC poprzez tworzenie i pomoc w tworzeniu CERT-ów/CSIRT-ów sektorowych. Krajowy system reagowania musi zostać odpowiednio wyskalowany poprzez rozbudowywanie hierarchii kolejnych zespołów reagujących, które będą ze sobą operacyjnie współpracowały.

Oczywiście, dużym wyzwaniem jest jednoczesne pełnienie przez CERT Polska roli analitycznej, operacyjnej i badawczej na najwyższym poziomie, ale takie działanie stanowi właśnie paliwo dla zespołu tej klasy, więc życzę naszemu CERT-owi kolejnych sukcesów.

Mirosław Maj

KIEROWNIK CERT POLSKA W LATACH 2001–2010

Jak wyglądał krajobraz cyberbezpieczeństwa w Polsce, kiedy obejmowałeś stanowisko kierownika CERT Polska? Jakiego rodzaju zagrożenia dominowały?

Gdy obejmowałem stanowisko kierownika CERT Polska w maju 2001 roku, krajobraz cyberbezpieczeństwa w Polsce wyglądał zupełnie inaczej niż dziś. Zagrożenia już stawały się coraz bardziej powszechne, ale jednocześnie poziom e-usług był na kompletnie innym etapie – skala cyfryzacji i zależności od usług online była nieporównywalnie mniejsza.

Jeśli chodzi o dominujące zagrożenia, to nie było jeszcze zagrożeń klasy APT w dzisiejszym rozumieniu. Za to codzienną udręką pozostawały masowe skanowania – szerokie, „hurtowe" próby wykrywania podatnych usług i systemów.

Równocześnie od dawna byliśmy przekonani, że możliwe są masowe zagrożenia obejmujące całą sieć, a nie tylko pojedyncze komputery czy instytucje. I właśnie rok 2001 dostarczył na to najlepszych dowodów: robaki takie jak Nimda czy Code Red pokazały, jak szybko i szeroko mogą rozprzestrzeniać się incydenty o skali „internetowej".

Jakie były największe wyzwania w okresie kierowania zespołem?

Największe wyzwania w okresie, gdy kierowałem zespołem, wynikały przede wszystkim z bardzo szybkiego wzrostu liczby incydentów przy jednocześnie bardzo małym składzie. Skala pracy rosła szybciej niż nasze możliwości operacyjne.

Dodatkowo postawiliśmy sobie ambitny cel: poczucie odpowiedzialności za całą domenę .pl, stąd zresztą zmiana nazwy zespołu z CERT NASK na CERT Polska. To dawało ogromną satysfakcję, ale oznaczało też masę pracy – zarówno w Polsce, jak i za granicą. W tym czasie zaczęliśmy też aktywnie działać w strukturach międzynarodowych, co otwierało nowe możliwości, ale dokładało kolejne obowiązki.

Dużym wyzwaniem było również budowanie sieci kontaktów: rozwijanie polskiej społeczności zespołów reagowania Abuse Forum i tworzenie realnej współpracy między podmiotami, które wcześniej często działały w izolacji albo ich nie było w ogóle, a przekonywaliśmy, że powinny powstać.

A jeśli miałbym wskazać najtrudniejsze zadanie, to chyba przekonywanie decydentów w kraju, że rola cyberbezpieczeństwa szybko rośnie i że potrzebne są konkretne działania.

Z perspektywy czasu które decyzje, zmiany lub osiągnięcia były Twoim zdaniem kluczowe?

Myślę, że wspomniana zmiana nazwy zespołu – choć wydaje się symboliczna, to była ważna. To był jasny sygnał – deklarujemy wsparcie, w kraju i za granicą, że będziemy pomagali przy obsłudze każdego incydentu związanego z „constituency" .pl. Nie mniej kluczowe było zaangażowanie się w projekty międzynarodowe. Budowaliśmy konsorcja, uczestniczyliśmy w projektach dla niektórych społeczności, np. rodzących się struktur CSIRT-ów w Europie Wschodniej, staliśmy się pomostem do współpracy międzynarodowej.

Jakie Twoim zdaniem będą największe wyzwania w cyberbezpieczeństwie w ciągu najbliższych 5 lat? W szczególności w kontekście roli, jaką może odegrać CERT Polska.

W perspektywie najbliższych 5 lat największe wyzwania w cyberbezpieczeństwie będą – moim zdaniem – bezpośrednio związane z rolą CSIRT-u poziomu krajowego. Zbiorcze constituency CSIRT NASK staje się olbrzymie, szczególnie w kontekście wdrażania NIS 2, która istotnie poszerza krąg podmiotów objętych wymaganiami.

CERT Polska ma już dziś ogromne doświadczenie w obsłudze bardzo wymagających, zaawansowanych przypadków. Kluczowym zadaniem na kolejne lata będzie jednak wypracowanie mechanizmów skalowania: wiedzy, działań operacyjnych, narzędzi, komunikacji i modeli współpracy tak, aby realnie przenosić skuteczne podejście na poszczególne sektory. Problem jest prosty – nie wystarczy specjalistów, więc nie da się tego rozwiązać wyłącznie zwiększaniem zespołu. Kluczowe będzie też wypracowanie modeli współpracy z CSIRT-ami sektorowymi, szczególnie że spodziewam się, że będą one działały w bardzo różny sposób.

Potrzebne będą więc skuteczne, powtarzalne mechanizmy zarówno dla prewencji, jak i dla reakcji – takie, które pozwolą podmiotom szybciej osiągać wymagany poziom odporności i sprawniej obsługiwać incydenty, bez pełnego uzależnienia od zasobów CSIRT-u krajowego.

Posługując się przykładem: nadchodzi moment, w którym nie wystarczy „tylko" zaoferować usługę taką jak moje.cert.pl (swoją drogą – to bardzo dobre rozwiązanie). Konieczne będzie również nauczenie, jak z tej usługi skutecznie korzystać – a być może nawet wyegzekwowanie określonych działań po stronie podmiotów objętych regulacjami, tak aby wsparcie przekładało się na realną poprawę bezpieczeństwa, a nie kończyło się na samej dostępności narzędzia.

Piotr Kijewski

KIEROWNIK CERT POLSKA W LATACH 2010–2016

Jak wyglądał krajobraz cyberbezpieczeństwa w Polsce, kiedy obejmowałeś stanowisko kierownika CERT Polska? Jakiego rodzaju zagrożenia dominowały?

Dominowały botnety złożone z zainfekowanych komputerów osobistych z systemem Windows, których skala (światowa) zazwyczaj była liczona w setkach tysięcy, a nawet milionach maszyn. Oczywiście nie brakowało w tym systemów z Polski.

Prym wiodły trojany bankowe, które przechodziły przez bardzo szybki rozwój zarówno pod kątem metod wyłudzania pieniędzy czy sposobów uzyskiwania dostępu do kont bankowych (w tym przez infekcje urządzeń mobilnych), jak i pod względem botnetów (mechanizmy P2P lub DGA do zarządzania), które te ataki umożliwiały. Po raz pierwszy w sposób zorganizowany zaczęliśmy temu procesowi przeciwdziałać – zarówno poprzez rozwój metod wykrywania/blokowania tzw. webinjectów (złośliwy kod wstrzykiwany przez malware, podszywający się pod stronę bankową), jak i poprzez aktywne rozbijanie botnetów w ramach współpracy międzynarodowej.

W owym czasie sporo infrastruktury do zarządzania botnetami (w tym słynnym w owym czasie Virutem, jednym z największych ówczesnych botnetów na świecie) znajdowało się w domenie .pl i stawało się to coraz poważniejszym problemem.

Spam i ataki DDoS były również większym wyzwaniem niż obecnie, również napędzanym przez duże botnety. Pojawiały się też pierwsze obserwacje ataków APT, przypisywane państwom, co było nowością. Ataki te były oczywiście bardziej ukierunkowane, w przeciwieństwie do masowych ataków napędzanych botnetami, i ich obserwacje w owym czasie stanowiły większe wyzwanie niż obecnie.

Ransomware był w powijakach i zazwyczaj polegał na wyświetlaniu komunikatów o zaszyfrowaniu (lub wycieku danych) i na zastraszaniu niż na prawdziwym szyfrowaniu systemów ofiar.

Za sprawą ataków trojanów bankowych i wczesnego ransomware po raz pierwszy przeciętni użytkownicy w Polsce zaczynali odczuwać skutki ataków na własnym portfelu – co również było nowością.

Jakie były największe wyzwania w okresie kierowania zespołem?

Cyberbezpieczeństwo nie było jeszcze traktowane tak poważnie, jak obecnie, zarówno w samym NASK, jak i w kraju czy na poziomie rządowym. CERT Polska był w tym czasie de facto CERT-em narodowym, mającym uznanie zarówno w kraju, jak i za granicą, ale bez oficjalnego mandatu ze strony państwa. Oznaczało to między innymi konieczność zapewnienia finansowania z własnych środków NASK lub z grantów europejskich

i w mniejszym stopniu grantów krajowych. Nie było nas stać na większe inwestycje, ale udało się zainwestować w to, co najważniejsze – w ludzi.

Kluczowe w tym okresie było podjęcie decyzji co do kierunku rozwoju zespołu, co wcale nie było w owym czasie oczywiste.

Z perspektywy czasu które decyzje, zmiany lub osiągnięcia były Twoim zdaniem kluczowe?

Przede wszystkim podjęcie decyzji o specjalizacji, niezależności i rozwoju własnych narzędzi. Zdając sobie sprawę, że kilkunastoma osobami w CERT nie jesteśmy w stanie być dobrzy we wszystkich aspektach związanych z reagowaniem na incydenty na skalę krajową, skupiliśmy się na tematach, w których mogliśmy osiągnąć największy impakt. Były to między innymi rozwój i dystrybucja feedów threat intelligence w kraju, rozwój situational awareness tego, co się dzieje w kraju, rozwój samodzielnej analizy malware i systemów detekcji zagrożeń, aktywne rozbijanie botnetów i przeciwdziałanie im (w tym poprzez sinkholowanie).

Kluczowe działanie, które bardzo zmieniło obraz cyber w Polsce, to wypracowanie procesu zawieszenia i przejmowania domen .pl (tzw. sinkholing), które były wykorzystywane do zarządzania botnetami lub do dystrybucji malware'u – w tym ówcześnie bardzo znanym botnetem Virut. Dzięki temu szybko „wyczyściliśmy" domenę .pl z tego typu zagrożeń, co zyskało uznanie również za granicą. To z kolei doprowadziło do wielu kolejnych współdziałań w tym obszarze na skalę międzynarodową, a publikacje w języku angielskim napędzały pozytywny wizerunek zespołu.

Udało się stworzyć pozytywną atmosferę w zespole, która przetrwała lata i przyciągnęła osoby, które chciały coś zmienić dla dobra ogółu. Zachętą dla wielu była duża swoboda w wyborze tego, na czym ktoś chciał się skupić, rozwój osobisty poprzez udział w konkursach CTF (z licznymi sukcesami) czy międzynarodowych konferencjach, które były też okazją do nawiązywania kontaktów ze specjalistami z innych krajów.

Efektem różnych naszych działań są systemy funkcjonujące do dziś, takie jak ARAKIS, n6, BotSense czy MWDB, a zespół do tej pory znany jest na świecie z własnych (nowych) rozwiązań.

Jakie Twoim zdaniem będą największe wyzwania w cyberbezpieczeństwie w ciągu najbliższych 5 lat? W szczególności w kontekście roli, jaką może odegrać CERT Polska.

Wyzwań jest trochę, ale skupię się na tym najbliżej związanym z efektywnym reagowaniem na incydenty w skali kraju, w sytuacji, kiedy pojawienie się nowej podatności umożliwiającej zdalne wykonanie kodu w popularnym produkcie z automatu oznacza pojawienie się ataków.

Obecnie mówi się, że „cybersecurity is national security". Każde urządzenie podpięte do sieci może stać się celem ataku nie tylko cyberprzestępczego, lecz także takiego, za którym stoi inne państwo. I tak już się dzieje. Każda nowa wykryta podatność, która umożliwia zdalne wykonanie

kodu na podatnym urządzeniu, czy jest to router firmowy, czy domowy, firewall, VPN, PLC czy system dzielenia plików itp., jest natychmiast wykorzystywana, zarówno przez cyberprzestępców, jak i wrogie państwa.

Aby chronić państwo, kluczowe jest zrozumienie, jak w danym momencie wygląda tzw. attack surface infrastruktury sieciowej w Polsce – który to może zmieniać się z dnia na dzień, a nawet z godziny na godzinę. Konieczne jest także wypracowanie sprawnego systemu, tak aby móc jak najszybciej reagować na nowe podatności i nowe ataki z partnerami w całym kraju, w dużej mierze z wykorzystaniem automatyzacji (i być może w jakimś stopniu, na ile się da, AI).

W tym obszarze jest wiele do zrobienia w Polsce (co pokazały zresztą niedawne ataki na energetykę). CERT Polska jest w dobrym miejscu, aby w tym obszarze odegrać wiodącą role.

Przemysław Jaroszewski

KIEROWNIK CERT POLSKA W LATACH 2016–2021

Jak wyglądał krajobraz cyberbezpieczeństwa w Polsce, kiedy obejmowałeś stanowisko kierownika CERT Polska? Jakiego rodzaju zagrożenia dominowały?

Dla wszystkich użytkowników internetu niewątpliwie momentem definiującym był początek pandemii COVID. Wymusił on gwałtowne przyspieszenie cyfryzacji usług, zarówno w sektorze rządowym, jak i prywatnym. Niestety, trend ten natychmiast wykorzystali przestępcy, mnożąc scenariusze wyłudzeń – od fałszywych sklepów po strony rządu czy organizacji społecznych.

Okres ten był także początkiem intensywnych dyskusji na temat zagrożenia wojną informacyjną i zwalczania dezinformacji w sieci.

Jakie były największe wyzwania w okresie kierowania zespołem?

Czas ten zbiegł się z wprowadzaniem w życie ustawy o krajowym systemie cyberbezpieczeństwa. Była to pierwsza tak kompleksowa regulacja dotycząca obowiązków i odpowiedzialności podmiotów kluczowych dla państwa i obywatela. Największym wyzwaniem było zbudowanie zaufania przedsiębiorstw i instytucji objętych ustawą do państwowych CSIRT-ów, które zbierają szereg wrażliwych informacji o infrastrukturze, ale jednocześnie wspierają swoje constituency w reagowaniu i budowaniu odporności.

Z perspektywy czasu które decyzje, zmiany lub osiągnięcia były Twoim zdaniem kluczowe?

Na pewno kluczowe było wejście w życie wspomnianej ustawy o KSC, co pociągnęło za sobą szereg zmian organizacyjnych w NASK, a także przedefiniowało rolę zespołu CERT Polska. Od tego momentu zespół

po raz pierwszy uzyskał prawnie zdefiniowane obowiązki i narzędzia do walki z cyberzagrożeniami.

Jakie Twoim zdaniem będą największe wyzwania w cyberbezpieczeństwie w ciągu najbliższych 5 lat? W szczególności w kontekście roli, jaką może odegrać CERT Polska.

Myślę, że największym wyzwaniem pozostanie budowanie i utrzymywanie zaufania do instytucji państwowych i partnerstwa publiczno-prywatnego. Ważna jest tu rola podmiotów takich jak CSIRT-y sektorowe, które powinny działać, angażując bezpośrednio w swoje struktury podmioty objęte regulacjami.

Sebastian Kondraszuk

KIEROWNIK CERT POLSKA W LATACH 2021–2024

Jak wyglądał krajobraz cyberbezpieczeństwa w Polsce, kiedy obejmowałeś stanowisko kierownika CERT Polska? Jakiego rodzaju zagrożenia dominowały?

Lata 2021–2024 to czas bardzo dynamicznego przyrostu zgłoszeń w kategorii oszustw internetowych. Za niezwykle istotne uważam to, że nie pozostawaliśmy biernym obserwatorem wydarzeń. To czas, w którym zostało przetestowanych wiele metod wykrywania zagrożeń wspierających bardzo wczesne oznaczanie infrastruktury zaangażowanej w oszukańczy proceder. Niektóre z tych pomysłów przełożyliśmy z sukcesem na wewnętrzne projekty ukierunkowane na jakość rejestracji w domenie .pl prowadzonej przez NASK–PIB. Lista Ostrzeżeń, której działanie zapoczątkowaliśmy w 2020 roku, stała się kluczowym ogniwem w łańcuchu ochrony internautów przed wyłudzeniami w sieci. Warto o tym pamiętać, kiedy dziennie na Listę trafia blisko 700 domen!

Jakie były największe wyzwania w okresie kierowania zespołem?

Siłą CERT Polska od zawsze byli ludzie go tworzący. Działając jednak wobec stale rozwijanego zakresu działania, przy równoczesnym dynamicznym wzroście otrzymywanych zgłoszeń, stanęliśmy przed wyzwaniem zapewnienia dopływu, jak i utrzymania, potrzebnych nam zasobów ludzkich. Ze względu na ograniczoną możliwość konkurowania z rynkiem komercyjnym jeszcze mocniej postawiliśmy na rozwój zdolności wewnątrz. Dla nikogo nie będzie też zaskoczeniem, że dla ludzi pracujących w CERT Polska nie mniej ważna od wynagrodzenia jest i zawsze była możliwość realizacji przedsięwzięć rozwijających Polskę. Wierzę, że tak długo, jak utrzymamy te dwa filary, tak długo będziemy przyciągać najlepszych ekspertów w kraju.

Drugi obszar, na który patrzyłem jak na wyzwanie, to stale rosnąca skala otrzymywanych zgłoszeń oraz ich nierównomierny rozkład, w szczególności wobec potrzeby zachowania priorytetów, które nie kończyły się przecież na problematyce oszustw w internecie. Dobrym testem naszych zdolności była reklama zachęcająca do wykonywania zgłoszeń do CERT Polska wyemitowana podczas mistrzostw świata w piłce nożnej w trakcie meczu Polska – Argentyna. Tego dnia odnotowaliśmy rekordowy wskaźnik dobowy zgłoszeń. Dziś, głównie dzięki rozwiniętej automatyzacji, nagły i znaczący napływ zgłoszeń to sytuacja, z którą sobie dobrze radzimy.

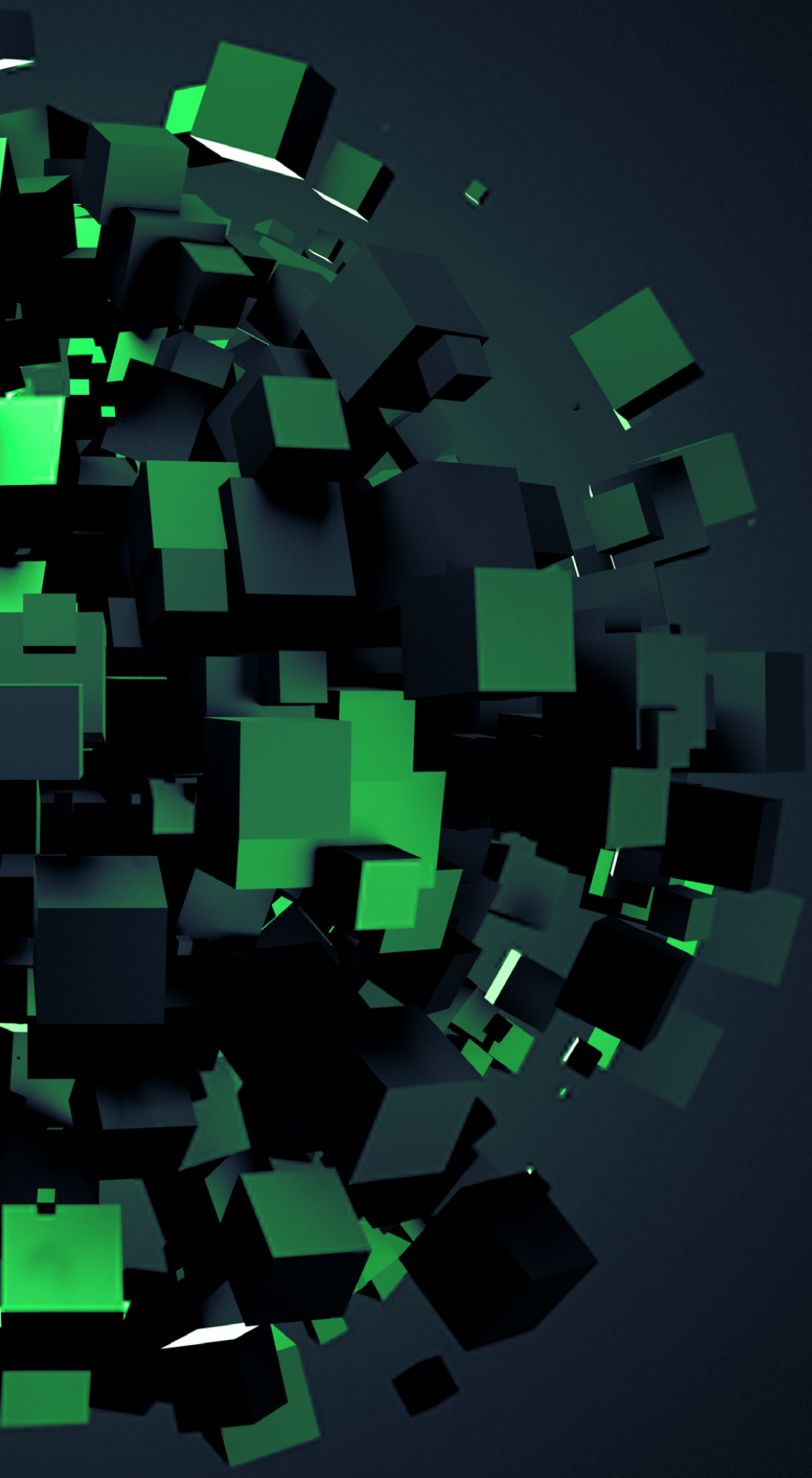
Z perspektywy czasu które decyzje, zmiany lub osiągnięcia były Twoim zdaniem kluczowe?

Na polu walki z oszustwami w internecie za olbrzymi sukces należy uznać wypracowanie akceptowalnych przez strony oraz skutecznych rozwiązań legislacyjnych, a następnie wdrożenie ich w praktyce. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej to idealny przykład tego, jak skoordynowana wymiana informacji pomiędzy uczestnikami rynku może podnosić poziom bezpieczeństwa. Kieruję tutaj słowa uznania do wszystkich byłych i obecnych operatorów CERT Polska za wkład wniesiony w proces podejmowania bardzo ważnych dla internautów decyzji, które chroniły ich dane oraz pieniądze. Pragnę też równie mocno docenić proces profesjonalizacji obszaru informatyki śledczej. Wnioski wyciągane z analizy najpoważniejszych incydentów w kraju przyczyniły się do rozwoju kompetencji oraz warsztatu, dzięki któremu często mamy komfort pełnego rozumienia przebiegu ataku. Co więcej, z sukcesem wspieramy też zdobytym doświadczeniem krajowe organy ścigania.

Jakie Twoim zdaniem będą największe wyzwania w cyberbezpieczeństwie w ciągu najbliższych 5 lat? W szczególności w kontekście roli, jaką może odegrać CERT Polska.

Według mnie dalej będziemy obserwować skracanie cyklu życia schematów stosowanych przez przestępców. CERT Polska ma i dalej będzie mieć niebagatelną rolę w zakresie ich rozpoznawania oraz dokumentowania. Wyzwaniem na pewno będzie dotarcie w możliwie najkrótszym czasie z informacją, która przysłuży się internautom na polu podejmowania przez nich decyzji. Za drugi bardzo ważny cel uważam dalszy przewidywany wzrost świadomości uczestników systemu cyberbezpieczeństwa, a także dostrzeganie korzyści wynikających z aktywnego uczestnictwa w nim. Te podmioty w znakomitej większości będą obszarem odpowiedzialności CSIRT NASK. Wierzę w to, że nadal będziemy jednym z wiodących miejsc na mapie polskiego cyberbezpieczeństwa, z szeroką, a przede wszystkim użyteczną ofertą.

Incydenty i zagrożenia



Przegląd nowych kampanii

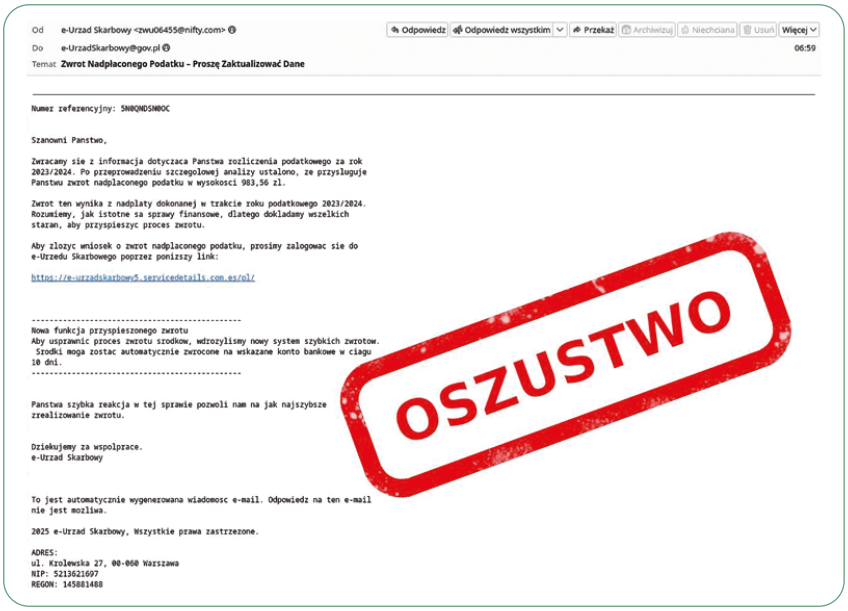
Krajobraz zagrożeń w polskiej cyberprzestrzeni nieustannie ewoluuje. Przestępcy systematycznie doskonalą swoje metody, a ich kampanie stają się coraz trudniejsze do odróżnienia od autentycznej korespondencji. Wśród utrwalonych schematów ataków dominują kampanie phishingowe ukierunkowane na kradzież haseł do kont poczty elektronicznej oraz serwisów społecznościowych. Niezmiennie wysoką aktywność wykazują również fałszywe witryny podszywające się pod serwisy rządowe i dostawców usług kurierskich, w szczególności pod Pocztę Polską oraz InPost.

W dalszej części rozdziału przedstawiliśmy przegląd najczęściej występujących kampanii w 2025 roku wraz z opisem technik stosowanych przez oszustów oraz potencjalnych konsekwencji dla użytkowników.

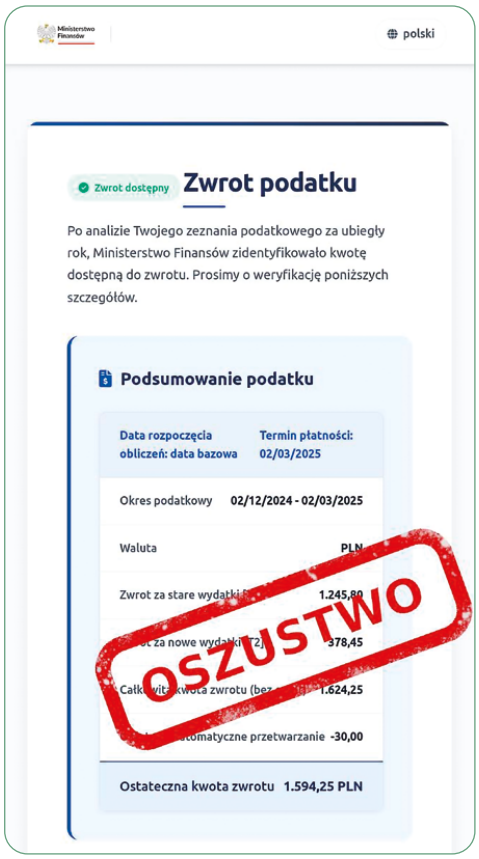
Zwrot podatku – e-Urząd Skarbowy oraz KAS

Jednym z najpopularniejszych scenariuszy phishingowych pozostaje obietnica zwrotu podatku. Przestępcy wykorzystują wizerunek Ministerstwa Finansów, rozsyłają wiadomości e-mail o rzekomym zwrocie oczekującym na zatwierdzenie. Komunikaty charakteryzują się profesjonalnym wyglądem naśladującym oficjalną korespondencję instytucji państwowych, co zwiększa ich wiarygodność. Wiadomości zawierają odnośnik do fałszywej strony imitującej portal rządowy. Pod pretekstem finalizacji procedury zwrotu strona wyłudza dane logowania do bankowości elektronicznej i dane karty płatniczej. Przechwycone dane umożliwiają sprawcom przejęcie kont bankowych ofiar oraz dokonywanie transakcji w ich imieniu.

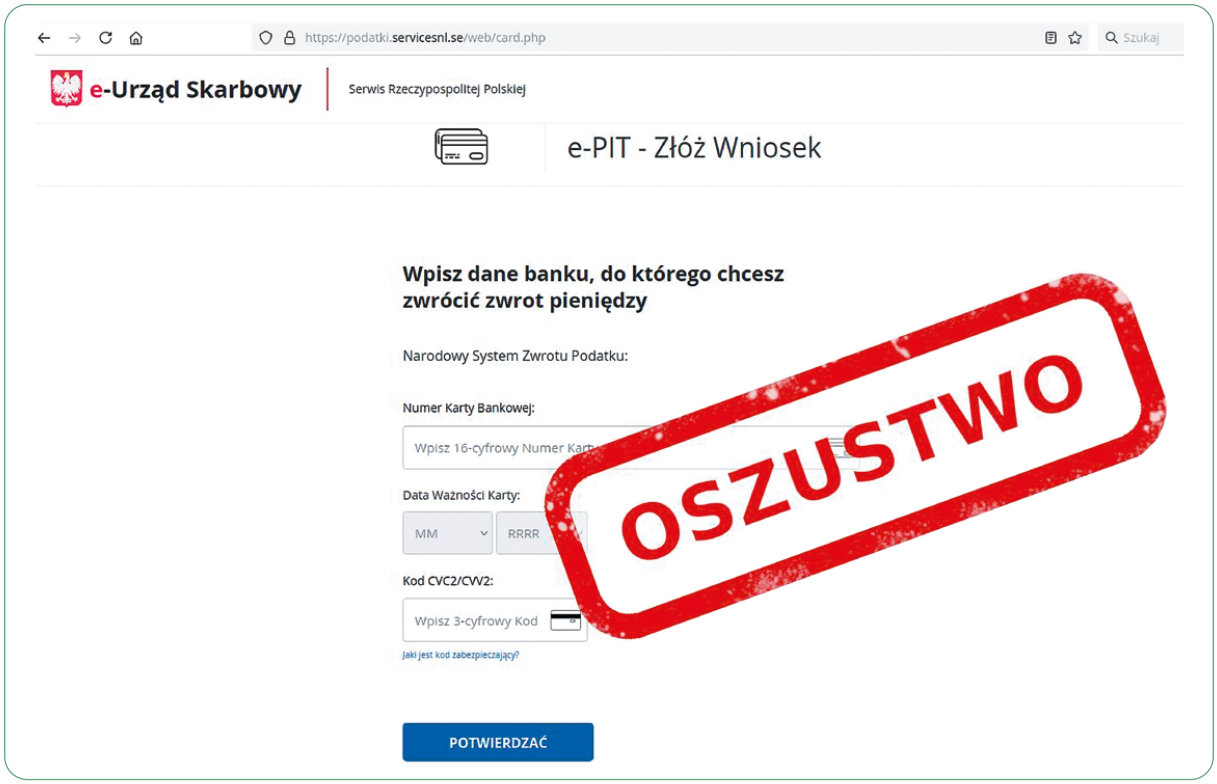
RYSUNEK 1. Fałszywa wiadomość informująca o zwrocie nadpłaconego podatku



RYSUNEK 2. Przykład oszustwa na zwrot podatku



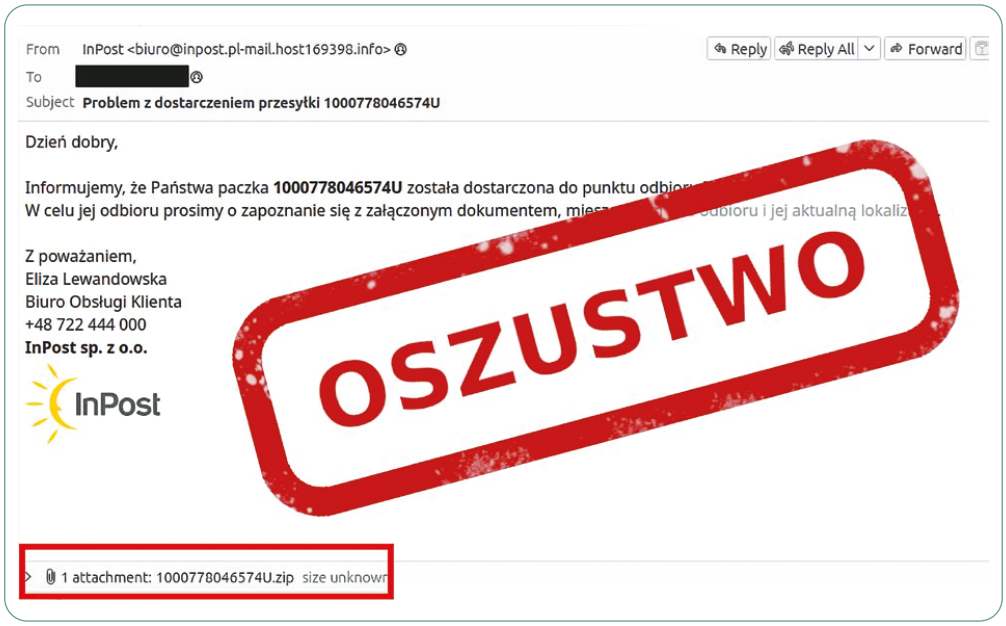
RYSUNEK 3. Fałszywa strona służąca do wyłudzania danych karty płatniczej



Niedostarczone paczki – InPost, Poczta Polska, e-Doręczenia

Popularność zakupów internetowych sprawia, że wiadomości dotyczące przesyłek kurierskich są skuteczną przynętą wykorzystywaną przez cyberprzestępców. Szczególnie często podszywają się oni pod firmę InPost. W fałszywych wiadomościach e-mail informują o rzekomych problemach z doręczeniem przesyłki i nakłaniają odbiorcę do pobrania i uruchomienia załącznika. Załącznik zawiera złośliwy skrypt, który po uruchomieniu instaluje na urządzeniu ofiary szkodliwe oprogramowanie. Umożliwia ono kradzież haseł do kont poczty elektronicznej, a ponadto wykorzystuje moc obliczeniową zainfekowanego urządzenia do wydobywania kryptowalut (tzw. cryptojacking).

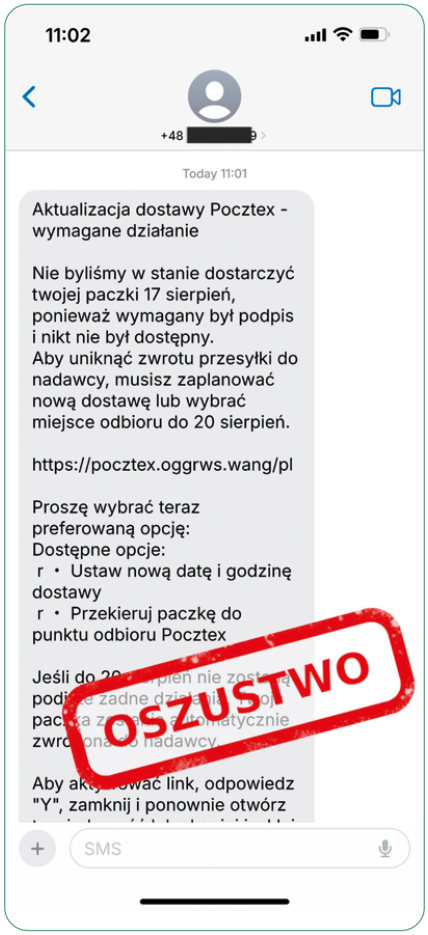
RYSUNEK 4. Fałszywa wiadomość, w której oszuści informują odbiorcę o problemie z dostarczeniem przesyłki



Oprócz wiadomości e-mail przestępcy wykorzystują także kanał SMS. Oszukańcze wiadomości tekstowe informują o fikcyjnych problemach z doręczeniem przesyłki i kierują odbiorców do witryn phishingowych imitujących strony popularnych firm kurierskich w celu wyłudzenia danych osobowych oraz informacji o kartach płatniczych.

Szczególnie ciekawy jest wariant kampanii omijający wbudowane zabezpieczenia telefonów przed otwieraniem linków od nieznanych nadawców. Nakłonienie odbiorcy do wysłania odpowiedzi na wiadomość powoduje aktywację zawartego w niej odnośnika i ułatwia przejście do strony phishingowej. To pokazuje, jak przestępcy zmieniają swój sposób działania w odpowiedzi na wprowadzanie nowych mechanizmów bezpieczeństwa.

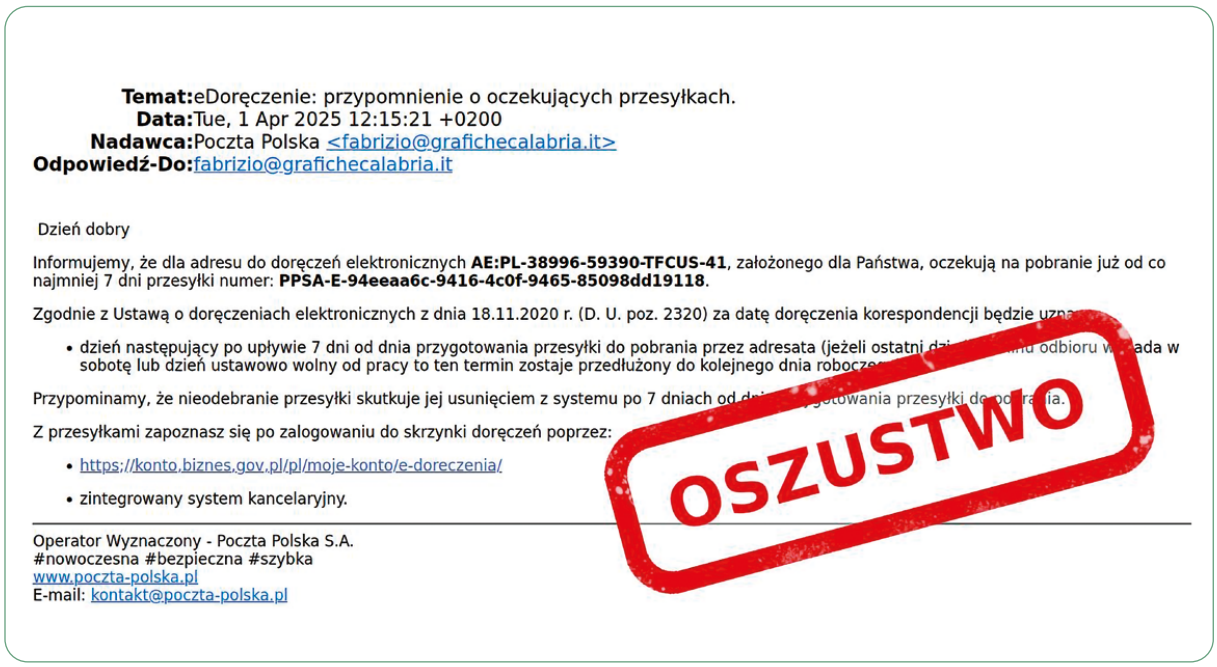
RYSUNEK 5. Przykład fałszywej wiadomości SMS, w której oszuści nakłaniają użytkownika do wysłania odpowiedzi



Wraz z rosnącą popularnością usług cyfrowej administracji pojawiły się kampanie podszywające się pod system e-Doręczeń. Sfałszowane wiadomości e-mail informują o nieodebranej przesyłce urzędowej i zawierają ostrzeżenie o jej usunięciu w razie braku reakcji w określonym terminie.

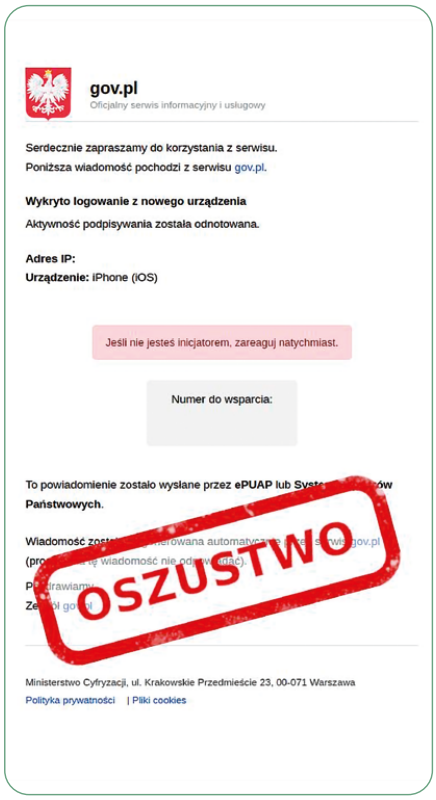
Komunikaty zawierają odnośnik do witryny imitującej portal biznes.gov.pl, na której wyłudzane są dane logowania do kont poczty elektronicznej. Kampania wykorzystuje poczucie pilności – groźba usunięcia dokumentów ma skłonić odbiorcę do natychmiastowego działania bez weryfikacji, czy wiadomość jest autentyczna.

RYSUNEK 6. Fałszywa wiadomość z linkiem do strony wyłudzającej dane logowania do poczty elektronicznej



Sprawy urzędowe – serwisy w domenie gov.pl

Serwisy rządowe w domenie gov.pl cieszą się wysokim zaufaniem społecznym, dlatego przestępcy często wykorzystują ich wizerunek w swoich kampaniach. Rozsyłane wiadomości występują w kilku wariantach: powiadomienia o oczekującej korespondencji urzędowej, o wykrytej aktywności na koncie użytkownika lub o zarejestrowaniu sesji na nieznanym urządzeniu mobilnym.

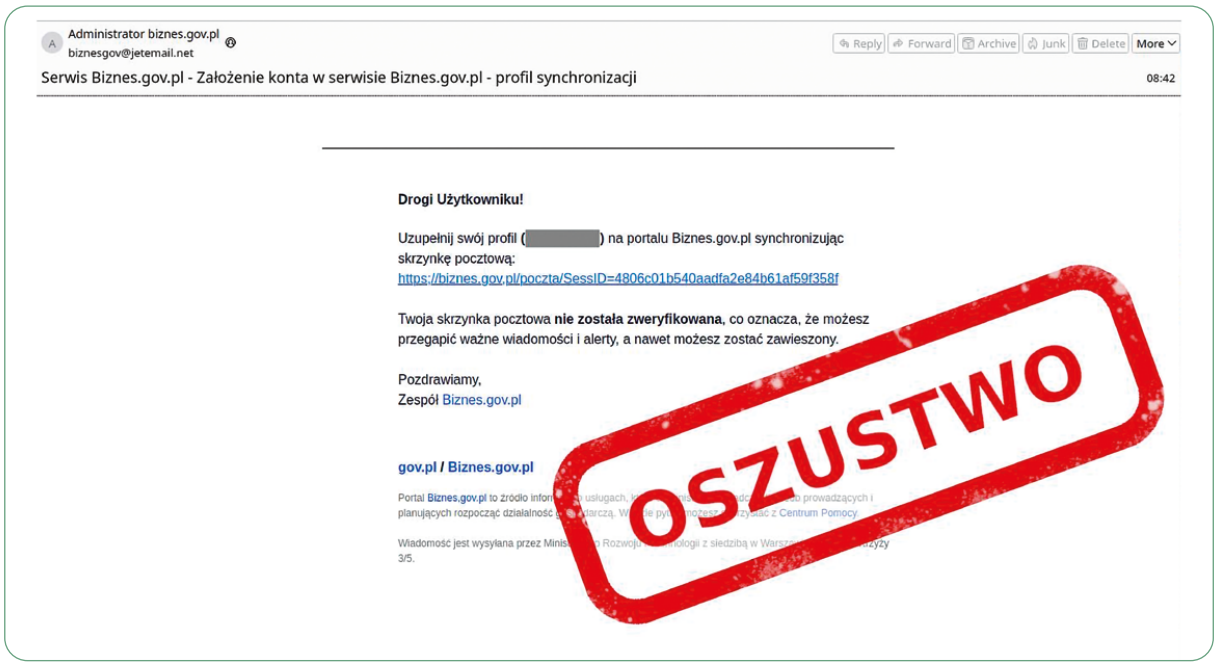


Wspólnym elementem wszystkich wariantów jest próba nakłonienia odbiorcy do nawiązania kontaktu telefonicznego pod wskazanym numerem. W trakcie rozmowy sprawcy stosują różne techniki manipulacji, aby skłonić ofiarę do instalacji oprogramowania umożliwiającego zdalny dostęp do jej komputera.

Przejęcie kontroli nad urządzeniem pozwala atakującym na wykonywanie przelewów z konta ofiary, co prowadzi do utraty zgromadzonych środków.

RYSUNEK 7. Fałszywa wiadomość informująca o nowej sesji na nieznanym urządzeniu mobilnym

RYSUNEK 8. Fałszywa wiadomość, w której oszuści nakłaniają użytkownika do synchronizacji skrzynki pocztowej

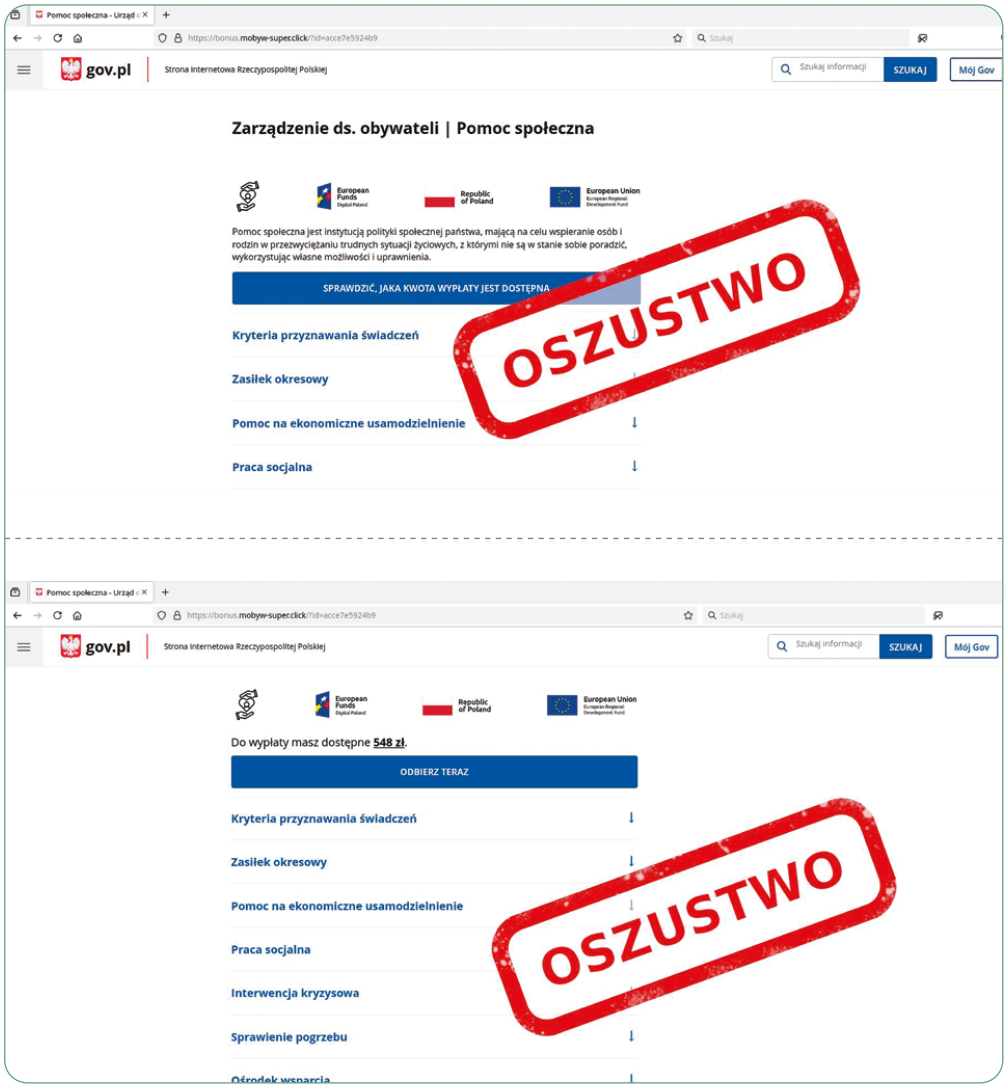


Weryfikacja uprawnień do świadczeń socjalnych

Obietnica łatwego dostępu do świadczeń socjalnych to kolejny skuteczny scenariusz oszustwa. W mediach społecznościowych rozpowszechniane są oszukańcze reklamy oferujące sprawdzenie uprawnień do dodatkowych wypłat. Reklamy kierują użytkowników do witryn imitujących portal gov.pl, gdzie jedynym wymaganym krokiem jest podanie numeru PESEL.

Po wprowadzeniu numeru PESEL następuje przekierowanie do strony podszywającej się pod operatora płatności Przelewy24, zawierającej sfałszowane formularze logowania do bankowości internetowej. Przechwycone dane logowania umożliwiają dostęp do rachunków bankowych ofiar i kradzież środków.

RYSUNEK 9. Fałszywa strona podszywająca się pod portal gov.pl, na której można rzekomo sprawdzić przysługujące świadczenia socjalne

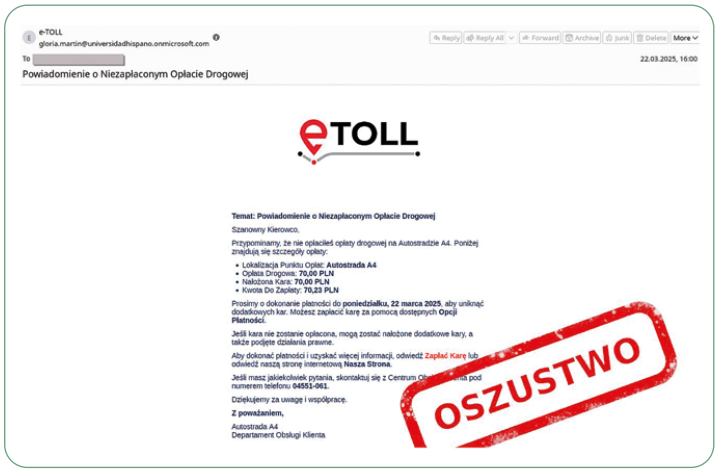


Opłata e-TOLL

Oszukańcze wiadomości dotyczące systemu e-TOLL trafiają na podatny grunt wśród kierowców. Komunikaty informują o rzekomym nieuregulowaniu opłaty za przejazd i zawierają odnośnik do strony naśladującej oficjalny serwis.

Strona zawiera dwuetapowy mechanizm wyłudzenia danych. Pierwszy formularz służy do pozyskania danych osobowych ofiary, w tym numeru dowodu osobistego. Drugi przechwytuje dane karty płatniczej wraz z kodem CVV/CVC. Pozyskane informacje umożliwiają sprawcom kradzież pieniędzy z konta ofiary.

RYSUNEK 10. Fałszywe powiadomienie o niezapłaconej opłacie drogowej



Urząd Statystyczny

Przestępcy wykorzystują także nazwę Urzędu Statystycznego w Warszawie. Rozsyłane wiadomości e-mail informują o fikcyjnym obowiązku uzupełnienia dokumentacji i zawierają złośliwy załącznik.

Wiarygodność komunikatów jest wzmacniana dzięki profesjonalnej strukturze wiadomości, łącznie ze szczegółową stopką, która pojawia się w oficjalnej korespondencji instytucji publicznej. Załącznik zawiera oprogramowanie typu RAT (ang. Remote Access Trojan – trojan umożliwiający zdalny dostęp), które po uruchomieniu pozwala sprawcom przejąć kontrolę nad komputerem ofiary. Złośliwe oprogramowanie wykrada zapisane hasła i inne poufne dane przechowywane na zainfekowanym urządzeniu.

RYSUNEK 11. E-mail zawierający złośliwy załącznik – przykład wykorzystania wizerunku Urzędu Statystycznego w Warszawie

Fałszywe inwestycje – reklamy w mediach społecznościowych

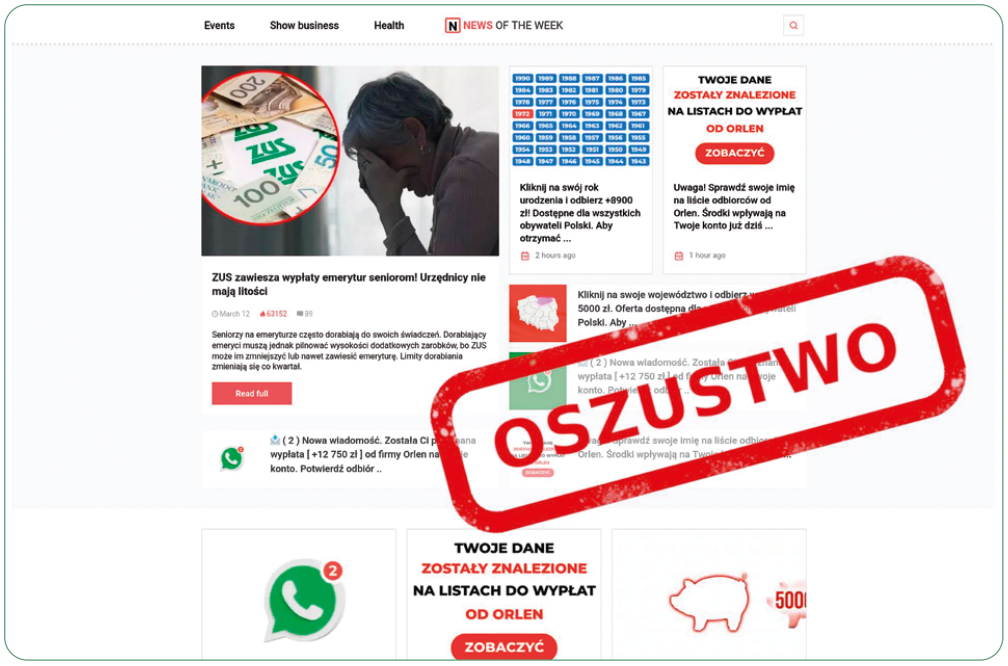
Oszustwa inwestycyjne należą do najbardziej dotkliwych finansowo zagrożeń w polskiej cyberprzestrzeni. Sprawcy masowo rejestrują witryny oferujące fikcyjne programy inwestycyjne i platformy transakcyjne, często przy tym posługują się wizerunkiem osób publicznych jako fałszywymi rekomendacjami.

Mechanizm oszustwa opiera się na manipulacji psychologicznej. Po dokonaniu wpłaty ofierze prezentowane są sfałszowane wykresy wykazujące pozorny wzrost wartości zainwestowanych środków. Symulacja zysków ma na celu budowanie zaufania i skłonienie użytkownika do dokonania kolejnych wpłat. Próba wypłaty środków ujawnia rzeczywisty charakter procederu – zgromadzone fundusze zostają przejęte przez sprawców.

Typowym elementem takich kampanii jest wywieranie presji czasowej oraz eksponowanie wizji ponadprzeciętnych zysków przy minimalnym ryzyku.

RYSUNEK 12. Fałszywa platforma inwestycyjna podszywająca się pod Baltic Pipe

RYSUNEK 13. Fałszywa platforma inwestycyjna podszywająca się pod firmę Orlen



NFZ – zwrot kosztów zakupu leków

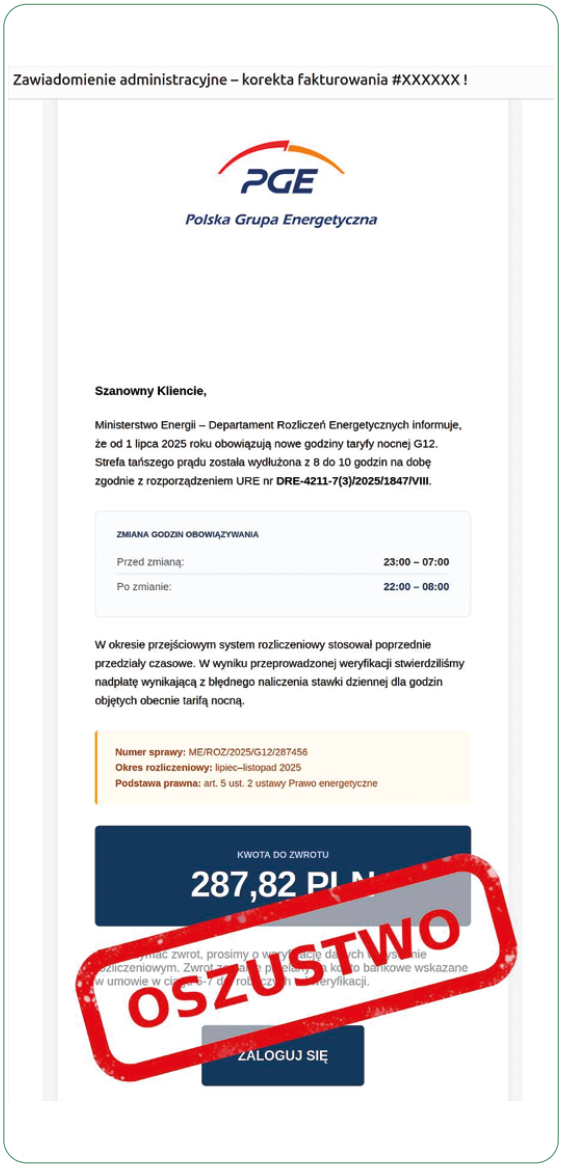
Sektor ochrony zdrowia nie pozostaje poza zainteresowaniem cyberprzestępców. Wiadomości, w których podszywają się oni pod Narodowy Fundusz Zdrowia, informują o możliwości uzyskania zwrotu kosztów zakupionych leków i kierują odbiorców do spreparowanej strony służącej wyłudzeniu danych osobowych i haseł.

Przestępcy stosują ponadto technikę presji czasowej – komunikaty zawierają informację o krótkim terminie na odebranie środków, co ogranicza czas na weryfikację autentyczności wiadomości i skłania użytkownika do nieprzemyślanej reakcji.

RYSUNEK 14. Oszustwo wykorzystujące motyw zwrotu kosztów zakupu leków

RYSUNEK 15. Fałszywe powiadomienie o zwrocie środków przyznanym przez NFZ

RYSUNEK 16. Fałszywy e-mail informujący o rzekomej nadpłacie za prąd i przysługującym zwrocie



Zwrot nadpłaty za energię elektryczną

W kontekście rosnących cen energii szczególną skuteczność wykazują kampanie obiecujące zwrot nadpłaty za prąd. Przestępcy podszywają się pod dostawców energii elektrycznej i powołują się na fikcyjne zmiany w przepisach prawnych. Komunikaty kierują odbiorców do fałszywych stron służących wyłudzeniu informacji o kartach płatniczych.

Kampania charakteryzuje się wysokim poziomem profesjonalizmu. Wiadomości napisane są poprawną polszczyzną, zachowany jest formalny styl korespondencji, a witryny phishingowe wiernie odwzorowują szatę graficzną oficjalnych stron operatorów energetycznych. Staranne wykonanie materiałów znacząco utrudnia rozpoznanie zagrożenia. Najważniejszą wskazówką pozostaje adres strony, który może być podobny do oryginalnego, ale na pewno różni się od niego choćby drobnym elementem.

Podsumowanie

Analiza przedstawionych kampanii phishingowych pozwala zidentyfikować wspólne cechy charakterystyczne współczesnych zagrożeń w polskiej cyberprzestrzeni, z których znakomita większość to phishing. Przestępcy konsekwentnie podszywają się pod zaufane instytucje – zarówno państwowe, jak i prywatne – profesjonalnie naśladując ich oficjalną korespondencję. Stosowane techniki manipulacji psychologicznej, zwłaszcza wywoływanie poczucia pilności, oraz obietnice korzyści finansowych skutecznie skłaniają ofiary do działania bez należytej weryfikacji.

Obserwowany trend wskazuje na systematyczny wzrost poziomu zaawansowania ataków. Materiały phishingowe charakteryzują się coraz wyższą jakością wykonania – poprawną polszczyzną, wiernymi kopiami oryginalnych interfejsów oraz przemyślaną strukturą komunikatów. Sprawcy elastycznie dostosowują scenariusze oszustw do bieżących wydarzeń, sezonowych trendów i zmian legislacyjnych, co dodatkowo zwiększa skuteczność prowadzonych kampanii.

Malware mobilny

W tym rozdziale prezentujemy statystyki dotyczące złośliwego oprogramowania na urządzenia mobilne z systemem Android obserwowanego i wykrytego przez zespół CERT Polska w 2025 roku. Analizowane próbki pochodzą z działań typu threat hunting, zgłoszeń od użytkowników oraz z platformy MWDB.

W 2025 roku zgłosiliśmy do Google łącznie 393 próbki złośliwego oprogramowania na urządzenia mobilne oraz 119 aplikacji podszywających się pod znane polskie firmy. Aplikacje te były dystrybuowane w Google Play Store, a po zgłoszeniach zostały zdjęte ze sklepu. Pozostałe złośliwe aplikacje były hostowane na zewnętrznych serwisach, a liczba unikalnych próbek wymierzonych w polskich użytkowników, które zaobserwowaliśmy, wyniosła 181.

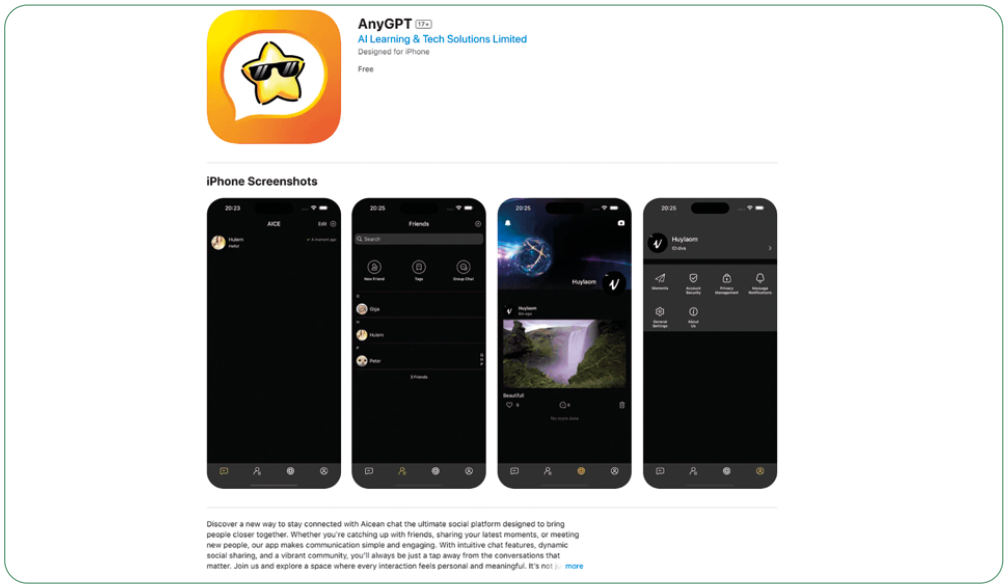
Przegląd wybranych kampanii mobilnego złośliwego oprogramowania w 2025 roku

Spark cat

Cyberprzestępcy zastosowali złośliwy kod wykorzystujący specjalny framework oparty na technologii OCR (optycznego rozpoznawania znaków). Dzięki niemu aplikacje były w stanie przeanalizować obrazy przechowywane na urządzeniu ofiary, a także odczytać z nich wrażliwe informacje, np. hasła czy frazy odzyskiwania portfeli kryptowalutowych.

Cyberprzestępcy skupiali się głównie na kradzieżach kryptowalut, takich jak Bitcoin, choć malware mógł również służyć do przechwytywania innych poufnych danych. Aplikacje były dystrybuowane przez AppStore oraz Google Play Store.

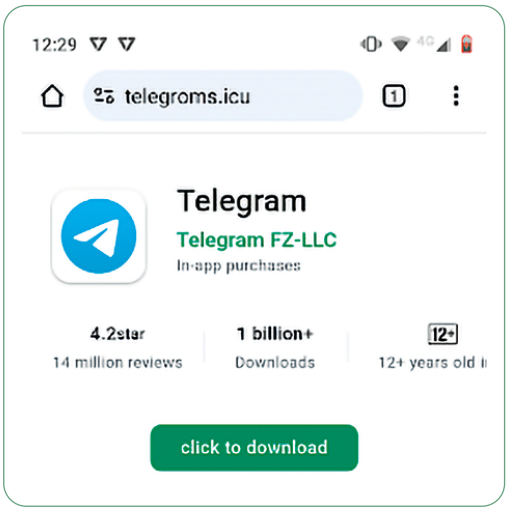
RYSUNEK 17. Zrzut ekranu z AppStore złośliwej aplikacji z rodziny Spark cat



SpyMax

Kampania złośliwego oprogramowania SpyMax, którą zaobserwowaliśmy, była wymierzona w użytkowników aplikacji Telegram. Szkodliwe aplikacje rozpowszechniano za pośrednictwem strony internetowej podszywającej się pod Google Play Store. Po uruchomieniu malware jest instalowany na urządzeniu pod postacią legalnej aplikacji Telegrama. Oprogramowanie SpyMax posiada typowe funkcje RAT, w tym keylogger i wykradanie poufnych informacji z zainfekowanych urządzeń.

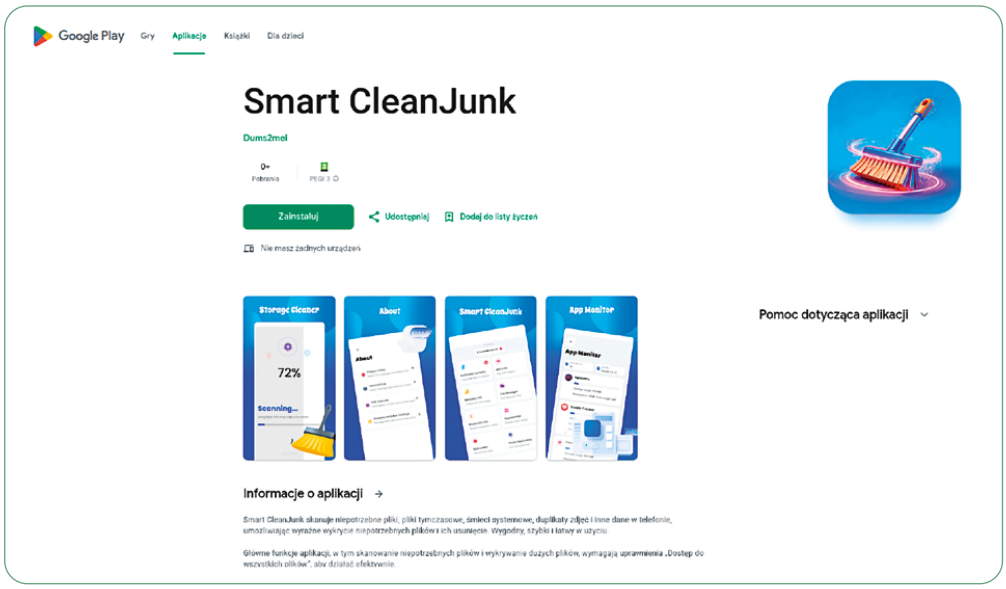
RYSUNEK 18. Zrzut ekranu ze strony internetowej podszywającej się pod Google Play Store



Joker

Na temat kampanii złośliwego oprogramowania Joker pisaliśmy szerzej w 2024 roku w artykule pt. „Mroczny rycerz powraca: Analiza złośliwego oprogramowania Joker” (https://cert.pl/posts/2024/10/analiza-joker). W 2025 roku wykryliśmy kolejne 352 próbki, które zostały przez nas przeanalizowane oraz zgłoszone bezpośrednio do Google. Wszystkie próbki zostały usunięte z Google Play Store.

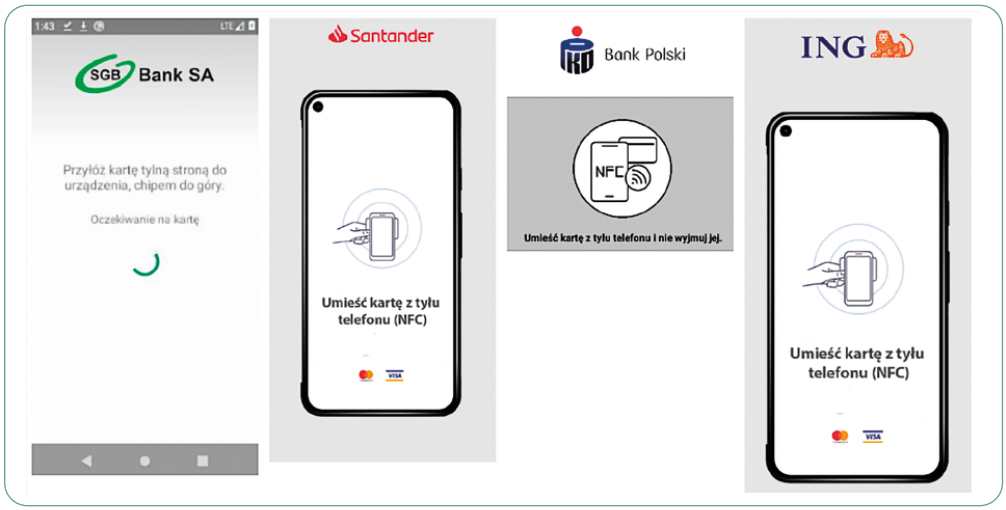
RYSUNEK 19. Zrzut ekranu z Google Play Store złośliwej aplikacji Joker



NGate

Najgroźniejszą kampanią złośliwego oprogramowania na urządzenia mobilne, którą zaobserwowaliśmy w 2025 roku, wymierzoną w polskich użytkowników, była kampania NGate. Celem ataku jest umożliwienie nieuprawnionych wypłat gotówki z bankomatów z wykorzystaniem kart płatniczych ofiar. Przestępcy nie kradną fizycznie karty. Zamiast tego przekazują ruch NFC karty z telefonu ofiary do urządzenia przestępcy stojącego przy bankomacie. Więcej na temat tego zagrożenia można przeczytać w naszym artykule pt. „Analiza kampanii złośliwego oprogramowania NGate (NFC relay)" (https://cert.pl/posts/2025/11/analiza-ngate).

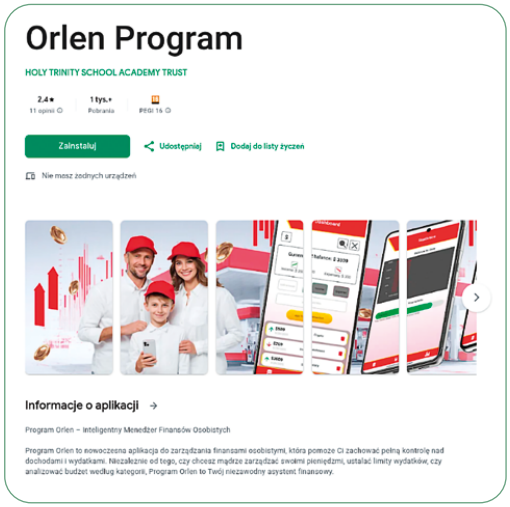
RYSUNEK 20. Zrzuty ekranu z aplikacji NGate



Aplikacje podszywające się pod znane polskie firmy w Google Play Store

W 2025 roku zaobserwowaliśmy wzrost liczby aplikacji podszywających się w Google Play Store pod znane polskie koncerny paliwowo-energetyczne, firmy, instytucje – zgłosiliśmy 119 takich aplikacji, a najczęściej pojawiającą się firmą był Orlen. Przeważnie zadaniem tych aplikacji jest próba wyłudzenia pieniędzy z fałszywych inwestycji. W obecnym modelu działania aplikacje te zazwyczaj są reklamowane w innych, zainstalowanych już na urządzeniu potencjalnej ofiary, aplikacjach wraz z linkiem do Google Play Store, a sama reklama oraz aplikacja wykorzystują wizerunek innej znanej i rozpoznawalnej firmy.

RYSUNEK 21. Zrzut ekranu z Google Play Store aplikacji podszywającej się pod firmę Orlen



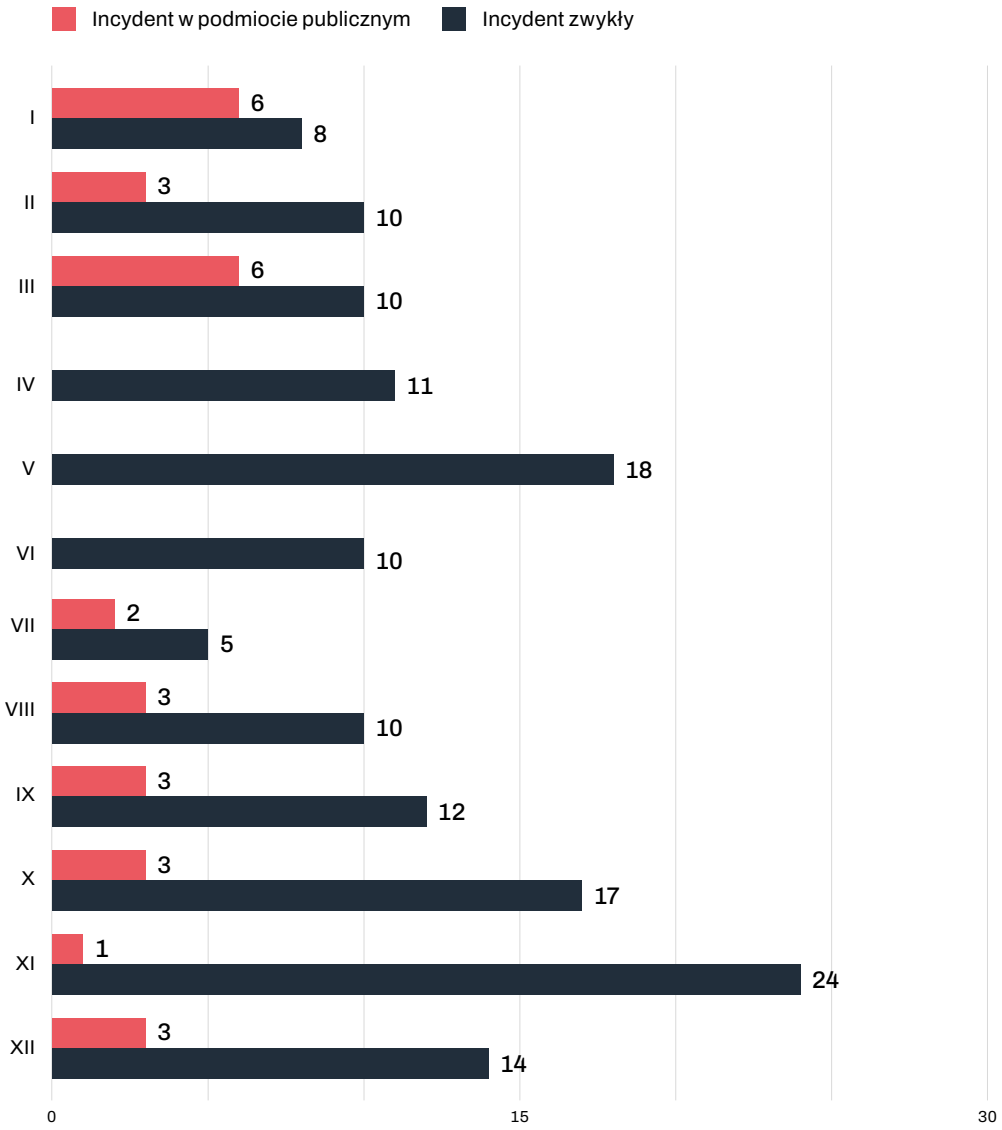
Ransomware

2025 rok przyniósł nam kolejny rekord liczby odnotowanych incydentów związanych z atakami szkodliwego oprogramowania typu ransomware. Incydenty te w dalszym ciągu są zagrożeniem, które wywiera najbardziej destrukcyjny i najpoważniejszy wpływ na działanie organizacji. Ataki z wykorzystaniem oprogramowania ransomware obserwowane przez nasz zespół najczęściej są wymierzone w podmioty działające komercyjnie oraz w instytucje publiczne. Atakującymi są grupy przestępcze motywowane finansowo, które starają się zaszyfrować jak najwięcej systemów informatycznych zaatakowanego podmiotu i celują przede wszystkim w dane krytyczne dla ciągłości działania. Zwyczajowo podczas tych ataków operatorzy ransomware starają się też zniszczyć kopie zapasowe, by następnie zażądać od ofiar opłacenia okupu w zamian za udostępnienie klucza deszyfrującego pozwalającego na odzyskanie danych objętych atakiem. Wiele grup stosuje też technikę double extortion – przestępcy przed zaszyfrowaniem danych transferują je z zaatakowanej infrastruktury na kontrolowane przez siebie serwery, aby móc później szantażować zaatakowane organizacje groźbą opublikowania wykradzionych informacji lub odsprzedania ich na czarnym rynku.

W 2025 roku zespół CERT Polska odnotował 179 ataków ransomware, co stanowi znaczący wzrost w stosunku do roku 2024 (147 incydentów) i przewyższa nawet dotychczasowy rekord z 2023 roku (161 incydentów). W 2025 roku dominowały zgłoszenia od podmiotów prywatnych (129), 30 incydentów zostało zgłoszonych przez podmioty publiczne, a 20 zgłoszeń pochodziło od osób fizycznych. Spośród zgłoszeń incydentów w podmiotach publicznych połowa (15 incydentów) dotyczyła zdarzeń w administracji

publicznej na poziomie samorządowym. Drugim najczęstszym sektorem pozostawał sektor oświaty (w tym uczelnie wyższe). Żaden z zarejestrowanych incydentów nie spełniał progów zakwalifikowania go jako incydentu poważnego w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.

WYKRES 1. Liczba ataków ransomware w podziale na miesiące i typ podmiotu



Główne zagrożenia

Pomimo dużego zróżnicowania krajobrazu zagrożeń związanych ze szkodliwym oprogramowaniem typu ransomware podobnie jak w poprzednich latach kilka rodzin obserwowanych było szczególnie często.

TABELA 1. Liczba zarejestrowanych incydentów w podziale na najczęściej obserwowane rodziny ransomware

Rodziny ransomware	Liczba zarejestrowanych incydentów
Qilin	13
Proxima	8
Makop	8
LockBit	8
Beast	7
RansomHub	6
Nieznany	46*

* W 33 przypadkach nie mieliśmy żadnych informacji pozwalających na podjęcie próby identyfikacji użytego ransomware.

Qilin

Ransomware z rodziny Qilin jest udostępniane w modelu Ransomware-as-a-Service (RaaS) – ataki są przeprowadzane przez podwykonawców, którzy wykorzystują szkodliwy kod i infrastrukturę dostarczaną przez twórców ransomware, a w zamian dzielą się z nimi okupem wyłudzonym od ofiary. Grupa Qilin wypełniła lukę na rynku RaaS powstałą w wyniku skutecznych działań organów ścigania wymierzonych w największe grupy ransomware (operacje Cronos[1] i Endgame[2]), które skutkowały rozbiciem lub rozwiązaniem istotnych grup przestępczych działających w tym obszarze. W 2025 roku odnotowaliśmy 13 ataków związanych z użyciem szkodliwego oprogramowania z tej rodziny. Ataki te były wymierzone głównie w średnie i duże przedsiębiorstwa. Niemal w połowie przypadków typowanym wektorem ataku były przejęte dane dostępowe do VPN umożliwiające zdalny dostęp do infrastruktury ofiary. Grupa Qilin prowadzi tzw. leak site, czyli blog, na którym publikuje informacje o zaatakowanych podmiotach oraz wykradzione materiały. Informacja o większości zgłoszonych do nas incydentów nie została jednak zamieszczona na blogu grupy. Należy też podkreślić, że nie każda publikacja informacji o ataku ma ciąg dalszy w postaci ujawnienia materiałów. Jednocześnie grupa czasami nie publikuje przykładowych plików, mimo że analiza po incydencie wykazała transfer danych poza infrastrukturę zaatakowanego podmiotu.

1 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

2 https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame

LockBit

W 2025 roku zespół CERT Polska odnotował 8 ataków z użyciem ransomware z rodziny LockBit, podobnie jak Qilin działającego w modelu RaaS. Przez ostatnie lata grupa LockBit pozostawała liderem w zakresie aktywności i liczby zaatakowanych podmiotów, jednak dzięki działaniom organów ścigania w 2024 roku skalę jej aktywności udało się znacząco zredukować. W maju 2025 roku strona grupy została zaatakowana i podmieniona. Opublikowano wówczas bazę danych zawierającą między innymi portfele kryptowalutowe wykorzystywane przez klientów grupy oraz zapisy konwersacji z ofiarami. Grupa wciąż jednak pozostaje aktywna – we wrześniu 2025 roku zapowiedziała wydanie kolejnej wersji szkodliwego oprogramowania oznaczonej jako LockBit5.0. Należy podkreślić, że z uwagi na wyciek części narzędzi do budowania plików wykonywalnych LockBit3.0 nie wszystkie ataki z wykorzystaniem tej rodziny są realizowane przez operatorów powiązanych z twórcami tego szkodliwego oprogramowania. W 2025 roku grupa LockBit opublikowała na swoim blogu tylko jeden atak dotyczący polskiego podmiotu.

Beast

Beast to kolejna rodzina ransomware funkcjonująca w modelu RaaS. W 2025 roku zespół CERT Polska odnotował 7 incydentów związanych z atakami z wykorzystaniem tego szkodliwego oprogramowania. W trzech przypadkach potwierdzonym wektorem ataku była usługa pulpitu zdalnego RDP (Remote Desktop Protocol), natomiast w jednym przypadku wektora nie udało się potwierdzić, zaatakowany podmiot udostępniał jednak taką usługę. Grupa prowadzi tzw. leak site, jednak w 2025 roku nie opublikowała na nim żadnej informacji dotyczącej ataków na podmioty z Polski.

Makop i Proxima

Makop jest odmianą ransomware wywodzącą się ze szkodliwego oprogramowania Phobos, która funkcjonuje w modelu RaaS i pozostaje aktywna od 2020 roku. W 2025 roku odnotowaliśmy 8 incydentów przypisywanych tej rodzinie. Z kolei ransomware Proxima (znane również jako BlackShadow) było aktywne w pierwszym kwartale 2025 roku, kiedy to odnotowaliśmy wszystkie 8 incydentów, z czego 5 przypadło na luty. W większości zgłoszonych incydentów związanych z tymi rodzinami ransomware nie otrzymaliśmy informacji pozwalających na ustalenie wektora ataku (ani nie został on wytypowany przez podmiot zgłaszający). W przypadku ransomware Proxima zaobserwowaliśmy, że aż w pięciu przypadkach zaatakowany podmiot udostępniał zdalny dostęp do wykorzystywanych komputerów poprzez usługę pulpitu zdalnego RDP.

Obserwacje dotyczące zagrożeń ransomware

Niebezpieczne usługi dostępu zdalnego

W znacznej większości zdarzeń – w przypadkach, w których zaatakowane podmioty były w posiadaniu odpowiednich logów pozwalających na ustalenie wektora ataku – doszło do nieuprawnionego dostępu poprzez usługi dostępu zdalnego, które nie były zabezpieczone dwuskładnikowym uwierzytelnieniem. Atakujący mogą pozyskać dane uwierzytelniające na wiele sposobów – poprzez phishing, wyciek z zewnętrznych serwisów, aktywność oprogramowania typu stealer. Mogą też je odgadnąć w wyniku ataku siłowego. Niestety, w przypadku wielu incydentów zgłaszanych do naszego zespołu ustalenie wektora ataku było niemożliwe. Na szczególną uwagę zasługuje fakt, że w 46 incydentach związanych z atakami ransomware zgłoszonych do zespołu CERT Polska zaatakowany podmiot posiadał publicznie dostępną usługę pulpitu zdalnego RDP. Liczba ta najpewniej jest zaniżona, ponieważ w wielu zgłoszeniach nie uzyskaliśmy informacji na temat infrastruktury i metod zdalnego dostępu do sieci zaatakowanego podmiotu. W dwóch incydentach zgłoszonych do naszego zespołu przełamanie hasła oraz infekcja ransomware nastąpiły w czasie krótszym niż 2 tygodnie od wystawienia usługi RDP do internetu. Wskazuje to, jak krytyczne dla bezpieczeństwa jest wdrożenie dwuskładnikowego uwierzytelnienia we wszystkich usługach umożliwiających zdalny dostęp do infrastruktury.

Ataki

Znaczącym wyzwaniem w analizie incydentów ransomware pozostaje niedostateczna retencja logów, zwłaszcza z urządzeń brzegowych oraz kontrolera domeny Active Directory. Wiele zgłoszeń pochodziło od podmiotów, które nie posiadają centralnego kolektora logów, przez co sięgają one zaledwie kilku dni wstecz. W wielu przypadkach logi z incydentów analizowanych przez nasz zespół jednoznacznie wskazywały, że infiltracja infrastruktury zaatakowanego podmiotu była prowadzona przez operatora ransomware, a nie w sposób całkowicie automatyczny. Takie ataki bardzo często były rozłożone w czasie (nawet na kilka tygodni), a priorytetem w nich było nie tylko zdobycie najwyższych możliwych uprawnień, lecz także zlokalizowanie serwerów kopii zapasowych oraz wirtualizatorów. W przypadku kopii zapasowych przechowywanych na serwerach typu NAS atakujący zazwyczaj ich nie szyfrowali, a po prostu reinicjalizowali przestrzeń dyskową, dążąc do wymazania znajdujących się tam danych. W przypadku przejętych wirtualizatorów atakujący zazwyczaj szyfrowali pliki maszyn wirtualnych oraz usuwali utworzone migawki, a czasami także zmieniali hasła do kont administracyjnych. Operatorzy ransomware bardzo często posługiwali się legalnymi narzędziami i programami wbudowanymi w system operacyjny (tzw. living off the land), a szkodliwe oprogramowanie było wgrywane dopiero po wyłączeniu mechanizmów bezpieczeństwa.

Trudności z identyfikacją atakującego

Szybkie ustalenie grupy odpowiedzialnej za atak oraz znajomość wykorzystywanych przez nią technik znacznie ułatwiają typowanie potencjalnego wektora ataku, ocenę ryzyka eksfiltracji danych czy wiarygodności gróźb pozostawionych w notce wzywającej do opłacenia okupu. Tymczasem w 2025 roku, podobnie jak w roku 2024, w wielu przypadkach rozpoznanie wykorzystanej rodziny ransomware stanowiło duże wyzwanie. Ze względu na presję organów ścigania część grup przestępczych rezygnuje z rozgłosu, aby uniknąć w ten sposób uwagi ze strony podmiotów i instytucji zajmujących się cyberbezpieczeństwem. Tego typu atakujący nie zamieszczają charakterystycznych elementów w pozostawianych notkach wzywających do opłacenia okupu, nie podpisują się w nich, często nie prowadzą też publicznie dostępnych blogów, na których publikowaliby informacje o nowych ofiarach. Sytuację komplikują również wycieki kodu źródłowego niektórych rodzin ransomware oraz wykorzystywanie fragmentów lub całych notek pochodzących z innych rodzin szkodliwego oprogramowania. Widzieliśmy też sytuacje, gdzie w trakcie jednego ataku wykorzystano kilka różnych rodzin ransomware. Wszystkie wymienione czynniki stanowią utrudnienie nie tylko dla osób odpowiedzialnych za reagowanie na incydenty i analizę powłamaniową, lecz także dla zaatakowanego podmiotu – w sytuacji, gdy nie posiada on kopii zapasowej danych objętych atakiem i jest zmuszony do oczekiwania na pojawienie się publicznego dekryptora.

Fałszywe podwójne wymuszenie

Technika podwójnego wymuszenia (ang. double extortion) i transfer danych poza organizację przed rozpoczęciem szyfrowania pozostaje standardem w krajobrazie zagrożeń ransomware. Niektóre grupy ransomware deklarują wręcz, że nie będą stosować szyfrowania, tylko ograniczą się wyłącznie do kradzieży danych (była to oficjalna przyczyna zawieszenia działalności i rebrandingu grupy RansomHub w pierwszym kwartale 2025 roku). Zdecydowana większość notek pozostawianych przez oprogramowanie szyfrujące zawiera groźbę publikacji wykradzionych danych, nawet jeśli do eksfiltracji w rzeczywistości nie doszło. W celu wywarcia dodatkowej presji atakujący mogą podawać fałszywe informacje o tym, że rzekoma infiltracja infrastruktury trwała od miesięcy. W 2025 roku do CERT Polska zostały zgłoszone pojedyncze incydenty, w których notka pozostawiona przez atakujących nie była stworzona na podstawie ogólnego szablonu, lecz faktycznie została przygotowana pod konkretną ofiarę i na podstawie informacji zdobytych w trakcie włamania. Generyczna treść pozostawionej notki nie oznacza jednak, że do eksfiltracji nie doszło. Należy też liczyć się z tym, że od momentu ataku do ujawnienia zdarzenia przez atakujących może minąć wiele miesięcy. Nie ma też reguły odnośnie do informacji publikowanych przez atakujących – np. wylistowanie plików rzekomo będących w posiadaniu atakującego nie musi oznaczać, że faktycznie zostały one wykradzione.

Obserwowane działania grup APT

W 2025 roku CERT Polska zaobserwował intensyfikację działań grup APT, wiązanych z obcymi państwami. Ataki były skierowane przeciwko polskim podmiotom publicznym, firmom prywatnym, ale także w znacznym stopniu były one nastawione na pozyskiwanie informacji od osób fizycznych, które mogą lub mogły w przeszłości pełnić funkcje publiczne, są zaangażowane w życie polityczne lub prowadzą badania naukowe. Warto również odnotować wzrost liczby przypadków wykorzystania motywów politycznych przez atakujących do osiągania swoich celów, takich jak wyłudzanie informacji czy polaryzacja społeczeństwa. Po raz pierwszy w historii CERT Polska zaobserwował również skoordynowane ataki na sektor energii w Polsce, które miały na celu działanie destrukcyjne.

Przypadki opisane w raporcie stanowią wyłącznie fragment działalności grup APT monitorowanej przez CERT Polska i nie odzwierciedlają w pełni skali znanych ataków tych grup na polskie instytucje.

Wszystkie incydenty opisane w tym rozdziale wiązane są przez CERT Polska z aktywnością grup APT, w części przypadków szczegółowa lub jednoznaczna atrybucja nie została jednak przedstawiona, co wynika z ograniczeń dostępnych danych lub decyzji wewnętrznych.

Wybrane kampanie oraz incydenty

Aktywność grupy UNC1151/Ghostwriter

W 2025 roku grupa UNC1151, podobnie jak w latach ubiegłych, pozostawała jednym z najbardziej aktywnych spośród klastrów aktywności przypisywanych przez CERT Polska do grup APT. Według publikacji firmy Google[3] grupa UNC1151 z dużym prawdopodobieństwem powiązana jest z rządem Białorusi, ale według innych źródeł ma również związek z rosyjskimi służbami specjalnymi[4]. Działania tej grupy były bardzo różnorodne. Starała się ona dynamicznie zmieniać stosowane techniki zarówno w przypadku ataków phishingowych, ataków z użyciem szkodliwego oprogramowania, jak i wtedy gdy wykorzystywała podatności[5] w oprogramowaniu czy angażowała się w działania dezinformacyjne mające na celu polaryzację polskiego społeczeństwa m.in. w trakcie kampanii wyborczej przed wyborami prezydenckimi. Ze względu na różnorodność przeprowadzonych kampanii przez grupę UNC1151 opisaliśmy je poniżej w punktach A–D.

3 https://blog.google/threat-analysis-group/update-threat-landscape-ukraine

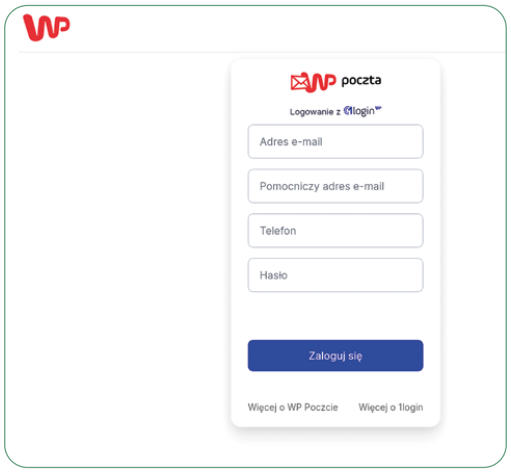
4 https://www.gov.pl/web/sluzby-specjalne/ustalenia-abw-i-skw-dot-atakow-hakerskich

5 https://cert.pl/posts/2025/06/unc1151-kampania-roundcube/

A. KAMPANIE PHISHINGOWE NA SERWISY POCZTOWE

Grupa UNC1151 już od kilku lat koncentruje się na uzyskiwaniu dostępu do skrzynek pocztowych polskich obywateli[6], by następnie przeprowadzić eksfiltrację wiadomości, które mogą zawierać cenne informacje lub które mogą być wykorzystane w celach propagandowych. Ataki te charakteryzują się dużą różnorodnością, a także częstymi zmianami stosowanych technik. Obserwowane przez nas kampanie były prowadzone przez wiele tygodni regularnie od poniedziałku do piątku, a celami były setki osób, których skrzynki mailowe znajdowały się w serwisach Interia, Onet oraz Wirtualna Polska.

RYSUNEK 22. Przykładowy panel phishingowy wykorzystywany przez grupę UNC1151



Warta podkreślenia jest również kwestia wykorzystywanych domen w kampaniach phishingowych. Na początku roku grupa wykorzystywała rejestrowane przez siebie domeny do hostowania paneli phishingowych imitujących strony logowania do serwisów pocztowych. W kolejnych kwartałach aktor zaczął wykorzystywać w tym celu przejęte strony internetowe należące zazwyczaj do polskich podmiotów.

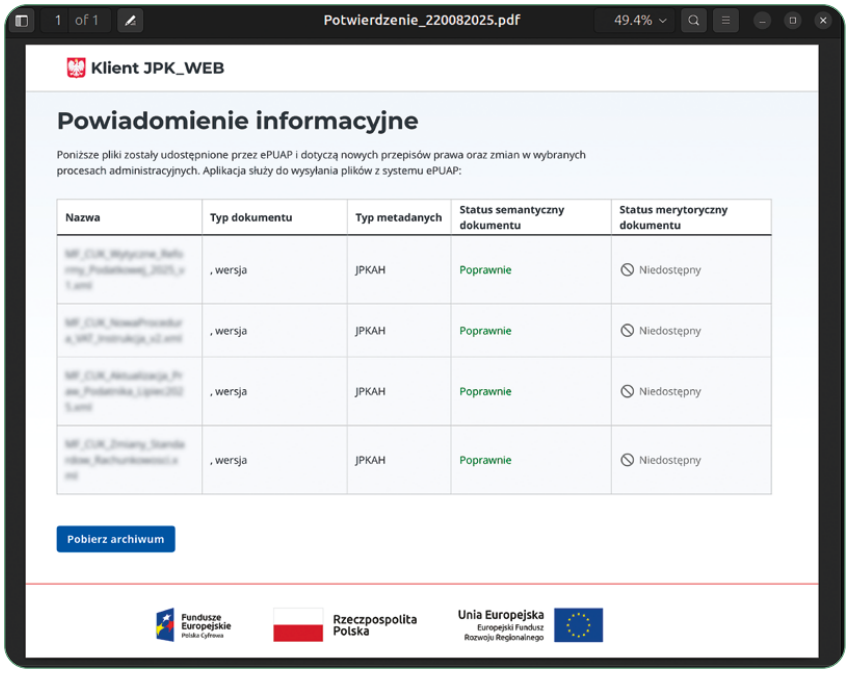
B. DYSTRYBUCJA SZKODLIWEGO OPROGRAMOWANIA

Grupa UNC1151 oprócz przeprowadzania kampanii phishingowych na serwisy pocztowe w 2025 roku intensywnie starała się dystrybuować szkodliwe oprogramowanie, co miało na celu uzyskanie zdalnego dostępu do komputerów ofiar oraz kradzież danych uwierzytelniających do różnych serwisów zewnętrznych i zasobów wewnętrznych.

Atakujący regularnie zmieniają techniki oraz typy plików, w których ukrywają szkodliwe oprogramowanie. W ubiegłym roku najczęściej jako pierwszy etap infekcji wykorzystywane były pliki CHM, czyli Microsoft Compiled HTML Help file, a także pliki XLS z makrami i pliki prezentacji PPT. Jako socjotechniczną przynętę grupa stosowała motywy podjętych uchwał na uczelniach, windykacji, płatności składki członkowskiej partii politycznej, ale także tematykę związaną z rolnictwem i terenami wiejskimi.

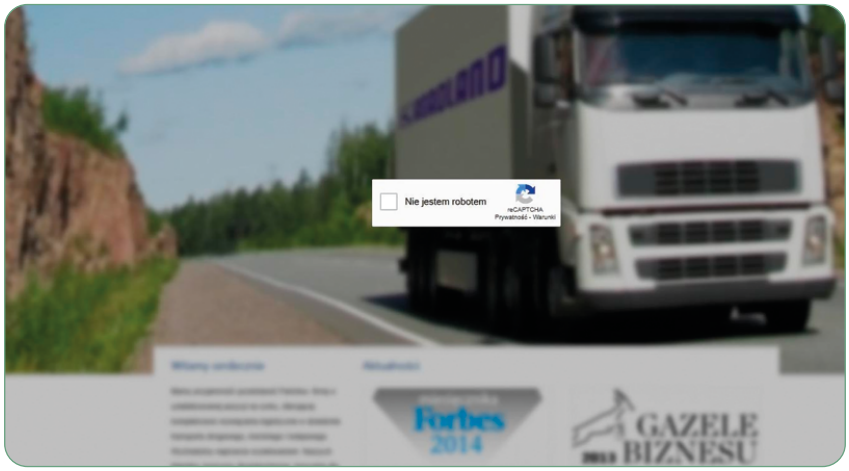
6 https://cert.pl/posts/2022/07/techniki-unc1151/

RYSUNEK 23. Przykład wabika zastosowanego przez grupę UNC1151 w celu dystrybucji szkodliwego oprogramowania

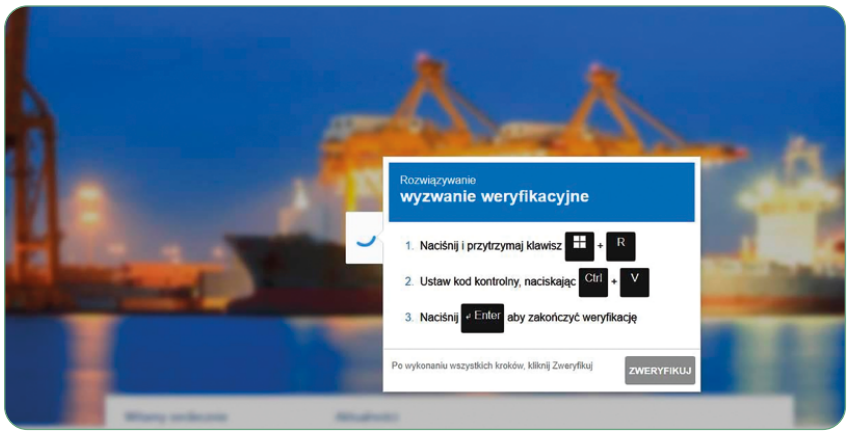


Oprócz wykorzystywania motywu rolnictwa grupa w trakcie roku prowadziła kampanię wymierzoną wprost w sektor rolnictwa. Wykorzystano w tym celu mechanizm fałszywej Captchy (tzw. ClickFix) umieszczanej na popularnych stronach związanych z rolnictwem, do których wcześniej grupa uzyskała dostęp. Nieświadomy użytkownik po odwiedzeniu zainfekowanej strony proszony był o przeklejenie zawartości schowka do okna dialogowego „Uruchamianie” w systemie Windows, aby rzekomo zweryfikować, czy nie jest robotem. W rzeczywistości na jego komputer było pobierane szkodliwe oprogramowanie, którego celem była eksfiltracja danych.

RYSUNEK 24. Fałszywa weryfikacja użytkownika



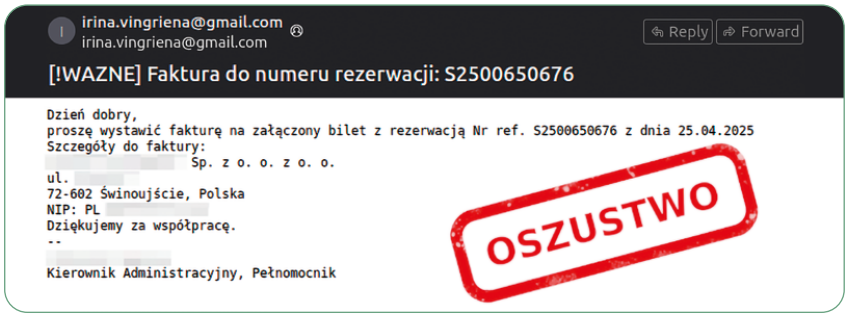
RYSUNEK 25. Fałszywa CAPTCHA zastosowana przez grupę UNC1151



C. WYKORZYSTANIE PODATNOŚCI W OPROGRAMOWANIU ROUNDCUBE

Grupa UNC1151 w ubiegłym roku przeprowadziła wielokrotnie kampanie wykorzystujące podatność CVE-2024-42009 w celu kradzieży poświadczeń. Podatność ta umożliwia wykonanie kodu JavaScript w momencie odczytania spreparowanego e-maila. Atakujący rozsyłali e-maile z tytułami mającymi nakłonić odbiorcę do zapoznania się z treścią wiadomości i podjęcia szybkiego działania.

RYSUNEK 26. Przykładowa wiadomość wykorzystująca CVE-2024-42009, dystrybuowana przez grupę UNC1151



Kiedy nieświadoma ofiara otwierała e-maila, na niezaktualizowanym przez administratora systemie dochodziło do wykorzystania podatności, która instalowała tzw. Service Workera w przeglądarce użytkownika. W dalszej kolejności użytkownik był przenoszony na stronę logowania do poczty, a Service Worker przechwytywał wszystkie próby zalogowania do aplikacji Roundcube i przesyłał kopię danych logowania na serwer atakującego. Więcej szczegółów technicznych ataku zostało opisanych w artykule „Kampania UNC1151 wykorzystująca podatność w oprogramowaniu Roundcube do kradzieży poświadczeń”[7].

7 https://cert.pl/posts/2025/06/unc1151-kampania-roundcube/

Grupa UNC1151 tak pozyskane dostępy do skrzynek pocztowych wykorzystywała na dwa sposoby. Jeśli zawartość skrzynki w ocenie atakujących była ciekawa ze względu na znajdujące się tam wiadomości i zawarte w nich informacje, wykorzystywali ją do dalszego ich pozyskiwania, w przeciwnym wypadku grupa dystrybuowała ze skrzynki kolejne wiadomości do innych instytucji oraz firm, które mogły wykorzystywać podatną wersję oprogramowania Roundcube. Atakujący wielokrotnie wykorzystywali prawdziwe wiadomości, które znaleźli na przejętych kontach pocztowych, do których dołączali exploit, a następnie dystrybuowali do nowych celów. Ten zabieg miał na celu uwiarygodnić kontakt.

Warto odnotować, że w 2025 roku podatność CVE-2024-42009 w kampaniach wymierzonych w polskie podmioty wykorzystywała również grupa APT28.

D. DEZINFORMACJA WYBORCZA

W marcu 2025 roku CSIRT NASK zaobserwował aktywność grupy UNC1151 w związku ze zbliżającymi się wówczas wyborami prezydenckimi. Kampanie te wykorzystywały m.in. wizerunek fundacji Ukraiński Dom oraz kandydatów biorących udział w wyborach. Ataki miały na celu m.in. pogłębianie polaryzacji polskiego społeczeństwa, ale również wzbudzanie niechęci do mniejszości ukraińskiej w Polsce.

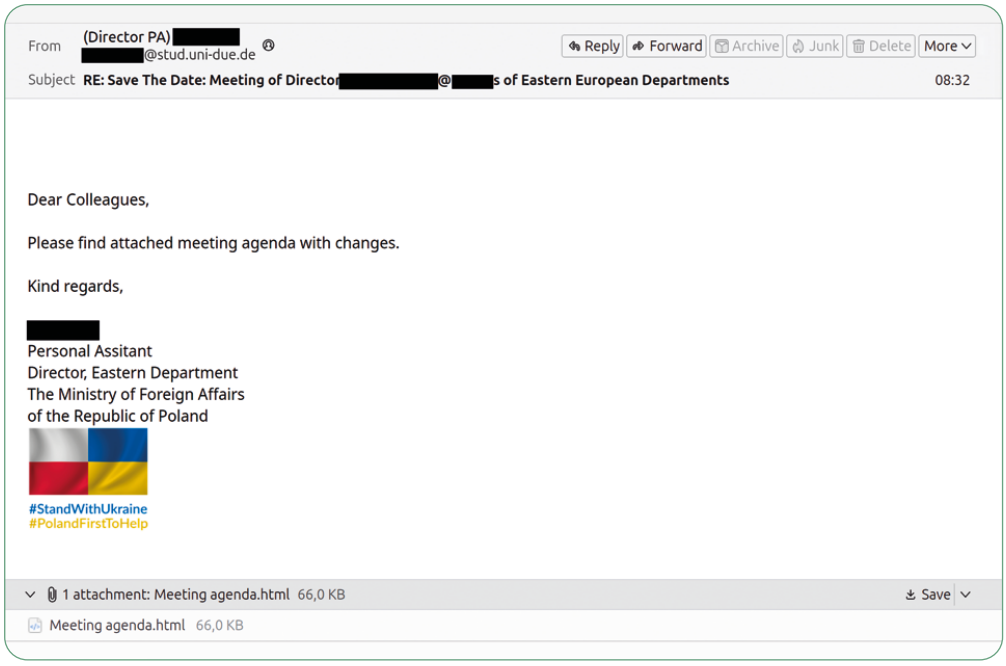
Materiały tworzone przez grupę były promowane m.in. w kampaniach reklamowych w serwisach YouTube oraz TikTok, ale również zamieszczano je w opisach aukcji w serwisie OLX, na którym grupa prowadziła fałszywą sprzedaż gadżetów z wulgarnymi treściami.

CSIRT NASK współpracował z Pionem Ochrony Informacyjnej Cyberprzestrzeni NASK–PIB w kontekście monitorowania tych kampanii.

Device Code Phishing

W lutym ubiegłego roku CSIRT NASK otrzymał informację w ramach europejskiej Sieci CSIRT o kampanii, w której przestępcy podszywali się pod pracownika polskiego Ministerstwa Spraw Zagranicznych. Atakujący za pomocą wiadomości e-mail dystrybuowali szkodliwy załącznik, do którego uwiarygodnienia wykorzystali prawdziwą wiadomość z zaproszeniem związanym z polską prezydencją w Radzie Unii Europejskiej. Wiadomość ta została najprawdopodobniej pozyskana przez atakujących ze skompromitowanego konta pocztowego jednego z jej odbiorców. Celem było uzyskanie dostępu do zasobów Microsoft 365 należących do pracowników europejskich ambasad.

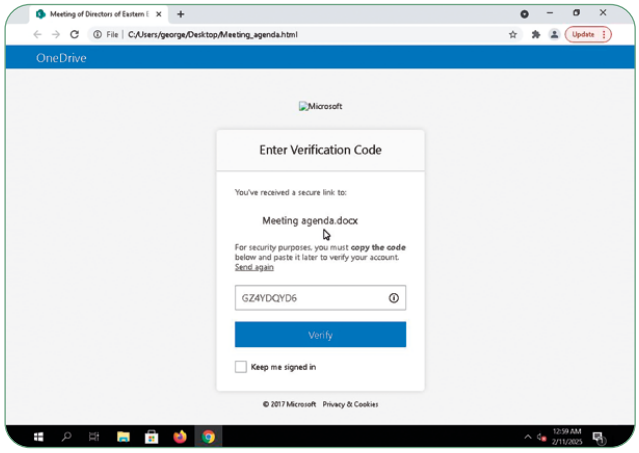
RYSUNEK 27. Treść wiadomości e-mail dystrybuowanej do pracowników europejskich ambasad



Atakujący próbowali wykorzystać mechanizm alternatywnego logowania do usług Microsoft poprzez plik HTML, który pobierał z serwera atakujących wygenerowany przez nich Device Code. W dalszej kolejności użytkownik proszony był o skopiowanie kodu, który miał wkleić na zalogowanym koncie na stronie Microsoft, co nadawałoby dostęp atakującemu do konta ofiary, jej danych oraz wszystkich zasobów i usług w tenancie organizacji.

W kolejnych tygodniach lutego CSIRT NASK śledził kolejne odsłony kampanii, w których atakujący wykorzystywali inne motywy – zaproszenie od polskiego ambasadora na wideorozmowę, wspólne oświadczenie osób popierających Aleksieja Nawalnego, wideokonferencje przedstawicieli zagranicznych agencji rządowych oraz think tanków.

RYSUNEK 28. Plik HTML z ataku Device Code Phishing



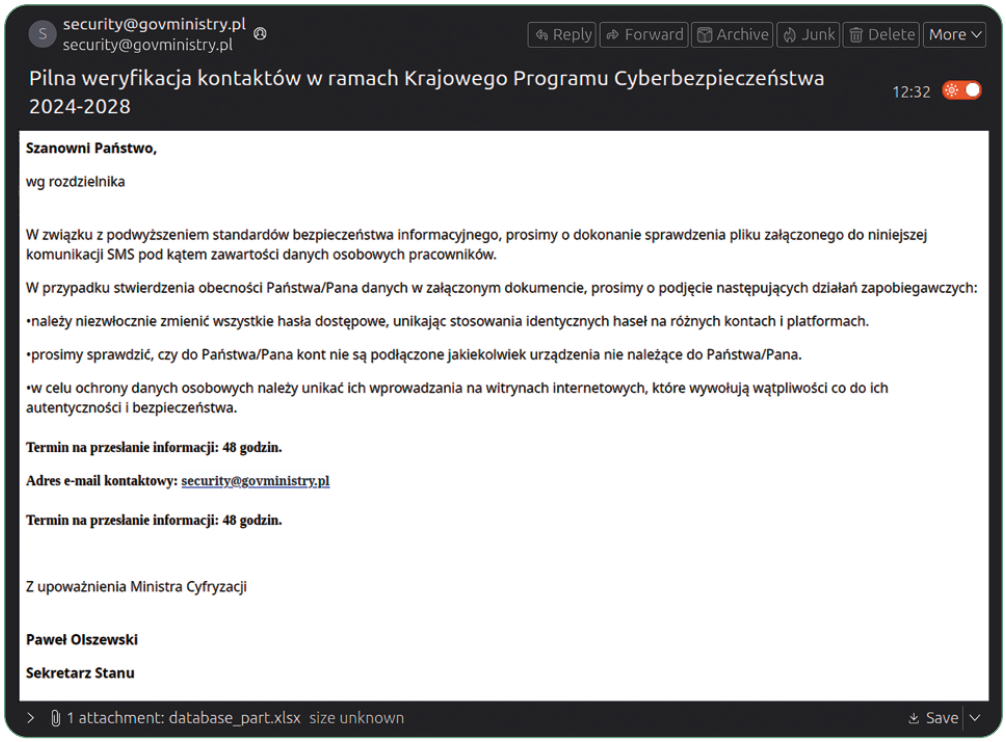
Polska Agencja Kosmiczna

Pod koniec lutego 2025 roku CERT Polska uzyskał informację o podejrzanej aktywności w infrastrukturze Polskiej Agencji Kosmicznej. W toku prowadzonej analizy potwierdzono obecność atakującego i wykryto pozostawione mechanizmy persystencji. Atakujący zarejestrował własne aplikacje w tenancie Microsoft Azure, z którymi komunikował się poprzez Graph API w celu eksfiltracji danych. Analiza incydentu oraz działania w tej sprawie były prowadzone wspólnie z zespołem CSIRT MON.

Wyłudzanie informacji o pracownikach krajowego systemu cyberbezpieczeństwa

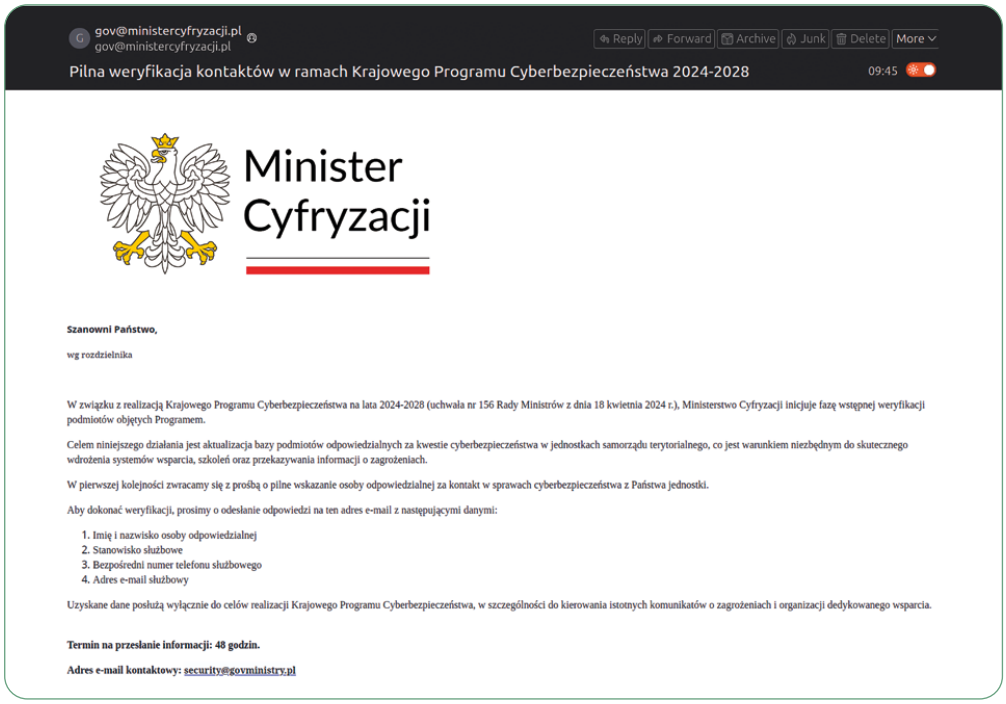
Pod koniec października 2025 roku CSIRT NASK po raz pierwszy zaobserwował kampanię, w której atakujący podszywali się pod Ministerstwo Cyfryzacji i wiceministra Pawła Olszewskiego. Celem tej kampanii były jednostki samorządu terytorialnego. Atakujący przygotowali 2 warianty kampanii dystrybuowane za pomocą wiadomości e-mail z domeny govministry[.]pl. W pierwszym wariancie do wiadomości załączany był plik arkusza kalkulacyjnego XLSX, który linkował do strony, na której rzekomo znajdował się drugi dokument z kompletem informacji. W rzeczywistości był to silnie zaciemniony plik wykonywalny, będący szkodliwym oprogramowaniem.

RYSUNEK 29. Zawartość wiadomości, w której atakujący podszywali się pod wiceministra cyfryzacji Pawła Olszewskiego



W drugim wariancie kampanii atakujący, wykorzystując elementy socjotechniki, próbowali nakłonić odbiorców wiadomości do przekazania szczegółowych informacji na temat osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w danych jednostkach samorządu terytorialnego, w tym imion, nazwisk, numerów telefonów oraz adresów mailowych. W przypadku skutecznego wyłudzenia tych danych atakujący najpewniej próbowaliby przeprowadzić ataki kierunkowe na te konkretne osoby. CSIRT NASK podjął działania mające na celu ostrzeżenie wszystkich polskich gmin o trwającej kampanii.

RYSUNEK 30. Treść wiadomości wyłudzającej informacje o pracownikach JST



Skoordynowane ataki na sektor energii

Pod koniec grudnia 2025 roku doszło po raz pierwszy w historii Polski do skoordynowanych, ukierunkowanych i mających charakter sabotażu ataków na podmioty z sektora energii. Przeprowadzona analiza wykazała, że odpowiedzialny jest za nie klaster aktywności znany w przestrzeni publicznej jako „Static Tundra" (Cisco), „Berserk Bear" (CrowdStrike), „Ghost Blizzard" (Microsoft) oraz „Dragonfly" (Symantec). Działania były wymierzone w co najmniej 30 farm wiatrowych i fotowoltaicznych, spółkę prywatną z sektora produkcyjnego oraz w dużą elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców w Polsce.

Zdarzenia te miały wpływ zarówno na systemy informatyczne, jak i na fizyczne urządzenia przemysłowe, co jest rzadko spotykane w dotychczas opisywanych atakach. Warto podkreślić, że był to okres, kiedy Polska zmagała się z niskimi temperaturami i zamieciami śnieżnymi.

Natomiast należy zaznaczyć, że ataki nie wpłynęły na bieżącą produkcję energii elektrycznej ani na dostawy ciepła.

CERT Polska od początku wykrycia incydentów uczestniczył w ich obsłudze oraz wspierał podmioty w analizie śledczej, w wyniku której opublikowany został raport, aby przekazać wiedzę o przebiegu zdarzenia oraz o technikach stosowanych przez atakującego. Raport jest dostępny na stronie internetowej cert.pl[8].

Najważniejsze podatności

W 2024 roku zintensyfikowaliśmy działania mające na celu skuteczne docieranie do podmiotów, które korzystają z oprogramowania zawierającego podatności stanowiące w naszej ocenie duże ryzyko. W związku z tym, że starania te przyniosły wymierne skutki, kontynuowaliśmy je w 2025 roku.

W dalszym ciągu monitorowaliśmy na bieżąco nowe informacje, aby zidentyfikować podatności, których wykorzystanie w atakach przez przestępców mogło stanowić duże ryzyko dla polskich podmiotów. Następnie przeprowadzaliśmy działania mające na celu zidentyfikowanie właścicieli instancji dostępnych z internetu. Wyniki skanowań związanych z podatnościami, które uznaliśmy za najistotniejsze w 2025 roku, przedstawiliśmy w tabeli 2. Nie wszystkie skanowania były wykonywane przez nasz zespół – w części przypadków informacja pochodziła od partnerów.

Sposób działania zespołu w zakresie wysyłania powiadomień uległ jednak pewnym zmianom. Nowym źródłem informacji o właścicielach urządzeń jest darmowy serwis moje.cert.pl, w którym administratorzy mogą podać domeny i zakresy sieciowe, którymi zarządzają. Dzięki temu, że przekazują oni swoje dane kontaktowe, zespół CERT Polska zyskuje możliwość znacznie szybszego i skuteczniejszego dotarcia z najważniejszymi informacjami dotyczącymi luk bezpieczeństwa.

Nowością są również ostrzeżenia publikowane w serwisie moje.cert.pl. W przypadku podatności stanowiących duże ryzyko równolegle do komunikatów mailowych kierowanych do konkretnych podmiotów publikujemy także ostrzeżenia w tym serwisie. Na ten krok decydowaliśmy się również wtedy, gdy zidentyfikowanie podatnych instancji oraz ich właścicieli okazywało się problematyczne. Więcej informacji o tym, w jaki sposób można śledzić wydawane komunikaty, znajduje się w rozdziale „Moje.cert.pl” (→ s. 106–107).

8 https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/

TABELA 2. Liczba instancji oprogramowania podatnych lub dostępnych z internetu w momencie wysłania powiadomień przez zespół CERT Polska

Produkt	Status	Liczba instancji
React Server Components	podatne	1943
PAD CMS	podatne	961
Cisco Secure Firewall ASA/FTD	podatne	427
FortiOS / FortiProxy (CVE-2024-55591, CVE-2025-24472)	podatne	240
Ivanti Connect Secure	podatne	120
NetBird VPN	podatne	40
Citrix NetScaler ADC/Gateway	podatne	17
Omnissa Workspace ONE UEM	podatne	15
Ivanti EPMM	podatne	4
SonicWall SonicOS	publicznie dostępne	440
FortiOS z włączonym SSO (CVE-2025-59718, CVE-2025-59719)	publicznie dostępne	326
Microsoft SharePoint Server	publicznie dostępne	50
Ingress-NGINX	publicznie dostępne	11
Cisco Secure Email Gateway	publicznie dostępne	4
Fortinet FortiWeb Manager	publicznie dostępne	2

Roundcube (CVE-2024-42009, CVE-2025-49113)

DATA PUBLIKACJI PODATNOŚCI: 05.08.2024, 02.06.2025

Roundcube to popularny klient poczty elektronicznej działający w przeglądarce, szeroko wykorzystywany przez wiele polskich podmiotów, w tym również przez największe hostingi. Zespół CERT Polska obserwował wykorzystanie krytycznej podatności XSS (CVE-2024-42009) do ataków pozwalających na przejmowanie poświadczeń do skrzynek.

Podatność CVE-2024-42009 polega na błędzie sanityzacji HTML umożliwiającym wykonanie kodu JavaScript w kontekście użytkownika odczytującego spreparowaną wiadomość e-mail. Atakujący mogli modyfikować interfejs klienta pocztowego, wprowadzać w błąd użytkownika lub przejmować dane uwierzytelniania, co prowadziło do pełnego dostępu do konta. CVE-2025-49113 to luka deserializacji PHP w pliku upload.php,

pozwalająca uwierzytelnionemu użytkownikowi na zdalne wykonanie kodu na serwerze Roundcube poprzez niezabezpieczony parametr _from. Połączenie tej podatności z poświadczeniami pozyskanymi w wyniku ataku XSS mogło pozwalać zdalnym atakującym na przejmowanie serwerów pocztowych.

CERT Polska wykrył kampanię UNC1151 wymierzoną w polskie podmioty, w której przejęte skrzynki wykorzystywano do dalszej dystrybucji exploitów XSS. Atakujący instalowali Service Workery jako mechanizm persystencji do przechwytywania poświadczeń. Skala ataków była wysoka, ponieważ Roundcube jest stosowany nie tylko przez pojedyncze organizacje, lecz także przez największe polskie hostingi, a więc narażeni byli ich wszyscy klienci. Więcej informacji o tych podatnościach zawarliśmy w artykule pt. „Kampania UNC1151 wykorzystująca podatność w oprogramowaniu Roundcube do kradzieży poświadczeń”[9].

Precyzyjne określenie liczby podatnych instancji okazało się niewykonalne z powodu backportingu (aktualizacje bez zmiany wersji) oraz ukrywania Roundcube za VPN-ami, co z kolei sprawiło, że nie było możliwości ani skanowania, ani kontaktu z administratorami. CERT Polska publikował ostrzeżenia dla użytkowników, w tym poprzez serwis moje.cert.pl[10] oraz wspierał podmioty dotknięte atakami.

Ivanti Connect Secure / Policy Secure / ZTA Gateway (CVE-2025-0282, CVE-2025-0283, CVE-2025-22457)

DATA PUBLIKACJI PODATNOŚCI: 08.01.2025, 03.04.2025

Ivanti Connect Secure, Policy Secure oraz ZTA Gateway to rozwiązania VPN i kontroli dostępu wykorzystywane w sieciach korporacyjnych.

Obserwowaliśmy wykorzystanie podatności CVE-2025-0282 oraz CVE-2025-0283, które umożliwiały zdalne wykonanie kodu bez uwierzytelnienia oraz eskalację uprawnień po uzyskaniu początkowego dostępu. Luki były aktywnie wykorzystywane jako zero-day na kilka tygodni przed publikacją informacji przez Ivanti. Firma Mandiant[11] potwierdziła, że chińska grupa UNC5221 stosowała je od połowy grudnia 2024 roku, a na przejętych urządzeniach dezaktywowała SELinux i syslog oraz pozostawiała skrypty (webshelle) do zapewnienia sobie trwałego dostępu oraz kradzieży poświadczeń. CERT Polska otrzymał informacje o wykorzystaniu tych podatności w kilku polskich podmiotach.

9 https://cert.pl/posts/2025/06/unc1151-kampania-roundcube

10 https://moje.cert.pl/komunikaty/2025/4/krytyczna-podatnosc-w-oprogramowaniu-roundcube

11 https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

W tych urządzeniach została również zidentyfikowana krytyczna podatność CVE-2025-22457 polegająca na przepełnieniu bufora stosu i pozwalająca zdalnym, nieuwierzytelnionym atakującym na wykonanie dowolnego kodu i pełne przejęcie kontroli nad urządzeniem. Mandiant[12] ponownie potwierdził aktywną eksploatację tej luki przez grupę podejrzewaną o powiązania z Chinami. Podatność była wykorzystywana jeszcze przed publicznym ujawnieniem, co również klasyfikuje ją jako zero-day.

Zespół CERT Polska przeskanował polski internet, zidentyfikował 120 podatnych urządzeń Ivanti Connect Secure i niezwłocznie powiadomił ich administratorów o konieczności wdrożenia aktualizacji oraz przeglądu urządzeń pod kątem infekcji.

SonicWall SonicOS (CVE-2024-53704)

DATA PUBLIKACJI PODATNOŚCI: 09.01.2025

SonicOS to system operacyjny urządzeń sieciowych firmy SonicWall. Zidentyfikowano w nich podatność w mechanizmie uwierzytelniania SSL VPN, która pozwala atakującym na ominięcie uwierzytelniania i przechwycenie sesji ostatnio zalogowanego użytkownika.

Wykorzystanie luki umożliwia dostęp do prywatnych sieci użytkownika, odczyt zakładek Virtual Office, pobieranie konfiguracji NetExtender oraz otwarcie tunelu VPN z uprawnieniami ofiary[13]. Po tym, jak w internecie ukazała się publikacja o podatności, pojawił się również skrypt wykorzystujący tę lukę, a sama podatność była aktywnie wykorzystywana w atakach.

Po opublikowaniu informacji o podatności zespół CERT Polska zidentyfikował ponad 440 urządzeń SonicWall w polskim internecie. Administratorzy zostali niezwłocznie powiadomieni o zagrożeniu.

FortiOS / FortiProxy (CVE-2024-55591, CVE-2025-24472)

DATA PUBLIKACJI PODATNOŚCI: 14.01.2025, 11.02.2025

W FortiOS oraz FortiProxy zostały zidentyfikowane krytyczne podatności pozwalające na ominięcie uwierzytelniania. Umożliwia to zdalnemu atakującemu

12 https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

13 https://bishopfox.com/blog/sonicwall-cve-2024-53704-ssl-vpn-session-hijacking

uzyskanie uprawnień administratora poprzez wysłanie odpowiednio spreparowanego żądania do modułu Node.js websocket lub proxy CSF.

Luki były aktywnie wykorzystywane tygodnie przed publikacją informacji o podatności. Arctic Wolf[14] powiązał z tą podatnością trwającą kampanię ataków, w której atakujący tworzyli konta administracyjne i modyfikowali konfiguracje VPN. Zespół CERT Polska również obserwował wykorzystanie podatności w Polsce.

W styczniu 2025 roku zidentyfikowaliśmy 240 podatnych urządzeń i powiadomiliśmy ich administratorów. Od tego czasu stale monitorujemy sytuację i informujemy o niezaktualizowanych instancjach. Na koniec grudnia 2025 roku pozostało 35 podatnych urządzeń.

Ingress NGINX Controller for Kubernetes (CVE-2025-1097, CVE-2025-1098, CVE-2025-24513, CVE-2025-24514, CVE-2025-1974)

DATA PUBLIKACJI PODATNOŚCI: 24.03.2025

Ingress NGINX Controller for Kubernetes (krótka nazwa: Ingress-NGINX) to domyślny kontroler ruchu sieciowego w klastrach Kubernetes, oferujący funkcje reverse-proxy oraz load balancingu. W wersjach do 1.12.0 i 1.11.4 włącznie wykryto krytyczne podatności umożliwiające zdalne wykonanie kodu bez uwierzytelnienia poprzez wykorzystanie webhooka wystawianego domyślnie przez tę usługę.

Usługa webhooka jest wystawiona na porcie TCP 8443 i z reguły jest osiągalna dla wszystkich podów w klastrze, co pozwala atakującemu, który posiada sieciowy dostęp, na wykonanie dowolnego kodu za pomocą spreparowanego żądania HTTP. Skutkiem wykorzystania podatności może być nieautoryzowany dostęp do danych przechowywanych we wszystkich przestrzeniach nazw klastra Kubernetes, prowadzący do pełnego przejęcia kontroli nad środowiskiem.

Zespół CERT Polska zidentyfikował 11 publicznie dostępnych instancji Ingress-NGINX w polskiej adresacji. Administratorzy tych urządzeń zostali powiadomieni o zagrożeniu i zaleceniach aktualizacji kontrolera do wersji eliminujących podatności, a na stronie internetowej CERT Polska ukazał się artykuł pt. „Krytyczne podatności w kontrolerze Ingress-Nginx w Kubernetes”[15], w którym dokładnie opisaliśmy wskazane zagrożenie.

14 https://arcticwolf.com/resources/blog/cve-2024-55591

15 https://cert.pl/posts/2025/03/krytyczne-podatnosci-w-kontrolerze-ingress-nginx-kubernetes

Ivanti Endpoint Manager Mobile (CVE-2025-4427, CVE-2025-4428)

DATA PUBLIKACJI PODATNOŚCI: 13.05.2025

Ivanti Endpoint Manager Mobile (EPMM) to system zarządzania urządzeniami w środowiskach korporacyjnych. Podatność CVE-2025-4427 umożliwia ominięcie mechanizmu uwierzytelniania w komponencie API, pozwalając atakującemu na dostęp do chronionych zasobów. CVE-2025-4428 to luka pozwalająca na zdalne wykonanie kodu w tym samym komponencie API, umożliwiająca uwierzytelnionemu atakującemu wykonanie dowolnego kodu za pomocą spreparowanych żądań.

Wykorzystanie obydwu podatności pozwala na nieuwierzytelnione zdalne wykonanie kodu oraz dostęp do danych o pracownikach i urządzeniach zarządzanych przez EPMM, w tym pozyskanie wrażliwych informacji o konfiguracjach oraz potencjalną eskalację ataków wewnątrz sieci. Ivanti potwierdziło wykrycie rzeczywistych ataków z wykorzystaniem tego łańcucha jeszcze przed oficjalną publikacją informacji o podatnościach, co oznacza, że luki funkcjonowały jako zero-day w środowiskach produkcyjnych części klientów[16].

CERT Polska zidentyfikował w maju 4 podatne instancje EPMM dostępne z internetu i od tego czasu ich administratorzy byli okresowo powiadamiani o problemie. Do grudnia 2025 roku liczba podatnych urządzeń Ivanti EPMM spadła do zera.

Citrix NetScaler ADC/Gateway (CVE-2025-6543)

DATA PUBLIKACJI PODATNOŚCI: 25.06.2025

NetScaler ADC i NetScaler Gateway to urządzenia sieciowe wykorzystywane do równoważenia obciążenia oraz realizacji zdalnego dostępu VPN. Podatność CVE-2025-6543 została oficjalnie opisana przez producenta jako podatność typu denial of service związana z przepełnieniem pamięci w instancjach skonfigurowanych jako brama zdalnego dostępu. W praktyce okazało się jednak, że ten sam mechanizm może zostać wykorzystany do zdalnego wykonania kodu i do pełnego przejęcia podatnych urządzeń[17].

Jeszcze przed publikacją poprawek obserwowano na świecie przypadki przejmowania urządzeń NetScaler, w których atakujący umieszczali szkodliwe skrypty (webshelle) lub inne trwałe mechanizmy dostępu, a skutki infekcji

16 https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

17 https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-netscaler-adc-and-netscaler-gateway

były trudne do jednoznacznego wykrycia bez ukierunkowanych działań typu threat hunting. CERT Polska otrzymywał od partnerów informacje o wykorzystaniu CVE-2025-6543 do kompromitacji urządzeń, co potwierdzało, że luka ma w praktyce charakter podatności pozwalającej na zdalne wykonanie kodu.

Po tym, jak opublikowano informację o podatności, zidentyfikowaliśmy kilkanaście publicznie dostępnych i podatnych instancji NetScaler ADC/Gateway. Jak najszybciej kontaktowaliśmy się z ich administratorami, aby zarekomendować wdrożenie aktualizacji bezpieczeństwa oraz przegląd logów pod kątem potencjalnego przejęcia urządzeń. Kontakt ten odbywał się mailowo, natomiast opublikowaliśmy także komunikat w serwisie moje.cert.pl[18]. Równolegle prowadziliśmy aktywne skanowanie instancji Citrix w poszukiwaniu pozostawianych znanych skryptów (webshelli) i innych śladów ataku. Nie potwierdzono jednak żadnej skutecznej infekcji w polskich organizacjach.

Sudo (CVE-2025-32463)

DATA PUBLIKACJI PODATNOŚCI: 30.06.2025

Sudo jest narzędziem do kontroli uprawnień w systemach Unix/Linux umożliwiającym wykonywanie wybranych poleceń z uprawnieniami administratora. Wykryta w nim podatność CVE-2025-32463 pozwala na lokalną eskalację uprawnień i powiązana jest z obsługą opcji chroot. Luka umożliwia uruchomienie dowolnych poleceń z poziomu użytkownika root, nawet jeśli użytkownik nie jest zdefiniowany w pliku sudoers. W konsekwencji atakujący, który posiada dostęp do systemu jako zwykły użytkownik, może przejąć pełną kontrolę nad systemem operacyjnym.

Luka wynika z nieprawidłowego wykorzystania pliku konfiguracyjnego nsswitch.conf z katalogu kontrolowanego przez użytkownika podczas wykonywania sudo z opcją chroot, co pozwala na załadowanie złośliwych bibliotek i eskalację uprawnień. Szczególnie istotne jest to, że podatność może być wykorzystywana również przy domyślnej konfiguracji sudo, bez dodatkowych modyfikacji po stronie administratora, co znacząco zwiększa ryzyko ataku. Podatność dotyczyła najnowszych w tamtym czasie wersji popularnych dystrybucji Linuxa, takich jak Ubuntu, Fedora czy Red Hat Enterprise Linux.

Ze względu na charakter podatności zdecydowaliśmy się na publikację ostrzeżenia dla administratorów za pośrednictwem serwisu moje.cert.pl[19] jako najbardziej efektywnego kanału komunikacji w sytuacji, gdy nie ma możliwości bezpośredniego powiązania podatności z konkretnymi, publicznie dostępnymi usługami.

18 https://moje.cert.pl/komunikaty/2025/17/aktywnie-wykorzystywane-krytyczne-podatnosci-narzedzia-citrix-netscaler

19 https://moje.cert.pl/komunikaty/2025/11/krytyczna-podatnosc-narzedzia-sudo-w-wersji-do-1917-wacznie

Microsoft SharePoint Server (CVE-2025-53770)

DATA PUBLIKACJI PODATNOŚCI: 19.07.2025

Microsoft SharePoint Server jest systemem zarządzania treścią, który może być zainstalowany lokalnie w infrastrukturze organizacji. Podatność oznaczona jako CVE-2025-53770 dotyczy wyłącznie instalacji on-premise i wynika z deserializacji niezaufanych danych, co pozwala nieautoryzowanym atakującym na zdalne wykonanie kodu poprzez specjalnie spreparowane żądania HTTP. Mechanizm wykorzystuje m.in. manipulację ViewState i ASP.NET MachineKey, umożliwiając przejęcie pełnej kontroli nad serwerem, w tym dostęp do danych i zasobów organizacji.

Informacja o luce została opublikowana w lipcu 2025 roku, a Microsoft początkowo nie wydał łatki, co znacząco utrudniało szybkie zabezpieczenie infrastruktury i zwiększało ryzyko udanych ataków. Obserwowano działania podejmowane przez aktorów państwowych, w tym przez chińskie grupy, co podkreśla poziom ryzyka powiązany z tą podatnością[20].

Zespół CERT Polska odnotował próby wykorzystania tej podatności w organizacjach zlokalizowanych w Polsce. Przeprowadzone skanowania wykazały 50 publicznie dostępnych instancji SharePoint Server w polskim internecie. Ich administratorzy zostali powiadomieni o zagrożeniu.

Omnissa Workspace ONE UEM (CVE-2025-25231)

DATA PUBLIKACJI PODATNOŚCI: 11.08.2025

Omnissa Workspace ONE UEM (dawniej VMware AirWatch) to system MDM służący do zarządzania urządzeniami mobilnymi w środowiskach korporacyjnych. Odkryto w nim podatność typu path traversal, która w wersji on-premise umożliwia atakującemu odczyt dowolnych plików z dysku serwera bez uwierzytelnienia.

Luka była aktywnie wykorzystywana w atakach wycelowanych w polskie podmioty do wykradania wrażliwych informacji, w tym danych o pracownikach. Na początku września otrzymaliśmy informację o 15 podatnych instancjach dostępnych z internetu i niezwłocznie powiadomiliśmy administratorów o zagrożeniu oraz o konieczności aktualizacji oprogramowania. W serwisie moje.cert.pl opublikowaliśmy także komunikat dla administratorów[21].

20 https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities

21 https://moje.cert.pl/komunikaty/2025/29/aktywnie-wykorzystywana-krytyczna-podatnosc-w-narzedziu-omnissa-workspace-one-uem-airwatch-mdm

Cisco Secure Firewall ASA/FTD (CVE-2025-20333, CVE-2025-20362, CVE-2025-20363)

DATA PUBLIKACJI PODATNOŚCI: 25.09.2025

Cisco Secure Firewall ASA (Adaptive Security Appliance) i FTD (Firewall Threat Defense) są urządzeniami sieciowymi typu firewall. Opublikowano 3 podatności dotyczące tych narzędzi, z czego 2 oceniono jako krytyczne (CVE-2025-20333 oraz CVE-2025-20362), wynikające z nieprawidłowej obsługi zapytań HTTP do komponentu WebVPN.

Luki umożliwiają nieuwierzytelnionemu atakującemu dostęp do zasobów sieciowych bez uwierzytelnienia oraz zdalne wykonanie kodu z uprawnieniami konta root, co prowadzi do pełnego przejęcia urządzenia. Obserwowaliśmy aktywne wykorzystywanie tych podatności w atakach na polskie podmioty.

Zidentyfikowaliśmy 427 podatnych urządzeń, powiadomiliśmy bezpośrednio ich administratorów oraz opublikowaliśmy komunikat z ostrzeżeniem w serwisie moje.cert.pl[22]. Ze względu na wysokie ryzyko oraz występowanie instancji w wersjach niewspieranych już przez producenta Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał rekomendację dotyczącą bezzwłocznej aktualizacji produktów Cisco ASA/Cisco Firepower lub ich wyłączenia[23].

PAD CMS (CVE-2025-7063, CVE-2025-7065, CVE-2025-8117, CVE-2025-8120, CVE-2025-8121, CVE-2025-8122)

DATA PUBLIKACJI PODATNOŚCI: 30.09.2025

PAD CMS to oprogramowanie do zarządzania treścią wykorzystywane głównie w podmiotach publicznych do prowadzenia stron Biuletynu Informacji Publicznej. CERT Polska koordynował proces ujawniania serii krytycznych podatności, w tym kilku zidentyfikowanych w ramach badań własnych[24].

Najpoważniejsze z luk umożliwiały nieuwierzytelnionemu atakującemu umieszczenie własnego skryptu na stronie, co mogło prowadzić do zdalnego wykonania kodu i pełnego przejęcia serwera.

22 https://moje.cert.pl/komunikaty/2025/36/aktywnie-wykorzystywane-krytyczne-podatnosci-w-urzadzeniach-cisco-asa-i-cisco-firepower

23 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-aktualizacji-produktow-cisco

24 https://cert.pl/posts/2025/09/CVE-2025-7063

Zidentyfikowaliśmy 961 podatnych instancji PAD CMS w polskim internecie, głównie w urzędach gmin, bibliotekach i szkołach.

Ze względu na powszechność wykorzystania w sektorze publicznym oraz brak szans na wydanie aktualizacji przez producenta z powodu zakończenia okresu wsparcia CERT Polska powiadomił wszystkich administratorów o konieczności zmiany oprogramowania, a Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał rekomendację z zaleceniem natychmiastowego wyłączenia z użytku oprogramowania PAD CMS[25].

Oracle E-Business Suite (CVE-2025-61882)

DATA PUBLIKACJI PODATNOŚCI: 05.10.2025

Oracle E-Business Suite to zintegrowany system ERP służący do zarządzania przedsiębiorstwem. Odkryta w nim krytyczna podatność CVE-2025-61882 w komponencie BI Publisher Integration umożliwia zdalne wykonanie kodu bez uwierzytelnienia przez atakującego posiadającego dostęp sieciowy.

Luka była wykorzystywana jako zero-day tygodnie przed publikacją aktualizacji bezpieczeństwa przez Oracle. Firmy CrowdStrike i Google potwierdziły wykorzystywanie podatności przez grupę CL0P w celu wykradania danych z organizacji. Pierwsze ślady ataków datowane były od sierpnia 2025 roku[26].

Mimo niskiej skali wykorzystania Oracle EBS w Polsce CERT Polska otrzymał zgłoszenie incydentu, w którym wykorzystano tę lukę. Łatwość eksploatacji oraz wysoki wpływ na organizacje, w tym możliwość wycieku wrażliwych danych biznesowych, plasują tę podatność wysoko w klasyfikacji ryzyka.

NetBird VPN (CVE-2025-10678)

DATA PUBLIKACJI PODATNOŚCI: 20.10.2025

NetBird jest platformą VPN opartą na protokole WireGuard. CERT Polska otrzymał zgłoszenie podatności związanej z domyślnymi poświadczeniami konta administratora utworzonego przez ZITADEL – domyślnego dostawcę tożsamości w rozwiązaniu NetBird. Skrypt instalacyjny producenta nie usuwał ani nie zmieniał domyślnego hasła, co umożliwiało zdalny dostęp administracyjny do panelu zarządzania VPN.

25 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-zaprzestanie-korzystania-z-oprogramowania-pad-cms

26 https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882

W rezultacie do wielu urządzeń można było zalogować się powszechnie znanymi domyślnymi danymi uwierzytelniającymi, co dawało pełną kontrolę nad infrastrukturą sieciową. CERT Polska przypisał tej podatności numer CVE i koordynował z producentem proces odpowiedzialnego ujawnienia informacji[27].

Zespół CERT Polska zidentyfikował ponad 40 instancji NetBird w polskim internecie z aktywnym domyślnym kontem administratora. Wszyscy administratorzy zostali powiadomieni o zagrożeniu na miesiąc przed publikacją podatności.

Fortinet FortiWeb Manager (CVE-2025-64446)

DATA PUBLIKACJI PODATNOŚCI: 14.11.2025

FortiWeb Manager to komponent systemu FortiWeb, webowego firewalla aplikacyjnego służącego do ochrony aplikacji internetowych przed atakami. Umożliwia centralne zarządzanie konfiguracją i politykami bezpieczeństwa dla instancji FortiWeb.

Wykryta w nim podatność oznaczona jako CVE-2025-64446 wynika z błędu path traversal umożliwiającego nieuwierzytelnionemu atakującemu wykonanie poleceń administracyjnych poprzez spreparowane żądania HTTP lub HTTPS skierowane do panelu GUI. Atak polega na wysłaniu żądania POST z payloadem tworzącym nowe konto administratora do specjalnej ścieżki, co daje atakującym pełną kontrolę nad urządzeniem. Podatność była aktywnie wykorzystywana przed oficjalną publikacją informacji przez Fortinet w listopadzie 2025 roku, a pierwsze próby eksploatacji pojawiły się w październiku 2025[28].

W Polsce skanowania przeprowadzone przez zespół CERT Polska wykazały tylko kilka publicznie dostępnych instancji FortiWeb Manager. Mimo małej skali taka podatność stanowi poważne zagrożenie szczególnie dla urządzeń umieszczonych w sieciach wewnętrznych o płaskiej topologii, gdzie niezaufani użytkownicy mogą mieć dostęp do panelu. Administratorzy zidentyfikowanych instancji zostali powiadomieni o ryzyku i zaleceniach dotyczących wyłączenia dostępu HTTP/HTTPS do panelu zarządzania do czasu aktualizacji, a w serwisie moje.cert.pl ukazał się komunikat o tym zagrożeniu[29].

27 https://cert.pl/posts/2025/10/CVE-2025-10678

28 https://arcticwolf.com/resources/blog/cve-2025-64446

29 https://moje.cert.pl/komunikaty/2025/57/aktywnie-wykorzystywana-krytyczna-podatnosc-w-urzadzeniach-fortinet-fortiweb-manager

React Server Components (CVE-2025-55182)

DATA PUBLIKACJI PODATNOŚCI: 03.12.2025

Wykryta podatność CVE-2025-55182 umożliwia zdalne wykonanie kodu w React Server Components (RSC) oraz innych aplikacjach korzystających z RSC, np. Next.js.

Wykorzystanie polega na wysłaniu spreparowanego żądania HTTP, które powoduje wykonanie dowolnego kodu na serwerze przed jakąkolwiek weryfikacją uwierzytelnienia. Publicznie dostępne opisy oraz kod PoC znacząco zwiększyły ryzyko masowych ataków na aplikacje RSC. Firma Mandiant[30] odnotowała wykorzystanie tej podatności przez liczne grupy, głównie powiązane z Chinami, które instalowały mechanizmy persystencji na przejętych serwerach.

Od pierwszego dnia po publikacji skanowaliśmy polski internet w poszukiwaniu podatnych stron. Zidentyfikowaliśmy blisko 2 tys. instancji umożliwiających zdalne wykonanie kodu i powiadomiliśmy administratorów. Mimo braku zgłoszeń incydentów dotyczących wykorzystania tej podatności w Polsce popularność tego rozwiązania wskazuje na wysokie ryzyko, dlatego wydaliśmy również komunikat w serwisie moje.cert.pl[31].

FortiOS / FortiProxy / FortiWeb / FortiSwitchManager (CVE-2025-59718, CVE-2025-59719)

DATA PUBLIKACJI PODATNOŚCI: 09.12.2025

FortiOS, FortiProxy, FortiWeb i FortiSwitchManager to produkty firmy Fortinet służące do zabezpieczania sieci oraz do zarządzania urządzeniami. Zidentyfikowano w nich podatności polegające na nieprawidłowej weryfikacji podpisu kryptograficznego. Luki umożliwiają nieuwierzytelnionemu atakującemu ominięcie uwierzytelniania FortiCloud SSO poprzez spreparowaną wiadomość SAML.

Luki dotyczą urządzeń z włączoną funkcją FortiCloud SSO, która aktywuje się automatycznie po rejestracji w FortiCare z poziomu GUI, chyba że administrator odznaczy odpowiednią opcję. Wykorzystanie podatności prowadzi do nieautoryzowanego dostępu administracyjnego. Arctic Wolf wkrótce po publikacji odnotował ataki wykorzystujące powyższe podatności[32].

30 https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182

31 https://moje.cert.pl/komunikaty/2025/61/krytyczna-podatnosc-w-react-server-components-oraz-innych-aplikacjach-z-tym-rozwiazaniem

32 https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-sso-logins-following-disclosure-cve-2025-59718-cve-2025-59719

Przeprowadziliśmy skanowanie polskiego internetu w poszukiwaniu produktów Fortinet FortiOS z włączonym logowaniem SSO. Zidentyfikowaliśmy 326 takich urządzeń, a ich administratorzy zostali poinformowani o zagrożeniu i zaleceniach wyłączenia funkcji lub aktualizacji zarówno mailowo, jak i za pośrednictwem komunikatu w serwisie moje.cert.pl[33].

Cisco Secure Email Gateway oraz Secure Email and Web Manager (CVE-2025-20393)

DATA PUBLIKACJI PODATNOŚCI: 17.12.2025

Firma Cisco oferuje rozwiązania Secure Email Gateway (dawniej IronPort) oraz Secure Email and Web Manager służące do ochrony poczty elektronicznej przed zagrożeniami. Oparte są one na systemie AsyncOS, w którym wykryto krytyczną podatność pozwalającą nieuwierzytelnionemu atakującemu na zdalne wykonanie dowolnego kodu z uprawnieniami konta root. Luka ta jest związana z niewłaściwą walidacją danych wejściowych w usłudze Spam Quarantine. Choć usługa domyślnie jest wyłączona i zgodnie z dobrymi praktykami nie powinna być dostępna z poziomu internetu, jej niewłaściwa konfiguracja otwiera drogę do całkowitego przejęcia urządzenia bez konieczności posiadania jakichkolwiek poświadczeń.

Podatność ta była aktywnie wykorzystywana w cyberatakach na długo przed opublikowaniem oficjalnych poprawek bezpieczeństwa. Według analizy Cisco Talos[34] za kampanią stoi chińska grupa szpiegowska śledzona jako UAT-9686 (wykazująca powiązania z grupami APT41 oraz UNC5174). Po przełamaniu zabezpieczeń atakujący instalowali na urządzeniach szkodliwe oprogramowanie, w tym backdoora AquaShell zapewniającego trwały dostęp, oraz narzędzia takie jak AquaTunnel czy Chisel do tunelowania ruchu i dalszej eksploracji sieci ofiary.

Zidentyfikowaliśmy w polskim internecie kilka urządzeń z niewłaściwie skonfigurowaną usługą Spam Quarantine wystawioną na świat. Właściciele tych instancji zostali niezwłocznie powiadomieni o krytycznym zagrożeniu. Należy jednak podkreślić, że ze względu na specyfikę usługi Spam Quarantine, która często funkcjonuje jedynie wewnątrz sieci organizacji, skanowanie zewnętrzne nie pozwala na wykrycie wszystkich zagrożonych podmiotów. Z tego powodu opublikowaliśmy komunikat dla administratorów na platformie moje.cert.pl[35], aby ostrzec przed ryzykiem wykorzystania tej luki do eskalacji uprawnień wewnątrz sieci korporacyjnych.

33 https://moje.cert.pl/komunikaty/2025/64/podatnosci-w-oprogramowaniu-fortios-fortiproxy-forti web-i-fortiswitchmanager

34 https://blog.talosintelligence.com/uat-9686

35 https://moje.cert.pl/komunikaty/2025/65/krytyczna-podatnosc-cve-2025-20393-w-oprogramo waniu-cisco-asyncos-software

Wycieki danych

W roku 2025 CERT Polska kontynuował działania operacyjne oraz współpracę z organami państwa na rzecz ujawniania informacji o wyciekach danych zawierających rekordy dotyczące obywateli Polski. Kluczowym działaniem w celu efektywnego przeciwdziałania skutkom takich zdarzeń jest proaktywne monitorowanie cyberprzestrzeni. Prowadzimy obserwację stron, na których przestępcy umieszczają dane pozyskane od ofiar ataków, forów w sieci TOR, kanałów komunikacyjnych używanych przez przestępców, a także gromadzimy i analizujemy informacje uzyskane za pomocą narzędzi od dostawców zewnętrznych. Każdorazowo przy wykryciu podejrzenia wycieku danych kontaktujemy się z dotkniętym podmiotem, aby ustalić źródło i zakres wycieku oraz aby pomóc w mitygacji skutków zdarzenia.

Bezpiecznedane.gov.pl

Niezmiennie od 2023 roku CERT Polska zasila serwis bezpiecznedane.gov.pl danymi z ujawnionych wycieków, aby polscy użytkownicy internetu mogli zweryfikować, czy i w jakim zakresie ich dane mogły zostać naruszone.

Z uwagi na krajowy charakter serwisu zawiera on często dane wykraczające poza te dostępne na innych, podobnych, międzynarodowych platformach. W niektórych przypadkach za sprawą współpracy z firmami i instytucjami, które padły ofiarą wycieków, CERT Polska jest w stanie umieścić w serwisie nie tylko te dane, które zostały upublicznione przez przestępców, lecz także kompletne zbiory wykradzionych danych. Dzięki temu obywatele potencjalnie dotknięci atakiem mogą uzyskać stosowną informację bez względu na to, czy ich dane pojawiły się w udostępnionej przez przestępców próbce, czy też nie.

Unikalną dla serwisu funkcjonalnością jest umożliwienie użytkownikom w przypadku niektórych wycieków sprawdzenia za pomocą numeru PESEL, czy ich dane mogły zostać ujawnione. W 2025 roku umieściliśmy w serwisie informacje o 10 wyciekach. Poniżej przedstawiamy te wycieki, które miały miejsce w 2025 roku.

Zbiór danych logowania opublikowany na forum dla przestępców

Na początku lutego 2025 roku na jednym z forów dla przestępców została opublikowana lista danych złożona z 11 mln par zawierających e-mail i hasło. Analiza CERT Polska wykazała, że znaczna część to rekordy historyczne, pojawiające się już we wcześniejszych wyciekach i sięgające nawet 10 lat wstecz.

Babyhit.pl

W marcu 2025 roku na przestępczym forum został opublikowany wyciek danych klientów sklepu babyhit.pl zawierający dane ok. 600 tys. osób. Analiza wykazała, że wyciek obejmuje takie dane, jak imię, nazwisko, adres dostawy, adres e-mail oraz numer telefonu.

Zbiór danych logowania opublikowany w aplikacji Telegram

We wrześniu 2025 roku na jednym z publicznych kanałów aplikacji Telegram pojawiła się lista danych zawierająca ponad 1,8 mln rekordów. I choć analiza CERT Polska wykazała, że w większości są to dane pojawiające się we wcześniejszych wyciekach, natrafiono również na takie, które mogły pochodzić z 2025 roku.

SuperGrosz.pl

W październiku 2025 roku w internecie pojawiła się oferta sprzedaży bazy danych klientów serwisu SuperGrosz.pl, a firma potwierdziła naruszenie bezpieczeństwa informacji. Próbka udostępniona przez przestępców zawierała dane: imię i nazwisko, adres zamieszkania lub pobytu, adres e-mail, numer telefonu, numer PESEL, informacje dotyczące dowodu osobistego oraz dane logowania z hasłami w formie hashy. Skontaktowaliśmy się z firmą, która potwierdziła wyciek i przekazała do serwisu bezpiecznedane.gov.pl bazę danych wszystkich klientów dotkniętych wyciekiem.

Itaka.pl

Również w październiku 2025 roku w sieci opublikowano ofertę sprzedaży bazy danych klientów biura podróży Itaka. Opis oferty mówił o 2,2 mln wpisów, a jako próbkę udostępniono ok. 10 tys. rekordów. Biuro Itaka potwierdziło, że doszło do naruszenia danych części systemu „Strefy Klienta". Wyciek zawierał imiona i nazwiska, adresy e-mail oraz numery telefonów. Firma zaznaczyła przy tym, że nie doszło do wycieku informacji finansowych ani numerów PESEL. Według komunikatów Itaki wyciek dotyczył co najmniej 10 tys. osób, chociaż firma przyznaje, że skala może być większa. W przeciwieństwie do wycieku z SuperGrosz.pl w tym przypadku w serwisie bezpiecznedane.gov.pl znajdują się jedynie dane upublicznione przez przestępców.

Wkdzik.pl

W grudniu 2025 roku doszło do włamania do systemów obsługujących sklep internetowy wkdzik.pl, w wyniku którego uzyskano dostęp do kilku

baz danych prowadzonych przez firmę. Na podstawie analizy materiału oraz wewnętrznych ustaleń potwierdzono, że zostały wykradzione bazy klientów oraz kontrahentów. Zawierały one imię, nazwisko, adres e-mail, numer telefonu oraz adres dostawy. Baza danych została następnie wystawiona na sprzedaż przez osobę podającą się za atakującego, co zwiększa ryzyko jej dalszego rozpowszechnienia i może oznaczać, że dane te w przyszłości zostaną wykorzystane w próbach wyłudzenia danych wrażliwych. Firma udostępniła dane z baz wykradzionych w wycieku celem zasilenia serwisu bezpiecznedane.gov.pl i umożliwienia użytkownikom weryfikacji, czy zostali dotknięci incydentem.

Abfoto.pl

W grudniu 2025 roku miało miejsce włamanie do systemów obsługujących sklep internetowy abfoto.pl, na skutek którego osoba nieuprawniona uzyskała dostęp do bazy danych klientów sklepu obejmującej takie dane, jak imię i nazwisko, adres e-mail, numer telefonu, adres zamieszkania lub wysyłki, kwotę zamówienia i liczbę zamówień, a także w niektórych wypadkach dane firmy. Z ustaleń wynika, że incydent dotyczył ponad 100 tys. klientów sklepu, a choć baza do tej pory nie została nigdzie opublikowana, firma udostępniła dane do serwisu bezpieczedane.gov.pl.

Zbiór danych logowania do portalu Facebook

Funkcjonariusze Zarządu w Białymstoku Centralnego Biura Zwalczania Cyberprzestępczości w toku prowadzonego śledztwa RSD.27/25 rozbili zorganizowaną grupę przestępczą, która najpierw za pomocą phishingu pozyskiwała dane logowania do kont na Facebooku, a następnie za pośrednictwem komunikatora na platformie wyłudzała kody BLIK od innych użytkowników Facebooka. Od maja 2022 roku do maja 2024 roku zabezpieczono ponad 100 tys. wykradzionych loginów i haseł do platformy. Baza ofiar oszustwa została przekazana do udostępnienia w serwisie bezpiecznedane.gov.pl. Warto podkreślić, że jest to pierwsza tego typu współpraca między instytucjami, dzięki której obywatele w razie upewnienia się, że ich dane logowania zostały przejęte w wyniku działań grupy, mają możliwość skontaktowania się z prowadzącym postępowanie, o czym CBZC informuje w swoim komunikacie umieszczonym w serwisie.

Powiadomienia o wyciekach w ramach moje.cert.pl

Jedną z głównych funkcji systemu moje.cert.pl jest monitorowanie informacji o wyciekach haseł użytkowników w ramach domen firm i instytucji. W przypadku ujawnienia takiego wycieku zarejestrowani administratorzy są o tym niezwłocznie powiadamiani. Więcej informacji o moje.cert.pl znajduje się w części raportu poświęconej naszym projektom (→ s. 106–107).

Rekomendacje po wycieku danych

Niezależnie od źródła i zakresu wycieku wszystkie dane zdobyte przez przestępców mogą posłużyć im do uwiarygodnienia przyszłych ataków socjotechnicznych. Po wycieku może również wzrosnąć liczba otrzymywanych niechcianych wiadomości e-mail, połączeń telefonicznych o charakterze spamu bądź prób oszustwa. Przestępcy mogą też wykorzystywać pozyskane dane w celu uzyskania dostępów do różnych serwisów, dlatego tak ważne jest dokładne czytanie powiadomień bezpieczeństwa otrzymywanych w aplikacji, np. o potwierdzeniu logowania lub autoryzacji przelewu.

Forma mitygacji skutków wycieku będzie zależna od tego, w jaki sposób i jakie dane wyciekły.

W przypadku złośliwego oprogramowania typu infostealer należy:

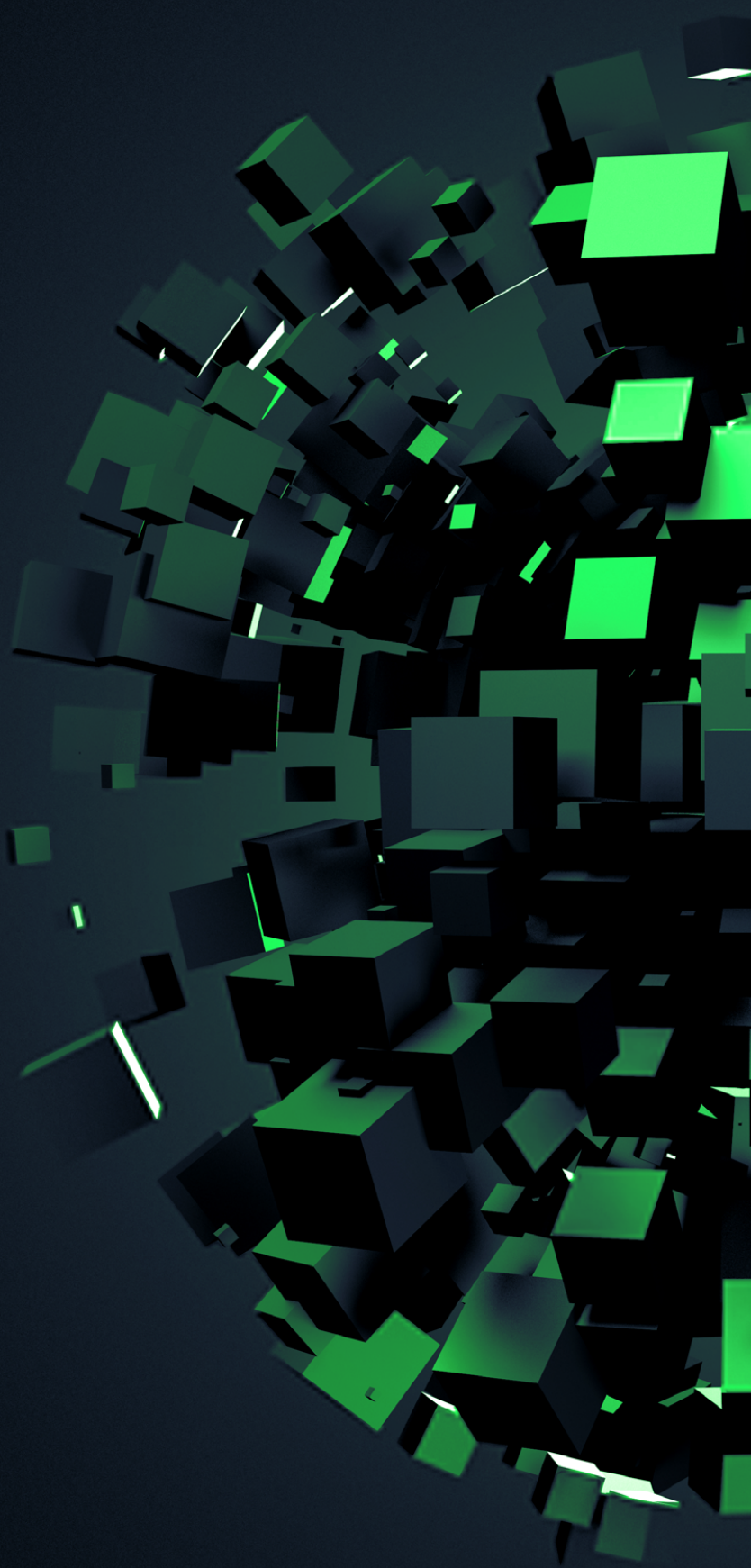
- niezwłocznie zmienić hasła do wszystkich serwisów, do których logowaliśmy się z potencjalnie zainfekowanej maszyny – zmian tych trzeba dokonać z innego systemu, z takiego, co do którego nie podejrzewamy infekcji,
- zmienić hasła wszędzie tam, gdzie były używane te same hasła co w punkcie powyżej,
- przeprowadzić pełną reinstalację systemu operacyjnego na potencjalnie zainfekowanej maszynie.

W przypadku bycia ofiarą phishingu lub wycieku danych z podmiotu zewnętrznego:

- w przypadku wycieku hasła – natychmiastowa zmiana hasła w serwisie i wszędzie tam, gdzie zostało użyte to samo hasło,
- w przypadku wycieku numeru PESEL – zastrzeżenie numeru PESEL, co może pomóc ograniczyć ryzyko nieuprawnionego wykorzystania danych (https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie),
- w przypadku wycieku danych karty debetowej/kredytowej (numer karty i CVV/CVC) – niezwłoczne zastrzeżenie karty oraz kontakt z bankiem,
- w przypadku wycieku informacji o dowodzie osobistym/skanu dowodu osobistego – niezwłoczne zastrzeżenie dokumentu oraz wyrobienie nowego.

Ponadto – niezależnie od tego, czy dane pojawiły się w którymś z wycieków, czy jeszcze nie – rekomendujemy przestrzeganie odpowiedniej higieny haseł oraz stosowanie uwierzytelniania wieloskładnikowego wszędzie tam, gdzie jest to możliwe. Więcej informacji na ten temat znajduje się w naszym poradniku dotyczącym cyberhigieny dostępnym pod adresem https://cert.pl/bezpieczne-hasla.

Działania CERT Polska



Lista Ostrzeżeń

W 2025 roku Lista Ostrzeżeń pobiła kolejny rekord. Setki tysięcy szkodliwych domen blokowanych przez CERT Polska pokazuje, jak ważnym jest ona narzędziem.

Obecnie utrzymywana jest druga wersja Listy Ostrzeżeń. Domeny umieszczane są na niej na okres 6 miesięcy od momentu analizy, a w przypadku dalszego utrzymywania szkodliwych treści domena zostaje ponownie wpisana na Listę. W porównaniu z pierwszą wersją, w której domeny były umieszczane na stałe, takie rozwiązanie pomaga ograniczyć rozmiar pliku, a także koncentruje się na aktualnych zagrożeniach i kampaniach obserwowanych przez nasz zespół. Widzimy, że domeny wykorzystywane są krótko, ale za to na szeroką skalę. Poprawna implementacja Listy Ostrzeżeń pozwala blokować takie zagrożenie w ciągu 5 minut od dodania domen przez nasz zespół.

Informacje o szkodliwych domenach zbierane są za pośrednictwem kilku kanałów, z których jednym z najczęściej wykorzystywanych nadal pozostaje numer 8080. Łatwość zgłoszenia poprzez przekazanie podejrzanego SMS-a na ten numer powoduje, że jest to często wybierana forma przesyłania nam stron do analizy, szczególnie tych, które otrzymali Państwo właśnie w wiadomości SMS. Zgłoszenia dotyczące podejrzanych stron internetowych czy wiadomości e-mail wysyłane są także m.in. za pomocą formularza dostępnego na stronie incydent.cert.pl czy przez aplikację mObywatel w ramach usługi Bezpiecznie w sieci. Na podstawie danych z tych źródeł, danych własnych i przekazanych przez naszych partnerów oraz po naszej analizie na Listę Ostrzeżeń w 2025 roku trafiło prawie 245 tys. domen.

Łatwość korzystania z Listy Ostrzeżeń połączona z jej wysoką skutecznością przyciąga użytkowników. Obserwujemy to na podstawie liczby pobrań, która w 2025 roku wyniosła prawie 1,3 mld, co przełożyło się na zablokowanie ok. 141,1 mln wejść na niebezpieczne strony. Oznacza to wzrost w stosunku do 2024 roku odpowiednio o 273% i 96,5%.

Dziękujemy wszystkim zgłaszającym oraz nieustająco zachęcamy do przesyłania nam podejrzanych linków, domen oraz SMS-ów także w 2026 roku.

Walka z oszustwami SMS

Od lat jednym z najpopularniejszych sposobów dotarcia do potencjalnych ofiar oszustwa są wiadomości SMS. Każdy z nas ma telefon niemal zawsze przy sobie, natychmiast reagujemy na większość powiadomień, zwłaszcza tych z komunikatorów. Większość wejść na strony phishingowe

następuje w ciągu 15 minut od otrzymania wiadomości. Najczęściej w takiej sytuacji nie zwracamy uwagi na to, kto do nas napisał, tylko zaczynamy od sprawdzenia, „co podesłał". Jednocześnie koszt wysłania wiadomości phishingowej jest znikomy – to ok. kilkunastu groszy. Można więc łatwo policzyć, że do „zwrotu z inwestycji" w postaci wysłania 10 000 wiadomości SMS wystarczy oszukać jedną osobę na 1000–2000 zł. Raporty publikowane przez NBP[36] pokazują, że skala strat finansowych jest znacznie większa.

Zgłoszenia wiadomości SMS

Wykorzystywaniu SMS-ów do dystrybucji oszustw przyglądamy się bliżej od przełomu 2020 i 2021 roku. Jednym z narzędzi służących do kontroli tego zjawiska są prowadzone przez nas statystyki, które prezentujemy i opisujemy w raportach rocznych. W kwietniu 2021 roku rozpoczęliśmy przyjmowanie zgłoszeń podejrzanych wiadomości za pośrednictwem kanału zgłoszeniowego. Aby uprościć proces zgłaszania, w listopadzie 2023 roku uruchomiliśmy darmowy numer 8080. Było to możliwe dzięki współpracy z rynkiem telekomunikacyjnym oraz za sprawą wejścia w życie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej[37].

Do tej pory co roku notowaliśmy rekordy liczby zgłoszeń SMS, jednak 2025 rok przyniósł załamanie trendu wzrostowego. Przyjęliśmy 295 169 zgłoszeń podejrzanych wiadomości SMS, co stanowi spadek o 16,8% względem roku poprzedniego (354 566). Jeszcze ciekawiej przedstawia się sytuacja związana z wiadomościami sklasyfikowanymi jako złośliwe. W 2024 roku było ich 140 659, a w 2025 roku wartość ta (81 395) spadła do poziomu porównywalnego z 2022 rokiem (82 319). Ciekawie również wygląda porównanie ostatnich kwartałów minionych lat. Dotychczas wzrastała wówczas liczba oszustw związanych z motywem niedostarczenia przesyłki wykorzystujących okres świątecznych zakupów. W latach 2022–2024 złośliwe wiadomości stanowiły średnio 35,4% wszystkich zgłoszeń z czwartego kwartału, natomiast w 2025 roku ten odsetek wyniósł jedynie 10,3%. Wynika to z wystąpienia czynników, które opisujemy poniżej.

Blokowanie złośliwych SMS-ów

Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej powstała m.in. po to, aby dać instytucjom państwowym narzędzia do walki z tego rodzaju zagrożeniami. Jednym z takich narzędzi jest mechanizm blokowania wiadomości SMS.

36 https://nbp.pl/system-platniczy/dane-i-analizy/transakcje-oszukancze

37 https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm

Na podstawie analizy otrzymywanych zgłoszeń upubliczniamy wyrażenia regularne, które opisują konkretne wiadomości lub całe kampanie SMS. Rejestr jest aktualizowany za pośrednictwem systemu, do którego dostęp mają operatorzy SMS. W ciągu 5 minut od upublicznienia wzorzec zostaje automatycznie pobrany i operator ma obowiązek blokowania każdej wiadomości, która pasuje do tego wzorca. W ramach walki ze smishingiem prowadzimy również wykaz nadpisów SMS zarezerwowanych dla podmiotów publicznych. Instytucja, która zgłosi taki nadpis, uzyskuje do niego pełne prawo, co skutkuje zablokowaniem próby wysłania wiadomości z danym nadpisem przez innego nadawcę. 2025 był pierwszym rokiem, w którym operatorzy telekomunikacyjni blokowali wiadomości przez okres od stycznia do grudnia. Na podstawie przedstawionych wcześniej statystyk dotyczących liczby samych zgłoszeń możemy stwierdzić, że system blokad może mieć wpływ na wykorzystanie SMS-ów do dystrybucji oszustw.

W 2024 roku wytworzyliśmy 746 wzorców, które przełożyły się na 1 475 678 blokad[38]. W 2025 roku 790 wzorców doprowadziło do zablokowania 1 883 610 złośliwych SMS-ów. Ta statystyka ukazuje rosnącą skuteczność systemu – pierwszy rok jego działania przyniósł średnio 1978 zablokowanych prób oszustwa na jeden wzorzec, w minionym roku były to już 2384 udaremnione próby.

Kluczowy w przeciwdziałaniu oszustwom jest czas reakcji. Zlecenia wysłania kilku czy kilkunastu tysięcy wiadomości trwają zazwyczaj do 30–40 minut. Z tego powodu 10 wzorców może doprowadzić do mniejszej liczby blokad niż pojedynczy, stworzony po otrzymaniu zaledwie kilku zgłoszeń. Dlatego też cały czas rozwijamy nasz system analityczny: w 2024 roku każda zgłoszona złośliwa wiadomość przełożyła się średnio na 24 blokady. W 2025 roku udało nam się utrzymać ten współczynnik na poziomie 23 niedostarczonych wiadomości. Ponownie rekordowym miesiącem okazał się listopad – 84 blokady na każde zgłoszenie smishingu.

Kampanie SMS

W 2025 roku obserwowaliśmy postępującą zmianę w scenariuszach oszustw wykorzystujących SMS-y. Przytoczone wcześniej statystyki sugerowały już, że zmniejszyła się popularność historii związanych z paczkami. Dotyczy to całej grupy wiadomości zawierających link do strony phishingowej. Natomiast odnotowujemy coraz większy odsetek oszustw, w których SMS jest jedynie zachętą lub przynętą do nawiązania kontaktu. Taki motyw pojawia się np. w rzekomych wiadomościach od dziecka o uszkodzeniu telefonu lub karty

38 Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

SIM i potrzebie kontaktu poprzez inny komunikator, w fałszywych SMS-ach zawierających informacje o zyskach na naszym koncie walutowym/inwestycyjnym lub powiadomienie o próbie logowania na nasze konto kryptowalutowe.

Część tych zmian możemy przypisać mechanizmowi blokowania podejrzanych SMS-ów – zdecydowanie łatwiej nam rozpoznawać smishing zawierający link dzięki analizie pod kątem umieszczenia adresu strony na Liście Ostrzeżeń. Dzięki temu wzorce blokujące wiadomości wysyłane z linkiem powstają trochę szybciej. Innym powodem jest to, że oszuści bardzo szybko dostosowują się do bieżących trendów. Przykładem jest wykorzystanie boomu na inwestycje w ostatnich latach. Przestępcy dobierają odpowiednie scenariusze, aby zwiększyć szanse, że adresat będzie miał znany sobie punkt odniesienia do wiadomości, którą otrzymuje. W znacznej większości nie są to spersonalizowane oszustwa, na korzyść przestępców działa tu efekt skali. Dlatego zawsze warto zadać sobie pytanie, czy paczka, na którą czekamy, na pewno jest dostarczana przez piszącą do nas firmę kurierską, z jakiego powodu doradca lub giełda pisze SMS zamiast wysłać powiadomienie w aplikacji albo czemu nasze dziecko nie poprosiło nauczyciela o poinformowanie nas o zdarzeniu, albo czy w ogóle mamy dziecko.

Niezmiennie zachęcamy do pomocy w walce ze smishingiem poprzez wysyłanie wiadomości pod numer 8080. Jest to nie tylko sposób na uzyskanie odpowiedzi na pytanie „Czy wiadomość jest złośliwa?”, lecz także na ochronę innych użytkowników. W tym procesie to czas reakcji ma największe znaczenie, dlatego prosimy bez wahania zgłaszać podejrzane materiały.

Skoordynowane ujawnianie podatności

W roku 2025 CERT Polska osiągnął znaczące wyniki w obszarze skoordynowanego ujawniania podatności. Opublikowaliśmy 165 identyfikatorów CVE, z czego 8 podatności zostało odkrytych w wyniku badań własnych. Działalność w tym obszarze jest ważnym filarem operacyjnym zespołu w kontekście wdrażania wymogów europejskiego prawodawstwa, szczególnie dyrektywy NIS 2 i rozporządzenia CRA, które definiują nowe obowiązki dla podmiotów uczestniczących w ekosystemie zarządzania podatnościami.

Działalność jako CNA

Od sierpnia 2023 roku CERT Polska ma status CNA (CVE Numbering Authority) i wciąż jest jedynym podmiotem w Polsce uprawnionym do przyznawania identyfikatorów w programie CVE (Common Vulnerabilities

and Exposures), będącym globalnym standardem numerowania i katalogowania podatności w oprogramowaniu. W pierwszym roku operacyjnym (sierpień 2023 – lipiec 2024) CERT Polska opublikował 73 identyfikatory CVE. Systematycznie zwiększamy nasze doświadczenie, zyskujemy zaufanie badaczy bezpieczeństwa i umacniamy kontakty z producentami oprogramowania, co pozwala na efektywniejsze obsługiwanie kolejnych podatności zgłaszanych nam do skoordynowanego ujawnienia.

Rok 2025 przyniósł znaczący wzrost aktywności: łącznie 165 identyfikatorów CVE opublikowanych przez CERT Polska oznacza podwojenie dotychczasowej pracy i odzwierciedla rosnącą liczbę zgłoszeń podatności pochodzących zarówno od badaczy zewnętrznych, jak i z wyników badań własnych zespołu.

TABELA 3. Opublikowane identyfikatory CVE od stycznia do grudnia 2025 roku

Miesiąc 2025	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	Razem
Liczba opublikowanych identyfikatorów CVE	4	9	11	15	22	3	6	36	16	12	21	10	165
Na podstawie badań własnych CERT Polska	0	0	0	0	0	0	0	0	7	1	0	0	8

Liczba opublikowanych w danym miesiącu informacji o podatnościach jest zmienna, ponieważ zgłoszone przypadki mogą dotyczyć jednego lub wielu błędów w tym samym produkcie. W 2025 roku rekordowy dla nas pod względem liczby był zbiór 17 podatności w CGM CLININET opublikowanych 27 sierpnia 2025 roku. Z tego powodu miesiąc ten zapisał się jako najbardziej aktywny pod względem ujawnionych podatności.

Do najistotniejszych podatności ujawnionych z naszą pomocą należały:

- CVE-2025-7063 oraz 8 innych CVE w oprogramowaniu PAD CMS umożliwiające m.in. zmianę hasła dowolnego użytkownika. W odpowiedzi na zidentyfikowane zagrożenia oraz brak dalszego wsparcia dla produktu Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał rekomendację zaprzestania korzystania z tego oprogramowania.
- CVE-2025-9313 w oprogramowaniu mMedica firmy Asseco Poland S.A. umożliwiające uzyskanie nieautoryzowanego dostępu do bazy danych.
- CVE-2024-8773 i CVE-2024-8774 w oprogramowaniu SIMPLE.ERP umożliwiające zwiększenie uprawnień użytkownika do administratora bazy danych.
- CVE-2025-10910 w produktach Govee z łącznością sieciową umożliwiające przejęcie kontroli nad urządzeniem.

Proces przeprowadzonych przez nasz zespół badań oprogramowania CMS dla Biuletynów Informacji Publicznej został opisany w osobnym artykule (→ s. 93).

Przykładem skoordynowanego przez nas przypadku ujawnienia podatności, który był szerzej komentowany w środowisku branżowym, jest CVE-2025-4049 w oprogramowaniu FARA firmy SIGNUM-NET. Kontrowersje wzbudziło kwestionowanie przez producenta istnienia i sposobu wykrycia zgłaszanych podatności. Przeprowadzone przez nas kolejne badanie potwierdziło raportowane błędy, co skłoniło producenta do podjęcia działań naprawczych.

Najtrudniejsze z naszej perspektywy są jednak niezmiennie przypadki, gdzie pomimo wielu prób kontaktu z producentem oprogramowania nie otrzymujemy żadnej odpowiedzi, a błędy nie są usuwane. W minionym roku problem ten dotyczył wielu zgłaszanych nieprawidłowości:

- CVE-2025-22270 i 4 innych CVE w oprogramowaniu CyberArk Endpoint Privilege Manager,
- CVE-2024-13892 i 2 innych CVE w kamerach Smartwares CIP-37210AT i C724IP,
- CVE-2025-2098 w oprogramowaniu Fast CAD Reader firmy Beijing Honghu Yuntu Technology,
- CVE-2025-3758 i 1 innego CVE w oprogramowaniu Netis Systems WF2220,
- CVE-2025-53811 w aplikacji Mosh-Pro na systemy operacyjne macOS,
- CVE-2025-7761 w oprogramowaniu Akcess-Net Lepszy BIP,
- CVE-2025-54172 i 14 innych CVE w oprogramowaniu OpenSolution: Quick.CMS, Quick.CMS.Ext, Quick.Cart,
- CVE-2025-9983 w kamerach GALAYOU G2,
- CVE-2025-53701 i 1 innego CVE w kamerach Vilar VS-IPC1002,
- CVE-2025-9977 w oprogramowaniu Times Software E-Payroll,
- CVE-2025-65007 i 4 innych CVE w oprogramowaniu routera WODESYS WD-R608U.

Funkcjonowanie CERT Polska w roli CNA wiąże się ze ścisłym respektowaniem wytycznych międzynarodowego programu CVE. Oznacza to m.in. możliwość obsługi zgłoszeń lub raportowania własnych odkryć jedynie w tych produktach, które nie należą do zakresu odpowiedzialności innych CNA – w takich sytuacjach naszym obowiązkiem jest przekierowanie zgłaszającego do właściwej organizacji. Artykuły zawierające informacje o wszystkich podatnościach ujawnionych przez zespół CERT Polska są publikowane na stronie cert.pl/cve. Więcej informacji o obsłudze zgłoszeń podatności przez nasz zespół znajduje się na stronie cert.pl/cvd.

Kryzys programu CVE

W kwietniu 2025 roku program CVE został dotknięty poważnym kryzysem związanym z finansowaniem. Dotychczasowy kontrakt na utrzymanie i rozwój CVE, realizowany przez organizację MITRE na zlecenie amerykańskiej agencji rządowej CISA, wygasł 16 kwietnia 2025 roku. Pojawiło się realne zagrożenie, że tworzona przez 25 lat baza przestanie być aktualizowana, co mogłoby doprowadzić do chaosu w światowym ekosystemie zarządzania podatnościami. W ostatniej chwili CISA ogłosiła przedłużenie umowy na utrzymanie programu CVE, aby uniknąć przerwania ciągłości usług.

Zakłócenia wpłynęłyby na krajowe bazy danych podatności, narzędzia wspierające tworzenie oprogramowania czy system reagowania na incydenty. W szczególności krótkoterminową konsekwencją byłoby uniemożliwienie rezerwowania i publikowania wpisów CVE, co doprowadziłoby do chaosu w komunikacji o podatnościach. W dalszej perspektywie powstawałyby zdecentralizowane, konkurencyjne bazy danych i utracono by zaufanie do globalnego rejestru.

Kryzys uwydatnił słabość w postaci zależności programu od jednego źródła finansowania. W odpowiedzi na tę sytuację zawiązały się inicjatywy, których celem jest wspieranie długoterminowej stabilności systemu zarządzania podatnościami. Przykładami takich inicjatyw są: powołanie fundacji CVE Foundation mającej zwiększyć niezależność programu CVE, przyspieszenie przez ENISA opublikowania Europejskiej Bazy Podatności (EUVD), zdecentralizowany system identyfikowania podatności Global CVE (GCVE) zaproponowany i rozwijany przez zespół CIRCL (Computer Incident Response Center Luxembourg).

Oczekiwane zmiany prawne

Kluczowe dla obszaru skoordynowanego ujawniania podatności jest umocowanie prawne, które bierze swój początek z dyrektywy NIS 2 (Network and Information Security Directive 2), zatwierdzonej przez Radę UE 28 listopada 2022 roku. Wdrażanie polskiej implementacji zostało opóźnione, a termin transpozycji do prawa krajowego minął 17 października 2024 roku. Zgodnie z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa do pełnienia funkcji koordynatora procesu ujawniania podatności wyznaczony jest nasz zespół.

Rok 2025 był okresem przygotowywania wdrożenia przyjętego przez Unię Europejską aktu o cyberodporności (Cyber Resilience Act, CRA), dotyczącego przede wszystkim producentów produktów z elementami cyfrowymi. Zapisy z rozdziału IV CRA (art. 35–51) zaczną być stosowane od 11 czerwca 2026 roku, natomiast te z art. 14 (określające obowiązki producentów w zakresie zgłaszania podatności i incydentów) – od 11 września 2026 roku. Pozostałe przepisy CRA będą stosowane od 11 grudnia 2027 roku. Producenci zostaną zobligowani m.in. do zapewnienia, że ich produkty

nie zawierają aktywnie wykorzystywanych podatności, do dokumentowania elementów oprogramowania wykorzystanego w produkcie poprzez Software Bill of Materials (SBOM), prowadzenia polityki skoordynowanego ujawniania podatności oraz do niezwłocznego raportowania incydentów i aktywnie wykorzystywanych podatności do wyznaczonego zespołu CSIRT.

Raportowanie i przekazywanie informacji będzie się odbywać za pomocą nowo utworzonej pojedynczej platformy sprawozdawczej (ang. single reporting platform, SRP), która ma zostać udostępniona przez ENISA do 11 września 2026 roku. Zespół CERT Polska aktywnie uczestniczy we wszystkich fazach projektowania i opiniowania nowej platformy. Braliśmy także udział w konsultacjach dotyczących rozporządzenia delegowanego, które Komisja Europejska opublikowała 11 grudnia 2025 roku. Uzupełnia ono CRA o warunki umożliwiające opóźnienie przekazywania zgłaszanych informacji między uprawnionymi CSIRT-ami. Wśród powodów uzasadniających odroczenie przekazania zgłoszenia znalazły się m.in. sytuacje, gdy informacje umożliwiają łatwe ponowne wykorzystanie podatności, zgłoszona podatność jest w trakcie procesu CVD czy jeden z pozostałych CSIRT-ów jest dotknięty incydentem naruszającym zapewnienie poufności przekazywanych informacji.

Rola CERT Polska w ekosystemie CVD

CERT Polska aktywnie uczestniczy w międzynarodowych inicjatywach związanych ze skoordynowanym ujawnianiem podatności. Angażujemy się w działania sieci CSIRTs Network – uczestniczymy jako współprowadzący w pracach grupy roboczej ds. skoordynowanego ujawniania podatności (WG CVD). Prace grupy dotyczą harmonizacji procedur i polityk CVD w Unii Europejskiej.

Ponadto w 2025 roku zostaliśmy zaproszeni do udziału w Global Community of Practice on CVD (CoP CVD), forum utworzonym przez CISA. Inicjatywa ta ma na celu promocję współpracy pomiędzy podmiotami rządowymi zaangażowanymi w proces ujawniania podatności, a także umożliwia wymianę doświadczeń i opracowywanie dobrych praktyk.

W 2025 roku dzieliliśmy się także swoimi doświadczeniami w skoordynowanym ujawnianiu podatności m.in. podczas warsztatów dla producentów oprogramowania sektora ochrony zdrowia w Polsce czy dla przedstawicieli organizacji rządowych i podmiotów infrastruktury krytycznej w Kosowie.

#BezpiecznyPrzemysł

W 2025 roku kontynuowaliśmy inicjatywę #BezpiecznyPrzemysł, mającą na celu podniesienie poziomu cyberbezpieczeństwa polskiej

infrastruktury przemysłowej. Koncentrujemy się na identyfikacji urządzeń przemysłowych dostępnych z publicznego internetu, takich jak sterowniki PLC i panele operatorskie (HMI), oraz na informowaniu właścicieli o zagrożeniach wynikających z niewłaściwej konfiguracji tych urządzeń. Dzięki autorskiemu systemowi Snitch (szczegóły na s. 109–110), który stale usprawniamy, zwiększyła się widoczność skanowanych urządzeń, a także wydajność procesu monitoringu, podejmowania decyzji i tym samym skrócił się czas reakcji na incydenty.

Wydarzenia

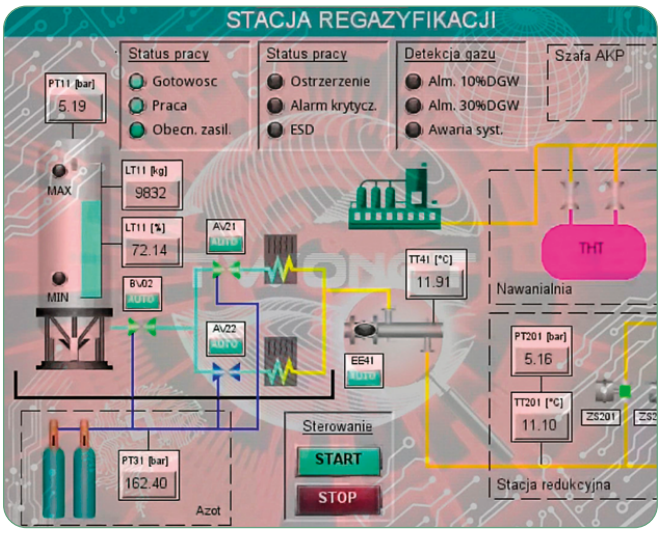
Stacja uzdatniania wody

W wyniku zalogowania się do urządzeń stacji uzdatniania wody hakerzy zmienili ustawienia pomp, co doprowadziło do wyczerpania zasobów w zbiorniku, a w konsekwencji spowodowało przerwę w dostawie wody. Po odzyskaniu dostępu do paneli sterujących wartości zostały przywrócone do stanu właściwego i po napełnieniu zbiorników przywrócono dostawę wody.

Incydent spowodował przerwę w dostarczaniu wody na ok. 6 godzin dla ok. 2,5 tys. mieszkańców gminy.

Stacja regazyfikacji

Stacja regazyfikacji to instalacja średniej wielkości przekształcająca skroplony gaz ziemny (LNG) z powrotem w gaz lotny, umożliwiająca dalsze jego wykorzystanie w sieciach gazowych oraz instalacjach przemysłowych. Grupa haktywistyczna opublikowała na komunikatorze Telegram nagranie, na którym zaprezentowała, jak zmienia nastawy parametrów pracy.



RYSUNEK 31. Fragment nagrania, na którym grupa haktywistyczna zmienia nastawy parametrów pracy stacji regazyfikacji

Pulpit zdalny

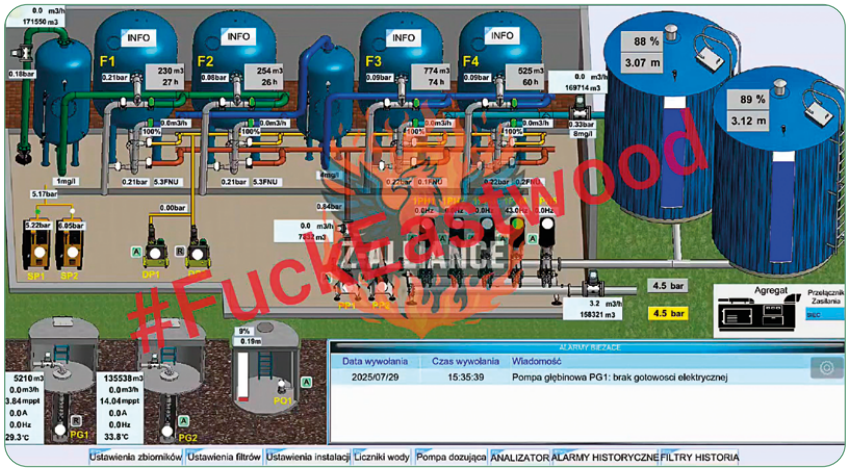
W 2025 roku kontynuowaliśmy inicjatywę sprawdzania domyślnych haseł do pulpitu zdalnego VNC. Protokół VNC jest łatwym wektorem ataku ze względu na archaiczny mechanizm uwierzytelnienia lub jego brak. Nie pomaga również zwyczaj ustawiania bardzo prostych haseł typu: 111111, 12345678. Ataki na panele HMI są bardzo medialne i widowiskowe ze względu na możliwość udokumentowania udanego zalogowania się do panelu zarządzania. Wśród atakujących wykorzystujących słabości protokołu VNC zaobserwowaliśmy grupy haktywistyczne.

W 2025 roku poszerzaliśmy nasze próby zalogowania się do paneli o nowe hasła, a w przypadku instancji zaatakowanych przez haktywistów uzupełnialiśmy naszą bazę do testów po uzyskaniu wykorzystanych haseł od administratorów. Z naszych obserwacji wynika, że protokół VNC jest wykorzystywany najczęściej przez:

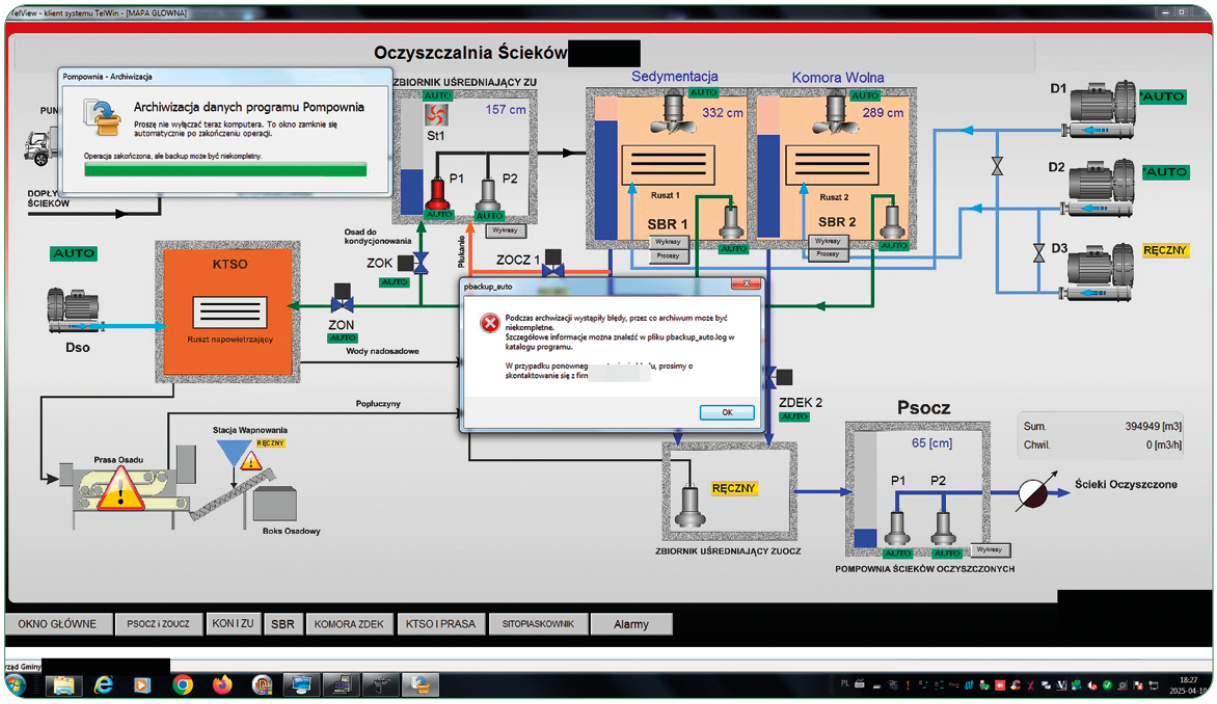
- małe elektrownie wodne,
- oczyszczalnie/przepompownie ścieków,
- systemy zarządzania budynkiem (ang. Building Management System, BMS), np. w szpitalach czy prywatnych domach,
- HVAC (ang. heating, ventilation, air conditioning), np. w centrach handlowych, dyskontach, obiektach wielkopowierzchniowych,
- panele zarządzania instalacjami basenów (np. baseny hotelowe, pływalnie).

W przypadku pozyskania informacji o dostępności systemu zespół kontaktuje się z podmiotem odpowiedzialnym, wysyła powiadomienia oraz przekazuje informację do odpowiedniego CSIRT-u.

RYSUNEK 32. Panel jednej ze stacji uzdatniania wody, w której były zmieniane nastawy parametrów pracy

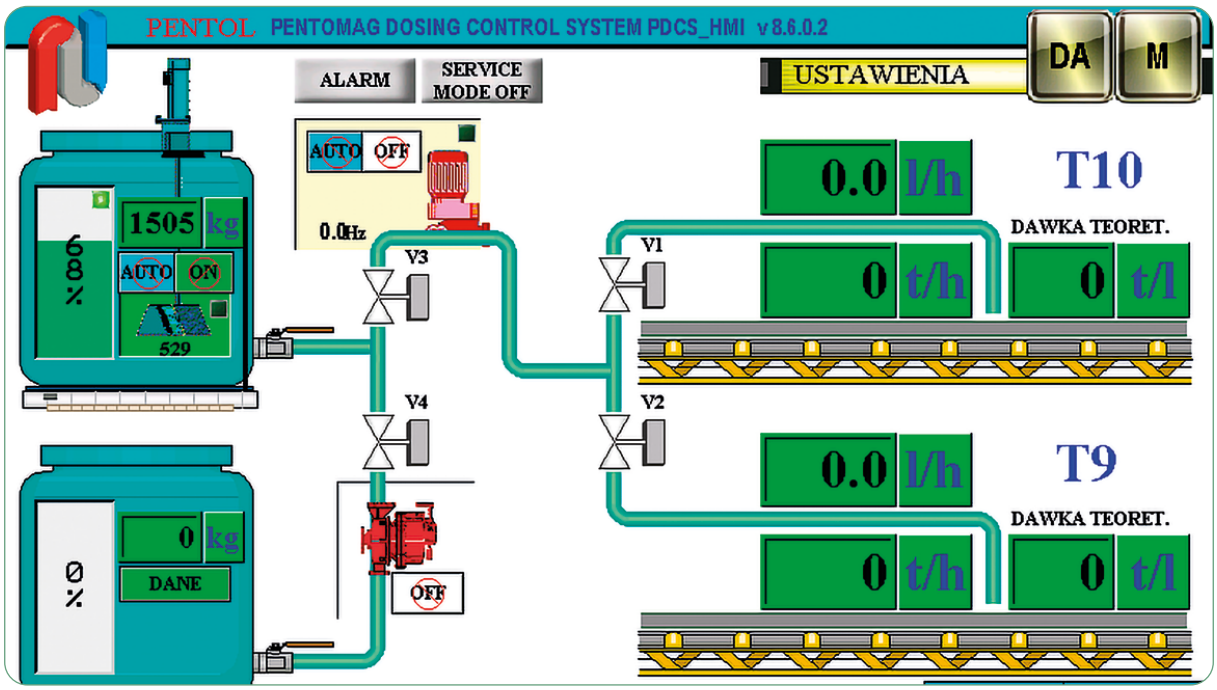


RYSUNEK 33. Panel miejskiej oczyszczalni ścieków, do której uzyskaliśmy dostęp, korzystając z prostego hasła



Z niestandardowych przypadków zaobserwowaliśmy system sterowania dozowaniem środka PentoMag, który jest specjalnym dodatkiem do paliw zapobiegającym korozji i osadzaniu się popiołu w kotłach, silnikach czy turbinach.

RYSUNEK 34. System sterowania dozowaniem dodatku do paliw



Audyty aplikacji webowych

Zespół Testów Bezpieczeństwa działający w ramach CERT Polska w 2025 roku przeprowadził serię audytów bezpieczeństwa, których 72% obejmowało testy penetracyjne aplikacji webowych. Celem prowadzonych badań była identyfikacja podatności, które w przypadku ich wykorzystania mogłyby stanowić zagrożenie dla poszczególnych komponentów lub całych systemów informatycznych.

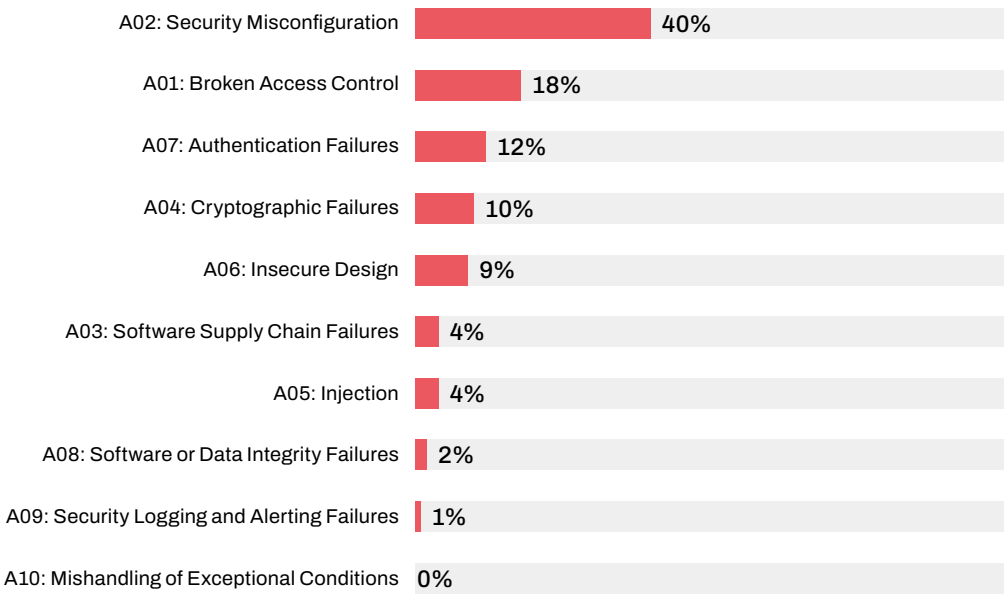
Wszystkie testy penetracyjne realizowaliśmy z wykorzystaniem autorskiej metodyki audytowej. W zależności od zakresu i charakteru badania stosowaliśmy odpowiednie strategie oraz techniki testowe, a scenariusze testów opracowywaliśmy na podstawie doświadczenia zespołu audytorskiego oraz sprawdzonych wzorców i standardów branżowych, takich jak wytyczne OWASP (Open Web Application Security Project).

Do kluczowych elementów przyjętej metodyki należały:

- analiza architektury systemu oraz identyfikacja potencjalnych zagrożeń,
- testy manualne wspierane narzędziami automatycznymi,
- sporządzanie raportów przedstawiających wyniki audytów z uwzględnieniem poziomu krytyczności wykrytych podatności,
- formułowanie rekomendacji dostosowanych do specyfiki badanego systemu.

Do klasyfikacji podatności wykorzystaliśmy standard OWASP Top Ten 2025.

WYKRES 2. Wykres przedstawiający podatności z podziałem na kategorie



Wyniki przeprowadzonych audytów umożliwiły wskazanie obszarów wymagających szczególnej uwagi i działań naprawczych. Zdecydowana większość wykrytych podatności została zidentyfikowana w 4 kategoriach, które opisujemy poniżej.

- A02 – Security Misconfiguration (nieprawidłowa konfiguracja systemów i usług): ok. 40%. Podatności te najczęściej wynikały z błędnych ustawień komponentów systemowych i mogły prowadzić do nieautoryzowanego dostępu do zasobów lub do eskalacji uprawnień.

- A01 – Broken Access Control (nieprawidłowa kontrola dostępu): ok. 18%. Podatności wskazywały na luki związane z niewłaściwym zarządzaniem dostępem do danych, co zwiększało ryzyko ich nieuprawnionego ujawnienia lub modyfikacji.

- A07 – Authentication Failures (nieprawidłowa implementacja mechanizmów uwierzytelniania): ok. 12%. Kategoria ta obejmowała błędy w obszarze uwierzytelniania, w tym nieprawidłowe zarządzanie sesjami, niewystarczającą weryfikację tożsamości użytkowników oraz słabą politykę haseł.

- A04 – Cryptographic Failures (błędna implementacja rozwiązań kryptograficznych): ok. 10%. Podatności dotyczyły m.in. stosowania przestarzałych algorytmów kryptograficznych, nieprawidłowego generowania kluczy oraz niewłaściwego przechowywania materiałów kryptograficznych.

Łącznie powyższe kategorie stanowiły ok. 80% wszystkich wykrytych podatności, co jednoznacznie wskazuje na obszary wymagające priorytetowych działań naprawczych.

Analiza wykazała również, że mniejszy odsetek podatności dotyczył kategorii:

- A06 – Insecure Design (nieprawidłowe projektowanie pod kątem bezpieczeństwa): ok. 9%,

- A05 – Injection (wstrzyknięcia): ok. 4%.

Oznacza to, że w badanych systemach relatywnie rzadko występowały problemy związane z błędami projektowymi w zakresie bezpieczeństwa oraz z klasycznymi atakami wykorzystującymi wstrzyknięcie kodu (np. SQL Injection). Należy jednak podkreślić, że podatności te mogą prowadzić do poważnych konsekwencji, takich jak obejście mechanizmów zabezpieczeń, eskalacja uprawnień czy nieautoryzowany dostęp do danych. W szczególności ataki pozwalające na wstrzyknięcie kodu umożliwiają manipulowanie danymi, wykonywanie nieautoryzowanych operacji, a w skrajnych przypadkach – przejęcie kontroli nad serwerem aplikacji.

Pomimo stosunkowo niskiej częstotliwości występowania podatności te wymagają stałego monitorowania i eliminowania, ponieważ ich potencjalny wpływ na bezpieczeństwo systemu może mieć charakter krytyczny.

Wyniki audytów potwierdzają zasadność prowadzenia regularnych testów penetracyjnych, które w połączeniu z systematycznym wdrażaniem rekomendacji znacząco redukują ryzyko wystąpienia incydentów bezpieczeństwa.

Analiza bezpieczeństwa aplikacji mobilnych sektora publicznego

Rosnąca liczba aplikacji mobilnych wykorzystywanych w sektorze publicznym powoduje istotne wyzwania w obszarze zapewnienia ich bezpieczeństwa. Aplikacje te są powszechnie dostępne dla obywateli i często operują na informacjach identyfikujących użytkowników oraz personel administracyjny, co podnosi wymagania w zakresie ochrony poufności oraz integralności danych. Jednocześnie ograniczone zasoby organizacyjne utrudniają prowadzenie pełnoskalowych manualnych testów bezpieczeństwa dla każdej aplikacji.

Odpowiedzią na te potrzeby jest rozwijane narzędzie Deckard, którego celem jest usprawnienie procesu analizy bezpieczeństwa aplikacji mobilnych poprzez automatyzację wybranych testów oraz ujednolicenie procesu zbierania i prezentacji wyników.

Zakres analizowanego materiału

W ramach projektu przeprowadziliśmy analizę 283 aplikacji mobilnych Android ujętych w „Wykazie aplikacji mobilnych podmiotów publicznych" opublikowanym na portalu dane.gov.pl[39], na podstawie stanu wykazu z lipca 2025 roku.

Analizowane aplikacje reprezentują różne obszary funkcjonowania sektora publicznego, w tym administrację publiczną, ochronę zdrowia, oświatę, transport, kulturę, gospodarkę odpadami, media oraz rolnictwo. Zgromadzony zbiór stanowi reprezentatywną próbkę aplikacji mobilnych udostępnianych przez podmioty publiczne.

39 https://dane.gov.pl/pl/dataset/1875,wykaz-adresow-stron-internetowych-i-wykaz-aplikacji--mobilnych-podmiotow-publicznych/resource/65295

Metoda analizy i założenia projektu Deckard

Projekt Deckard jest oparty na wytycznych OWASP Mobile Application Security Testing Guide (MASTG) oraz OWASP Mobile Application Security Verification Standard (MASVS). Na potrzeby automatyzacji wyodrębniliśmy zestaw sprawdzeń, które zostały uznane za bazowy poziom bezpieczeństwa (ang. baseline), wspólny dla wszystkich typów aplikacji mobilnych, niezależnie od ich funkcjonalności czy modelu biznesowego.

Lista obejmuje problemy bezpieczeństwa, które występują powszechnie w aplikacjach mobilnych i mogą być wykrywane automatycznie z wysokim poziomem pewności. Stanowią one podstawowe wymagania bezpieczeństwa aplikacji mobilnych.

Do bazowego zestawu błędów zaliczono m.in.:

- obecność trybu debugowania w wersji produkcyjnej,
- zaufanie do certyfikatów dodanych przez użytkownika,
- wsparcie dla przestarzałych wersji systemu operacyjnego (minSdkVersion < 23),
- brak wystarczających zabezpieczeń przy wykorzystaniu WebView,
- przechowywanie kluczy kryptograficznych w kodzie,
- użycie przestarzałych certyfikatów (przekroczony czas ważności),
- brak weryfikacji integralności pakietu APK,
- użycie nieszyfrowanej komunikacji sieciowej.

Deckard przeprowadza analizę w formie modularnego procesu, w którym poszczególne etapy wykorzystują mikroserwisy uruchamiane w środowisku kontenerowym. Wykorzystywane narzędzia (m.in. MobSF, JADX, autorskie skrypty) zwracają wyniki w ujednoliconym formacie, co umożliwia ich dalszą automatyczną agregację oraz przygotowanie raportów.

Klasyfikacja błędów bezpieczeństwa

Zidentyfikowane nieprawidłowości zostały pogrupowane w tematyczne klasy znalezisk, co pozwala na bardziej ogólny i czytelny opis wyników analizy na potrzeby raportu. Poniżej opisujemy typy błędów, które wyszczególniliśmy podczas analizy.

- Błędy konfiguracji środowiska uruchomieniowego – wynikają one z nieprawidłowej konfiguracji aplikacji w środowisku produkcyjnym, w szczególności z pozostawienia mechanizmów debugowania lub braku podstawowych zabezpieczeń platformowych.

- Niezabezpieczona komunikacja sieciowa – problemy związane z nieprawidłową obsługą protokołów sieciowych i TLS. Obejmują one m.in. akceptację certyfikatów użytkownika, wadliwą obsługę błędów SSL czy brak zdefiniowanej listy certyfikatów, którym aplikacja może zaufać. Skutkiem tych problemów może być przechwytywanie lub modyfikacja danych przesyłanych pomiędzy aplikacją a serwerem.

- Błędy kryptograficzne i zarządzania kluczami – dotyczą one niewłaściwego użycia mechanizmów kryptograficznych, takich jak stosowanie słabych algorytmów, zbyt krótkich kluczy czy przechowywanie kluczy bezpośrednio w kodzie aplikacji. Problemy te wpływają na poufność i integralność przetwarzanych danych.

- Integralność aplikacji i odporność na manipulację – są to błędy związane z brakiem mechanizmów chroniących aplikację przed modyfikacją, podmianą kodu lub analizą. Obejmują one m.in.: podatność Janus (CVE-2017-13156), brak nowoczesnych schematów podpisu APK (v2/v3/v4) oraz brak mechanizmów utrudniających inżynierię wsteczną.

- Ekspozycja powierzchni ataku i komunikacja między komponentami – dotyczy nadmiernej ekspozycji komponentów aplikacji, braku walidacji danych wejściowych oraz niebezpiecznych mechanizmów komunikacji międzyprocesowej (IPC). Problemy te zwiększają powierzchnię ataku i mogą prowadzić do nieautoryzowanego dostępu do funkcji aplikacji lub danych użytkownika.

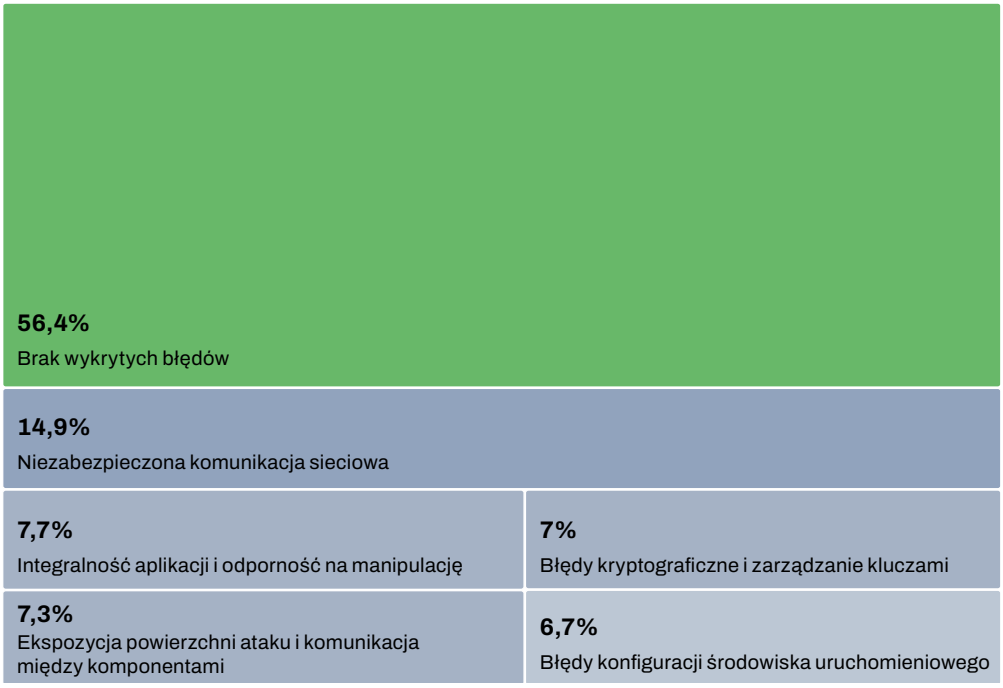
Statystyki wykrytych błędów bezpieczeństwa

W ramach przeprowadzonych analiz ilościowych określiliśmy częstość występowania poszczególnych klas znalezisk bezpieczeństwa w badanym zbiorze aplikacji mobilnych. Wyniki analizy statystycznej zostały wykonane w dwóch uzupełniających się wykresach przedstawiających:

- strukturę wszystkich wyników testów,
- częstość występowania błędów w aplikacjach.

Pierwszy z wykresów przedstawia rozkład wszystkich wyników wykonanych sprawdzeń, niezależnie czy dla danego sprawdzenia została wykryta nieprawidłowość, czy nie.

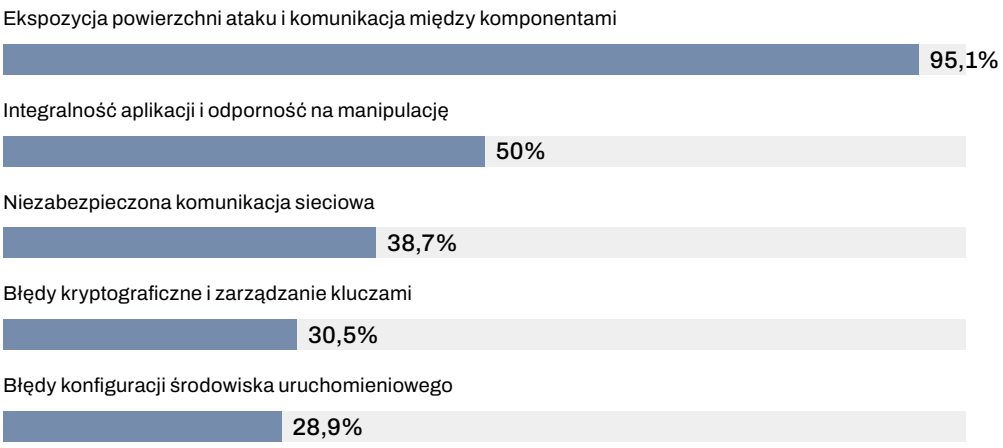
WYKRES 3. Struktura wszystkich wyników testów



Każdy wynik testu został przypisany do jednej z kategorii podatności lub oznaczony jako wynik negatywny, nieklasyfikujący się jako podatność bezpieczeństwa. W tej perspektywie ok. 56,4% wszystkich wykonanych sprawdzeń zakończyło się wynikiem negatywnym. Największy udział wśród wykrytych problemów stanowiły znaleziska z obszaru niezabezpieczonej komunikacji sieciowej (14,9%), podczas gdy pozostałe kategorie osiągały wartości na poziomie ok. 6–7%.

Drugi z wykresów prezentuje odsetek aplikacji, w których wykryto co najmniej jedno znalezisko z danej kategorii nieprawidłowości.

WYKRES 4. Częstość występowania błędów w aplikacjach



Wyniki wskazują, że największy odsetek aplikacji zawierał znaleziska z obszaru ekspozycji powierzchni ataku i komunikacji między komponentami (95,1%) oraz integralności i odporności na manipulację (50%). Pozostałe kategorie występowały również w istotnej części analizowanych aplikacji (niezabezpieczona komunikacja sieciowa – 38,7%, błędy konfiguracji środowiska uruchomieniowego – 28,9%).

Zaprezentowane statystyki obejmują wyłącznie te klasy błędów, które zostały zaimplementowane w systemie Deckard na obecnym etapie jego rozwoju. Wraz z dalszym rozszerzaniem funkcjonalności narzędzia oczekiwane jest zwiększenie liczby wykrywanych znalezisk oraz uzyskanie pełniejszego obrazu poziomu bezpieczeństwa analizowanych aplikacji.

Wnioski i kierunki dalszego rozwoju

Dotychczasowe prace nad projektem Deckard potwierdzają zasadność wykorzystania automatyzacji w procesie wstępnej analizy bezpieczeństwa aplikacji mobilnych sektora publicznego. Zastosowane podejście umożliwia szybkie wykrywanie powtarzalnych, bazowych błędów bezpieczeństwa oraz porządkowanie wyników w sposób spójny i skalowalny.

W kolejnych etapach planujemy dalszy rozwój narzędzia poprzez rozszerzanie zakresu obsługiwanych testów OWASP MASTG, zwiększanie pokrycia zarówno dla analiz statycznych, jak i dynamicznych oraz integrację wyników z systemami zarządzania podatnościami. Deckard stanowi fundament pod budowę ustandaryzowanego procesu oceny bezpieczeństwa aplikacji mobilnych w sektorze publicznym, umożliwiającego efektywne zarządzanie ryzykiem w skali całego ekosystemu usług cyfrowych.

Locked Shields 2025

Od 6 do 9 maja 2025 roku odbywała się 15. edycja Locked Shields – największych na świecie ćwiczeń z zakresu cyberobrony, organizowanych przez Centrum Doskonalenia Cyberobrony NATO (NATO CCDCOE). Wzięło w nich udział 41 państw podzielonych na 17 zespołów. Zadaniem ponad 4 tys. specjalistów w zakresie reagowania na incydenty, w dziedzinie prawa czy komunikacji była obrona fikcyjnej Berylii przed atakami stworzonej na potrzeby ćwiczeń wrogiej Crimsonii.

Rozmach, z jakim organizowane są czterodniowe ćwiczenia, wymaga od uczestników ścisłej współpracy, co doskonale odzwierciedla warunki prawdziwego ataku. Ponadto każdy zespół składa się z reprezentantów

co najmniej dwóch państw członkowskich Sojuszu, co dodatkowo pozwala na porównanie procedur i scenariuszy reakcji na zagrożenia.

W edycji Locked Shields 2025 polska drużyna pod przewodnictwem oficera Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) połączyła siły z przedstawicielami Francji reprezentującymi Commandement de la cyberdéfense (COMCYBER). Z niemałym wkładem ekspertów z CERT Polska ponownie stanęliśmy na podium – tym razem na jego drugim stopniu. Uplasowaliśmy się pomiędzy zwycięskim zespołem Niemiec i Singapuru a łączoną operacją Włoch, Słowenii i USA.

Ochrona infrastruktury przygotowanej na potrzeby ćwiczeń nie była łatwa – każdy zespół musiał zabezpieczyć ponad 8 tys. podległych sobie systemów. Scenariusz zakładał niemal ciągłą eskalację – od działań dezinformacyjnych, poprzez wycieki danych i rozprzestrzenianie się złośliwego oprogramowania, aż po bezpośrednie ataki na sieci energetyczne, zaplecze komunikacyjne czy systemy obrony przeciwlotniczej. Mitygacja skutków incydentu była tylko jednym z aspektów obrony – równie ważnymi elementami były strategiczna komunikacja kierowana do społeczeństwa Berylii i ciągła analiza prawnych aspektów podejmowanych działań.

Z roku na rok złożoność wyzwań przygotowanych na Locked Shields rośnie zgodnie z najbardziej aktualnymi trendami w cyberprzestrzeni. W 2025 roku obserwowaliśmy duży wzrost znaczenia sztucznej inteligencji w procesach zarówno ataku, jak i obrony, coraz większą rolę infrastruktury chmurowej, a także pierwsze podejście do problematyki obliczeń kwantowych. To wszystko w warunkach nieustannej presji czasu, stresu i rywalizacji. Aby jak najwierniej oddać realia, wprowadzono także element nacisków politycznych, a scenariusz ćwiczeń uwzględniał napięcie geopolityczne i naruszenia suwerenności państw.

Rolą ćwiczeń takich jak Locked Shields jest sprawdzenie gotowości państw do radzenia sobie z wyzwaniami zmieniającego się świata i cyberprzestrzeni, ale także, a może nawet przede wszystkim, budowanie mechanizmów wzajemnego zaufania, wsparcia i wymiany informacji, które w obliczu realnego zagrożenia będą kluczowe, by wspólnota NATO sprawnie i skutecznie odparła wszelkie wrogie działania. Polska cyberprzestrzeń jest chroniona przez setki specjalistów, którzy chcą i potrafią ze sobą współpracować. Tak było podczas Locked Shields pod przewodnictwem DKWOC, gdy eksperci z CERT Polska zajmowali się m.in. ochroną systemów specjalnych, sieci, aplikacji webowych czy tematami prawnymi, tak też jest na co dzień, gdy polskie instytucje dzielą się zadaniami w ramach swoich constituency, wymieniają informacje i doświadczenia oraz wspierają się operacyjnie.

Badanie oprogramowania CMS dla Biuletynów Informacji Publicznej

Systemy zarządzania treścią (ang. Content Management System, CMS) umożliwiają wygodne prowadzenie serwisów internetowych, jednak występowanie podatności w oprogramowaniu tego typu sprawia, że wiele stron internetowych może być celem ataków. Część z tych systemów jest wykorzystywana do prowadzenia Biuletynów Informacji Publicznych (BIP). Otrzymujemy znaczną liczbę zgłoszeń podatności w systemach CMS, dlatego postanowiliśmy w 2025 roku dodatkowo przetestować niektóre z tych rozwiązań w ramach działań własnych.

Podmioty publiczne mają obowiązek prowadzenia Biuletynów Informacji Publicznej, a wiele z nich decyduje się na gotowe rozwiązania przeznaczone do tego celu. Jak wynika z naszych obserwacji, zdarzają się produkty, których twórcy nie zapewniają bezpieczeństwa systemów, szczególnie pod kątem wdrażania poprawek usuwających zgłaszane podatności.

Skontaktowaliśmy się z producentami części rozwiązań i otrzymaliśmy oprogramowanie do testów. Mieliśmy możliwość weryfikacji bezpieczeństwa na odizolowanych instancjach, które nie są używane produkcyjnie, ponadto w niektórych przypadkach posiadaliśmy dostęp do kodu źródłowego. To pozwoliło nam przetestować produkty pod kątem występowania najpopularniejszych zagrożeń. Należy jednak pamiętać, że przeprowadzone przez nas testy nie dają gwarancji wykrycia wszystkich podatności. Dodatkowo aktualizacje wydawane przez twórców mogą wprowadzać w przyszłości nowe podatności.

W 2025 roku zespół CERT Polska nadał 43 numery CVE dla podatności w programach klasy CMS służących utrzymywaniu Biuletynów Informacji Publicznej. Wśród wykrytych problemów są m.in. błędy związane z autoryzacją (np. hasła przechowywane w jawnej postaci – CWE-256), z brakiem ograniczeń w możliwości przesyłania plików (CWE-434) czy z niepoprawną neutralizacją danych wejściowych (CWE-79). W przypadku otrzymania informacji o podatnościach krytycznych zespół identyfikuje potencjalnie podatne instancje oraz informuje administratorów o zagrożeniu związanym z tymi lukami bezpieczeństwa.

Z uwagi na wysoki poziom zagrożenia spowodowany podatnościami w oprogramowaniu PAD CMS Pełnomocnik Rządu ds. Cyberbezpieczeństwa zarekomendował zaprzestanie korzystania z tego produktu[40]. Jest to już druga rekomendacja dotycząca systemu BIP, po wydanej w 2024 roku rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotyczącej Biuletynów Informacji Publicznej[41].

40 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-zaprzestanie-korzystania-z-oprogramowania-pad-cms

41 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-biuletynow-informacji-publicznej

Współtworzenie zespołów CSIRT sektorowych

W minionym roku NASK–PIB zawiązał partnerstwo z Urzędem Komisji Nadzoru Finansowego[42] oraz z Ministerstwem Infrastruktury[43] w celu wsparcia w budowie sektorowych zespołów cyberbezpieczeństwa. Przedsięwzięcie jest finansowane ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności oraz Unii Europejskiej.

Rozwój CSIRT KNF

Zespół CSIRT KNF, powołany na mocy zarządzenia Przewodniczącego Komisji Nadzoru Finansowego, funkcjonuje od 1 lipca 2020 roku i realizuje zadania na rzecz cyberbezpieczeństwa podmiotów sektora finansowego. Jest on istotnym ogniwem w walce z oszustwami wymierzonymi w krajowych użytkowników systemów finansowych. Do kluczowych usług zespołu należą monitoring podatności identyfikowanych w sektorze oraz ograniczanie ich skutków, a także działalność edukacyjna. Rolą merytoryczną CSIRT NASK w projekcie jest doskonalenie procesów (przegląd i ocena) oraz systemów (testy bezpieczeństwa) partnera. Celem jest osiągnięcie przez CSIRT KNF zaawansowanego poziomu dojrzałości zgodnie z „ENISA CSIRT Maturity Framework”[44]. Prace projektowe koncentrują się również na rozwoju funkcjonalności serwisu moje.cert.pl, o którym szerzej piszemy w osobnym artykule (→ s. 106–107). Dzięki interfejsowi dostępowemu możliwy będzie skoordynowany przepływ informacji o zdarzeniach wymagających reakcji. Dodatkowo zostaną zagregowane statystyki zdarzeń dotyczących podmiotów sektora, co usprawni i przyspieszy proces wnioskowania o ogólnym poziomie ryzyka.

Budowa CSIRT Infrastruktura

CSIRT Infrastruktura to nowo powstająca jednostka, której formalne powołanie zaplanowano na rok 2026. Obszarem jej działań będą sektory transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji. Celem wsparcia udzielanego przez CSIRT NASK jest ustanowienie w pełni operacyjnych struktur sektorowego zespołu cyberbezpieczeństwa oraz osiągnięcie ich gotowości do realizacji zadań wynikających z ustawy o KSC.

42 https://www.nask.pl/projekty/csirt-knf-budowa-i-rozwoj-sektorowego-zespolu-cyberbezpieczenstwa-dla-sektora-bankowego-i-infrastruktur

43 https://www.nask.pl/projekty/utworzenie-csirt-sektorowego-o-nazwie-roboczej-csirt-infrastruktura

44 https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity

Powołanie nowej komórki tego typu ogłosiło również Ministerstwo Cyfryzacji[45]. CSIRT Cyfra będzie odpowiedzialny za sektor infrastruktury cyfrowej.

Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT

W 2025 roku w kraju obok wspomnianego wyżej CSIRT KNF funkcjonował także CSIRT CeZ dla podmiotów sektora ochrony zdrowia, powołany w styczniu 2023 roku. Nowelizacja ustawy o KSC zakłada znaczne poszerzenie katalogu sektorów, a także obligatoryjne ustanowienie CSIRT-u sektorowego przez nadzorujący je organ właściwy. W odpowiedzi na obecne i przyszłe wyzwania stojące przed organizatorami komórek tego typu zespół CERT Polska w sierpniu 2025 roku opublikował rekomendacje[46] kierunkowe w tym zakresie. Opracowanie to ma na celu pomóc decydentom określić zasoby niezbędne do organizacji zespołów reagujących w zgodzie z obowiązującymi standardami branżowymi, ale również zapewnić ich płynne włączenie w istniejący już system krajowy. Wcześniejsze, niepubliczne, wydanie rekomendacji zostało przygotowane z myślą o powstawaniu CSIRT-ów sektorowych. Wydanie udostępnione w sierpniu 2025 roku można odnieść odpowiednio również do innych zespołów bezpieczeństwa komputerowego, w tym komercyjnych, takich jak CERT, SOC czy ISAC. Zachęcamy do uwzględnienia naszych wskazówek podczas tworzenia lub rozwijania zespołów cyberbezpieczeństwa.

ECSC 2025

European Cybersecurity Challenge (ECSC) to międzynarodowe zawody cyberbezpieczeństwa, organizowane z inicjatywy Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Uczestnikami zawodów są reprezentacje krajów europejskich oraz drużyny z innych państw zaproszone do udziału. Każdy zespół składa się z 5 osób w wieku od 14 do 20 lat oraz z 5 osób w wieku od 21 do 25 lat.

Krajowe kwalifikacje

Tak jak w poprzednich latach CERT Polska przeprowadził krajowe kwalifikacje w celu wyłonienia uczestników drużyny, reprezentującej nasz kraj w zawodach finałowych. Rok 2025 był rekordowy pod względem zainteresowania tymi zawodami – w kwalifikacjach wzięło udział 186 osób,

45 https://www.gov.pl/web/cyfryzacja/ministerstwo-cyfryzacji-tworzy-csirt-cyfra--oto-wszystko-co-warto-na-ten-temat-wiedziec

46 „Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT”, https://cert.pl/posts/2025/08/rekomendacje-csirt

co jest wynikiem wyższym o 30 od poprzedniego rekordu. W trakcie rywalizacji zawodnicy mieli możliwość zmierzenia się z 22 zadaniami (z czego 4 były przygotowane z myślą o osobach rozpoczynających swoją przygodę z udziałem w konkursach typu CTF). Co najmniej jedną „flagę", potwierdzającą rozwiązanie zadania, wysłało 177 osób, co również było rekordowym wynikiem w historii prowadzonych przez nas eliminacji.

Finały w Warszawie

Zawody finałowe w 2025 roku były wyjątkowe – po raz pierwszy w historii ECSC gospodarzem była Polska. Wydarzenie zorganizowane przez Państwowy Instytut Badawczy NASK (wraz z CERT Polska) oraz Ministerstwo Cyfryzacji odbyło się w dniach 6–9 października w hali Torwar. Do rywalizacji przystąpiły reprezentacje z 39 krajów (w tym 5 reprezentacji biorących udział w roli gościa).

W pierwszym dniu zawodnicy mogli zapoznać się z platformami, które były używane podczas zawodów, oraz przetestować poprawność działania infrastruktury. Po zakończeniu tej części odbyła się uroczystość oficjalnego rozpoczęcia zawodów, poprowadzona przez Gynvaela Coldwinda – jedną z najbardziej rozpoznawalnych postaci polskiej społeczności CTF.

Podobnie jak w minionych edycjach właściwa rywalizacja składała się z dwóch części rozgrywanych w dwóch następujących po sobie dniach. Obejmowała ona formaty:

- CTF Jeopardy – zadania o różnym poziomie trudności inspirowane rzeczywistymi problemami związanymi z cyberbezpieczeństwem,
- CTF Attack & Defence – zestaw usług z podatnościami bezpieczeństwa, administrowanych przez każdą drużynę – celem była obrona własnych usług i atak na usługi przeciwników.

Ostatniego dnia wydarzenia odbyło się uroczyste podsumowanie. Zgromadzona widownia miała wówczas okazję wysłuchać prezentacji „CTF Stories" przygotowanej przez Michała „Redforda" Kowalczyka oraz prezentacji „Fun Facts" dotyczącej ciekawych statystyk i zdarzeń w trakcie rywalizacji, którą poprowadził Louis Burda, przedstawiciel Attacking-Lab (grupy zapewniającej zadania i obsługę techniczną drugiego dnia zawodów).

Końcowy wynik obliczany był na podstawie wyników dwóch dni rozgrywek, według formuły normalizującej wyniki osiągnięte w każdym z tych dni. Po podliczeniu punktów na najwyższym stopniu podium stanęła reprezentacja Włoch (wygrała ona również w każdym z dwóch dni), za którą kolejno uplasowały się reprezentacje Danii oraz Niemiec. Reprezentacja Polski zakończyła rywalizację na 7. miejscu, na które złożyło się 10. miejsce w kategorii Jeopardy oraz 5. miejsce w kategorii Attack & Defence. W rankingu reprezentacji gościnnych najlepsza okazała się drużyna z USA.

RYSUNEK 35. Polska reprezentacja na zawodach ECSC 2025

RYSUNEK 36. Zwycięzcy ECSC 2025 – reprezentacja Włoch

Polska prezydencja w Radzie Unii Europejskiej

Od 1 stycznia do 30 czerwca 2025 roku Polska przewodniczyła pracom Rady Unii Europejskiej. Hasło polskiej prezydencji: „Bezpieczeństwo, Europo!" znalazło swoje odzwierciedlenie również w kwestiach cyberbezpieczeństwa, które były traktowane priorytetowo. Zespół CERT Polska aktywnie uczestniczył w inicjatywach wspierających wymianę doświadczeń pomiędzy państwami Unii i wzmacniających jej odporność na cyberzagrożenia.

Zwiększone zaangażowanie w sprawy europejskie

Polska prezydencja wiązała się z intensyfikacją udziału krajowych instytucji w procesach decyzyjnych i eksperckich na poziomie Unii Europejskiej. Szczególną uwagę warto zwrócić na współtworzenie i wdrażanie rozwiązań podnoszących poziom bezpieczeństwa cyfrowego, udział w pracach legislacyjnych oraz aktywną reprezentację polskich interesów. Zespół CERT Polska uczestniczył w konsultacjach, grupach roboczych i inicjatywach mających na celu budowę wspólnej europejskiej odporności na zagrożenia cyfrowe.

SECURE International Summit

Jednym z najważniejszych wydarzeń polskiej prezydencji była konferencja SECURE International Summit 2025, która odbyła się w dniach 3–4 kwietnia w Bydgoszczy. CERT Polska odegrał centralną rolę w organizacji i merytorycznym przygotowaniu tego wydarzenia. W programie znalazły się panele dotyczące budowy unijnej odporności cybernetycznej, wdrożenia Cyber Resilience Act, wyzwań związanych z rozwojem AI i dezinformacją oraz współpracy cywilno-wojskowej w zakresie reagowania na incydenty cyfrowe.
Więcej o tym wydarzeniu piszemy w osobnym rozdziale (→ s. 99–101).

Przewodniczenie Sieci CSIRT

W styczniu 2025 roku przedstawiciel CERT Polska objął funkcję przewodniczącego Sieci CSIRT. Odpowiedzialność ta oznacza reprezentowanie Sieci na forach zewnętrznych oraz koordynację działań związanych z jej pracami, takimi jak ustalanie procedur reagowania, zaangażowanie w wymianę informacji o incydentach, zwiększanie aktywności Sieci. Kadencja przewodniczącego trwa półtora roku i wiąże się ze współpracą w ramach tzw. Trio, składającego się z trzech kolejnych państw przewodniczących Radzie Unii Europejskiej: Polski, Danii i Cypru.

Spotkanie Sieci CSIRT w Krakowie

W maju 2025 roku Kraków stał się miejscem cyklicznego spotkania w ramach tzw. CyberWeek, które zgromadziło przedstawicieli Sieci CSIRT, CyCLONe oraz innych grup Unii Europejskiej odpowiedzialnych za współpracę w obszarze cyberbezpieczeństwa. Wydarzenie to było okazją do wymiany doświadczeń oraz do dyskusji nad wyzwaniami, którym trzeba sprostać w związku z wdrażaniem nowych regulacji, w tym NIS 2 i Cyber Resilience Act. Uczestnicy wydarzenia omawiali także założenia dokumentu Cyber Blueprint, który zawiera plan skoordynowanego reagowania na incydenty w cyberbezpieczeństwie na dużą skalę. Zespół CERT Polska, we współpracy z Akademią Górniczo-Hutniczą w Krakowie i Ministerstwem Cyfryzacji, odpowiadał za organizację spotkania.

Cyber Blueprint

W czasie prezydencji zespół CERT Polska współpracował blisko ze Stałym Przedstawicielstwem RP przy Unii Europejskiej w celu skutecznego reprezentowania interesów Polski w negocjacjach legislacyjnych, wymianie wiedzy eksperckiej oraz promowaniu polskich rozwiązań w zakresie cyberbezpieczeństwa na forum unijnym.

Uczestniczyliśmy również w pracach nad Cyber Blueprint, dokumentem określającym nowe ramy zarządzania kryzysami cyfrowymi, który został przyjęty w czerwcu 2025 roku. Dokument ten wyznacza wspólne procedury reagowania na poważne incydenty cyfrowe w Unii Europejskiej i stanowi ważny punkt odniesienia w budowie odporności cyfrowej Unii. Nowa wersja Cyber Blueprint to pierwsza kompleksowa aktualizacja tego dokumentu od 2017 roku. Uwzględniono w niej aspekty praktyczne i operacyjne oraz zmiany wynikające z dyrektywy NIS 2 oraz wielu innych aktów prawnych. Pełny tekst dokumentu znajduje się na stronie: https://eur-lex.europa.eu/eli/C/2025/3445/oj/pol.

Wydarzenia towarzyszące

Zespół CERT Polska angażował się w wymianę doświadczeń między krajowymi i europejskimi instytucjami podczas warsztatów, paneli i sesji eksperckich, a także w trakcie kluczowych wydarzeń polskiej prezydencji, takich jak konferencja dla sektora zdrowia „Bezpieczeństwo zdrowotne – wyzwania, innowacje, przyszłość”, która odbyła się 8 kwietnia w Krakowie.

SECURE International Summit

W dniach 3–4 kwietnia 2025 roku w Bydgoszczy odbył się SECURE International Summit – specjalna edycja flagowej konferencji CERT Polska, zorganizowana w odpowiedzi na potrzebę rozwijania międzynarodowej współpracy w obszarze cyberbezpieczeństwa.

Przeszło 700 gości, ponad 30 paneli i wystąpień, szerokie grono ekspertów – tak w liczbach wyglądała największa konferencja poświęcona cyberbezpieczeństwu w ramach polskiej prezydencji w Radzie Unii Europejskiej. Jej uczestnicy wzięli udział w dyskusjach w gronie krajowych i międzynarodowych ekspertów o inicjatywach, projektach, najlepszych praktykach i trendach w cyberprzestrzeni. Integralną częścią wydarzenia były także warsztaty, które pozwalały na rozwinięcie praktycznych umiejętności technicznych.

Europejski wymiar spotkania

Program konferencji uwzględniał główne priorytety Polski i Unii Europejskiej w obszarze cyberbezpieczeństwa. Wśród prelegentów byli goście z zagranicy, reprezentujący zarówno instytucje europejskie, jak i krajowe organy budujące bezpieczeństwo w państwach członkowskich. Na scenie pojawili się m.in.: Christiane Kirketerp de Viron (Komisja Europejska), Hans de Vries (ENISA), Catherine Godin (Ambasada Kanady w Polsce) czy Stefania Ducci (Włoska Narodowa Agencja Cyberbezpieczeństwa – ACN). Polski rząd podczas tego wydarzenia reprezentował wicepremier i minister cyfryzacji Krzysztof Gawkowski.

Nie zabrakło rozmów o przyszłej, wspólnej strategii reagowania na cyberzagrożenia w Unii Europejskiej. Taka strategia to konieczność, bo incydenty są realnym zagrożeniem i mogą mieć wielkoskalowy charakter. Warto zauważyć, że dyskusja, która odbyła się w trakcie SECURE, miała przełożenie na ostateczny kształt regulacji w tym obszarze. Kilka tygodni później została przyjęta nowa wersja Cyber Blueprint, czyli właśnie planu działania w obliczu dużych incydentów o europejskim zasięgu. To pierwsza kompleksowa aktualizacja tego dokumentu od 2017 roku, a więcej na ten temat piszemy w rozdziale o polskiej prezydencji w Radzie Unii Europejskiej (→ s. 97–99).

Raport roczny CERT Polska – wyczekiwana premiera

Ataki, trendy, narzędzia. Premiera raportu rocznego CERT Polska na trwałe wpisała się w agendę SECURE. Marcin Dudek, szef naszego zespołu, informował uczestników konferencji o wnioskach zawartych w raporcie, a także o tym, jak wyglądał w ubiegłym roku krajobraz zagrożeń w polskiej cyberprzestrzeni. Tego samego dnia, gdy raport otrzymali uczestnicy konferencji, został on także opublikowany na stronie internetowej cert.pl.

Różnorodne tematy – jeden cel

W programie nie zabrakło również dyskusji o cyberwyzwaniach związanych z rozwojem sztucznej inteligencji, nowych regulacjach prawnych w tym obszarze czy o kwestiach dotyczących dezinformacji. Różnorodność w agendzie była celowa. Zależało nam, by zaprezentować treści, które będą atrakcyjne dla specjalistów ds. cyberbezpieczeństwa w obszarach zarządczych, technicznych, prawnych oraz dla pozostałych osób odpowiedzialnych za tę tematykę w instytucjach publicznych i firmach prywatnych.

SECURE International Summit czerpał z wieloletniej tradycji – konferencje SECURE od ponad ćwierć wieku skupiają ekspertów z branży cyberbezpieczeństwa. W kolejnej edycji wydarzenia, zaplanowanej na kwiecień 2026 roku,

chcemy powrócić do korzeni – dyskusja odbędzie się w Warszawie, a jej tematyka obejmie przede wszystkim zagadnienia techniczne.

Edukacja i promocja cyberbezpieczeństwa budują świadomość Polaków

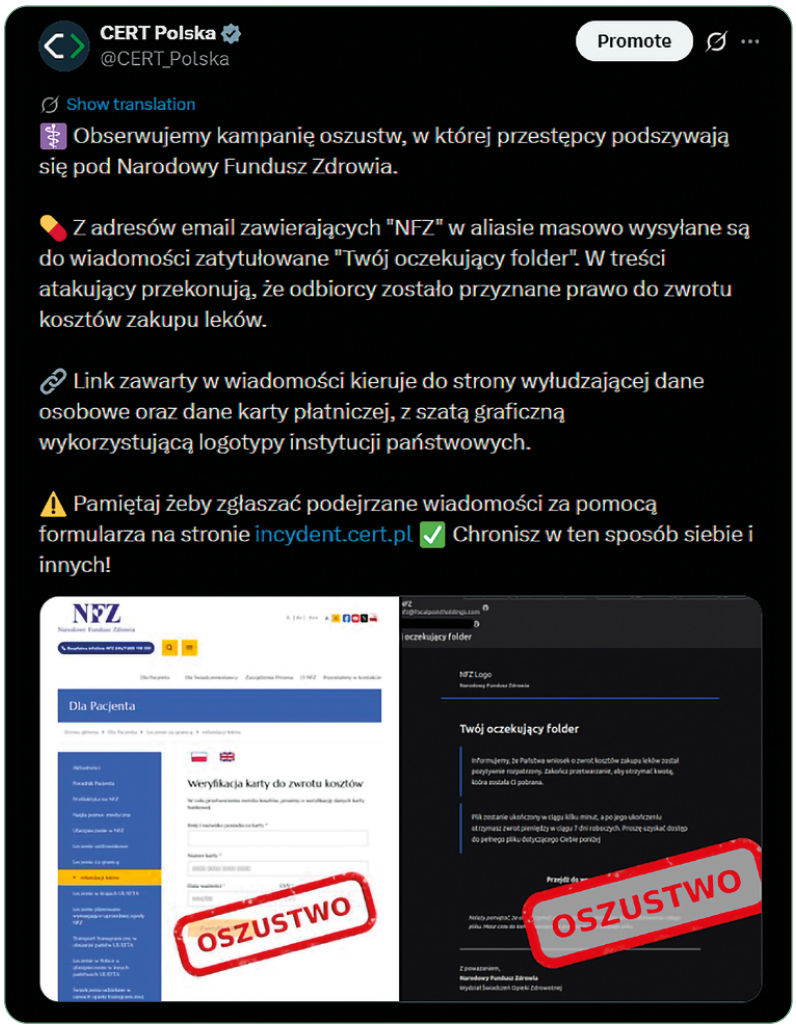
Artykuły na temat działań edukacyjnych w ostatnich raportach rocznych rozpoczynały się informacją, że odnotowujemy kolejne rekordy w liczbie zarejestrowanych zgłoszeń i incydentów. W 2025 roku było podobnie – 658,3 tys. zgłoszeń i 260,8 tys. incydentów to dane, które pokazują skalę codziennej pracy naszego zespołu. Wynika z nich, że średnia miesięczna liczba zgłoszeń przetwarzanych przez CERT Polska w 2025 roku wynosiła blisko 55 tys. Ten imponujący wzrost świadomości i gotowości do zgłaszania nam zagrożeń to także efekt działań z obszaru edukacji i promocji. Myślimy tu zarówno o kampaniach medialnych, jak i o obecności ekspertów podczas wydarzeń branżowych.

Social media – chcemy docierać szeroko

Nasza aktywność w mediach społecznościowych to dziś konieczność, bo chcemy docierać z treściami dotyczącymi cyberbezpieczeństwa jak najbliżej odbiorcy. Kluczowe dla budowania świadomości zarówno zagrożeń, jak i konieczności ich zgłaszania, są systematycznie wydawane ostrzeżenia. Dotyczą one największych kampanii oszustw i są publikowane równolegle na profilach CERT Polska na Facebooku, X oraz LinkedInie. Uzupełniamy je powiadomieniami push wysyłanymi za pośrednictwem aplikacji mObywatel. Stanowią one element usługi Bezpiecznie w sieci, która umożliwia zgłoszenie incydentu, otrzymywanie powiadomień o aktualnych cyberzagrożeniach, a dzięki artykułom o bezpiecznym poruszaniu się w internecie – także aktualizowanie wiedzy.

Poza ostrzeżeniami wydawanymi wówczas, gdy pojawia się konieczność, w kanałach social media publikowane są także cykle edukacyjne. Już kolejny raz zaproponowaliśmy naszym użytkownikom serię postów świątecznych. #CyberPrezent to 12 krótkich tekstów o systemach bezpieczeństwa, aktualnych zagrożeniach, ale także o sposobach, jak tym zagrożeniom zapobiegać. Przywołując kolejno wyzwania związane m.in. z wyciekami danych czy phishingiem, dawaliśmy naszym czytelnikom rady, jak z nimi walczyć.

RYSUNEK 37. Ostrzeżenie opublikowane w serwisie X

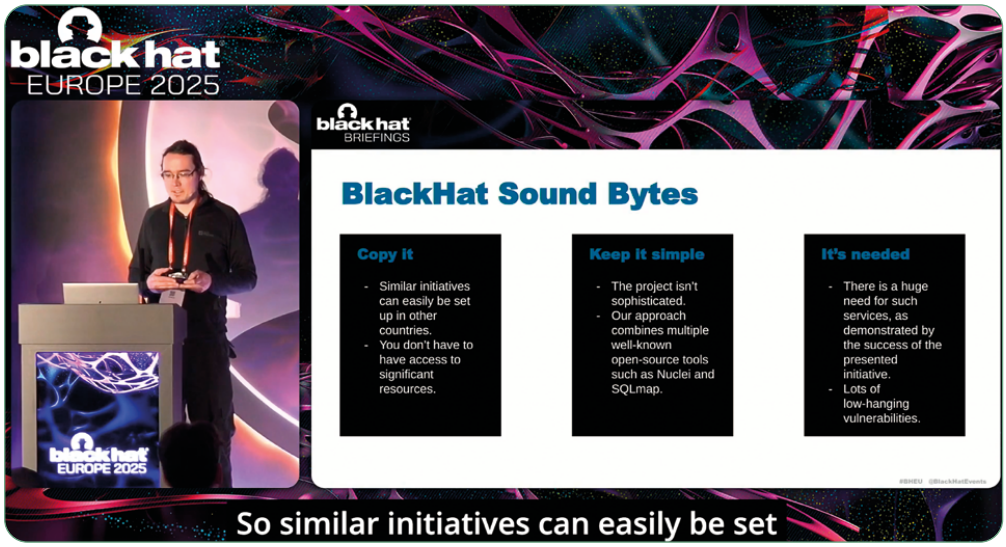


RYSUNEK 38. Ilustracja wykorzystywana do promocji cyklu #CyberPrezent w social mediach

Udział w konferencjach – budujemy ekspercki wizerunek

Działania edukacyjne wymienione powyżej uzupełnialiśmy obecnością na kluczowych konferencjach branżowych, takich jak Black Hat Europe w Londynie czy Oh My Hack w Warszawie. W Londynie Krzysztof Zając zaprezentował serwis moje.cert.pl, a podczas OMH mówiliśmy o wykrywaniu złośliwych plików i wykorzystywaniu AI do wyszukiwania podatności oraz w procesie fuzzingu. Było też o komunikacji incydentów i skanowaniu stron internetowych na naprawdę dużą skalę. Uczestniczyliśmy również w spotkaniach TF-CSIRT i targach pracy, braliśmy udział w międzynarodowych konkursach oraz ćwiczeniach (które także w tym raporcie opisujemy), a także wspieraliśmy merytorycznie uczestników hackathonów.

RYSUNEK 39. Fragment prezentacji z konferencji Black Hat Europe



W kontekście zawodów nie sposób nie wspomnieć o organizacji European Cybersecurity Challenge (ECSC). Blisko 400 młodych osób z całego świata przez dwa dni rywalizowało w Warszawie o tytuł najlepszych. To prestiżowe wydarzenie miało na celu przede wszystkim wzmocnienie międzynarodowej współpracy w cyberbezpieczeństwie oraz promocję tej dziedziny wśród młodych osób, które stoją u progu wyboru swojej ścieżki zawodowej. Zawody miały również zwiększyć potencjał obronny, edukacyjny oraz innowacyjny w tej kluczowej dziedzinie. Działaniami promocyjnymi wokół ECSC staraliśmy się dotrzeć do szerszego grona odbiorców, w tym młodzieży, studentów oraz specjalistów z innych branż, podkreślając wagę bezpiecznego korzystania z technologii. Więcej na temat ECSC 2025 piszemy w artykule na s. 95–97.

Artykuły i kampanie medialne – całe spektrum działania!

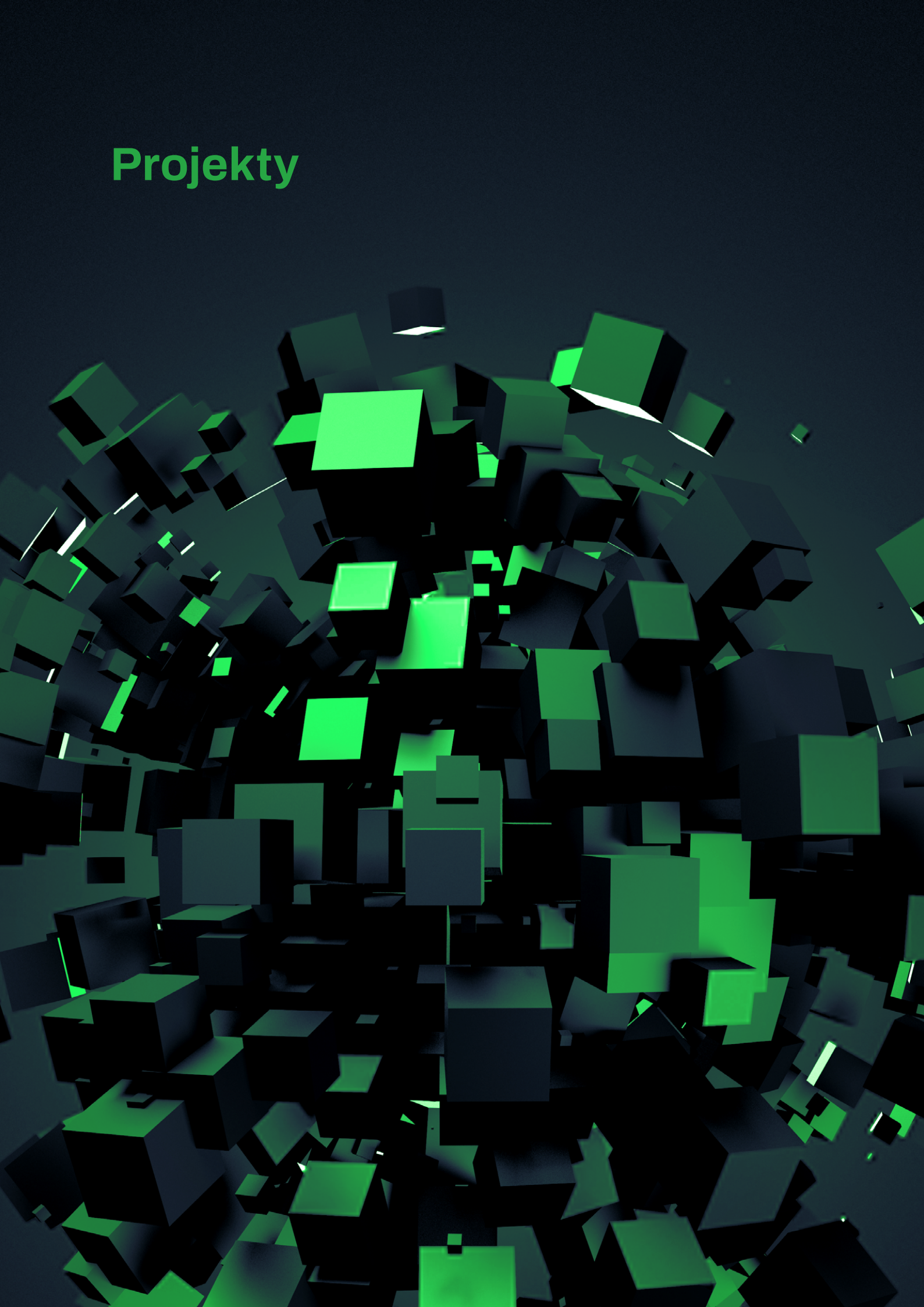
W ostatnim roku powstały też artykuły odnoszące się do aktualnych zagrożeń – opisywaliśmy m.in. złośliwe oprogramowanie NGate, odnosiliśmy się do mitów związanych z publicznym Wi-Fi, a także przybliżaliśmy działania grup APT, takie jak kampania UNC1151 wykorzystująca podatność w oprogramowaniu Roundcube do kradzieży poświadczeń.

Rozpoznawalność CERT Polska oraz znaczenie zgłaszania do nas incydentów podkreślaliśmy także w czasie ogólnopolskiej kampanii medialnej „Bezpieczny dzień". Kampania telewizyjna na antenach największych polskich telewizji – TVP, TVN i Polsat wystartowała 8 maja. Spot informacyjny z Markiem, który zgłasza niebezpieczne treści, by chronić innych, trafił do milionów odbiorców.

RYSUNEK 40. Fragment reklamy emitowanej podczas kampanii „Bezpieczny dzień"

Akcentowanie roli zgłaszania do nas incydentów to istotny fragment całości działań promocyjnych. Większa pula zgłoszeń to pełniejszy obraz tego, co dzieje się w cyberprzestrzeni, a dla nas możliwość skuteczniejszego działania. Takich wątków nie zabraknie także w 2026 roku, który jest dla nas szczególny. Zespół CERT Polska będzie wówczas obchodził swoje 30. urodziny, chcemy więc podkreślać to, co nam się w tym czasie udało, prezentować narzędzia i ich efekty. Już dziś zachęcamy więc do lektury przyszłorocznego raportu i obserwowania naszych działań w całym 2026 roku.

Projekty



Moje.cert.pl

12 lutego 2025 roku CERT Polska udostępnił publicznie portal moje.cert.pl, dzięki któremu każdy zarejestrowany użytkownik – od właściciela niszowego bloga aż po administratora wielu stron i systemów w dużej instytucji – może w łatwy sposób zwiększyć cyberbezpieczeństwo swoich domen czy sieci.

Po wprowadzeniu informacji o swoich domenach i sieciach, a następnie weryfikacji, że jest ich właścicielem, użytkownik otrzymuje informacje o podatnościach – od tych niskiego ryzyka, takich jak niepoprawna konfiguracja SSL/TLS, aż po bardzo poważne, takie jak możliwość zdalnego wykonania kodu. Dodatkowo serwis moje.cert.pl automatycznie powiadamia o wyciekach haseł, m.in. spowodowanych obecnością szkodliwego oprogramowania wykradającego hasła z komputera użytkownika, oraz daje możliwość pobrania informacji o różnych zdarzeniach sieciowych, np. gdy serwer stanie się częścią botnetu czy będzie udostępniać szkodliwe treści.

Skanowanie bezpieczeństwa odbywa się cyklicznie – w zależności od zapotrzebowania organizacji miesiąc, dwa lub cztery miesiące po zakończeniu poprzedniego skanowania. Podczas testów CERT Polska korzysta z systemu Artemis (więcej informacji na s. 107–109), który wykrywa dużą liczbę podatności i błędnych konfiguracji wpływających na bezpieczeństwo. Zdarzenia sieciowe są pobierane z systemu n6 (więcej na s. 126–142). Z kolei dane na temat wycieków haseł umieszczone w systemie moje.cert.pl pochodzą ze źródeł komercyjnych, takich jak Intelligence X, a także są wzbogacane zbiorami z własnych działań operacyjnych CERT Polska oraz z działań operacyjnych innych zespołów CSIRT, np. CSIRT KNF.

W serwisie – w zakładce „Komunikaty” – są na bieżąco zamieszczane ostrzeżenia skierowane do administratorów i użytkowników internetu dotyczące zagrożeń w polskiej cyberprzestrzeni. Komunikaty zawierają m.in. opis trwających kampanii prowadzonych przez przestępców oraz alerty o podatnościach. Dostęp do tych treści mają wszyscy zainteresowani, nie tylko osoby zarejestrowane w serwisie. Ponadto każdy może je otrzymywać również w wiadomości e-mail.

Serwis moje.cert.pl jest wytwarzany w sposób zwinny. Wersja, która została udostępniona użytkownikom w lutym 2025 roku, nie była wersją ostateczną. Serwis został upubliczniony niedługo po uruchomieniu wersji testowej, dlatego dość szybko mogliśmy zweryfikować, czy odpowiada on na potrzeby użytkowników, a także dowiedzieć się, jakie zmiany powinniśmy wprowadzić. Dzięki temu dalszy rozwój projektu uwzględniał potrzeby zgłaszane przez użytkowników, dotyczące zarówno usprawnień, jak i nowych funkcji portalu moje.cert.pl.

W 2025 roku w ramach rozwoju projektu dodaliśmy m.in.:

- publikację komunikatów bezpieczeństwa oraz dostarczanie ich za pomocą wiadomości e-mail, a także możliwość ich odczytu przez interfejs webowy czy RSS,
- API umożliwiające integrację innych systemów z portalem,
- funkcje umożliwiające rejestratorom domen .pl skanowanie bezpieczeństwa domen swoich klientów w ramach projektu Twoja Bezpieczna Strona,
- funkcje umożliwiające, za zgodą podmiotów, sektorowym zespołom CSIRT dostęp do informacji na temat infrastruktury i podatności podmiotów z ich sektora. Funkcje te są obecnie wykorzystywane przez zespół CSIRT KNF. W przyszłości zostaną udostępnione również pozostałym sektorowym zespołom cyberbezpieczeństwa.

Portal cieszy się dużą popularnością wśród użytkowników, co świadczy o tym, że doceniają oni jego funkcjonalności. Do końca 2025 roku w serwisie zarejestrowało się ponad 15 tys. użytkowników i dodało ponad 18 tys. domen. Szczegółowe statystyki prezentujemy w dalszej części raportu (→ s. 122).

Serwis moje.cert.pl był prezentowany na licznych konferencjach, zarówno krajowych: SECURE International Summit w Bydgoszczy, Security Case Study i Oh My Hack w Warszawie, jak i zagranicznych: TF-CSIRT w Oslo, NatCSIRT w Kopenhadze i Black Hat Europe w Londynie. Mamy nadzieję, że promocja naszego rozwiązania na forum międzynarodowym zachęci zespoły CSIRT w innych krajach do budowy analogicznych rozwiązań.

Artemis

Od 2023 roku system Artemis bada strony internetowe i inne systemy, takie jak np. poczta elektroniczna, w poszukiwaniu podatności bezpieczeństwa i błędów konfiguracyjnych. Za rozwój tego narzędzia odpowiada zespół CERT Polska. Regularne skanowanie systemów pozwala monitorować i poprawiać poziom ich bezpieczeństwa. Uzyskane wyniki nie są podawane do publicznej wiadomości. Są one przekazywane administratorom, dzięki czemu zyskują oni cenne informacje, które mogą wykorzystać do poprawy bezpieczeństwa systemów, którymi zarządzają, a przez to uniemożliwić atakującym wykorzystanie wykrytych problemów. Weryfikacji podlegają przede wszystkim podmioty we właściwości CSIRT NASK. Od 2024 roku podmioty nieobjęte skanowaniem mogą samodzielnie zlecić sprawdzanie swoich domen i sieci w serwisie moje.cert.pl.

System Artemis jest stale rozwijany. Wśród zmian, które wprowadziliśmy w 2025 roku, można wymienić:

- funkcję identyfikacji zasobów, tj. subdomen, adresów IP, technologii i wersji technologii powiązanych ze skanowaną stroną, co umożliwia m.in. prezentację tych informacji w ramach portalu moje.cert.pl,
- możliwość modyfikacji konfiguracji konkretnego skanowania, np. przez zwiększenie liczby wykonywanych testów czy włączenie dodatkowych modułów – dokładniejsze i dłuższe testy mogą być prowadzone m.in. w przypadku domen o większym znaczeniu, np. subdomen gov.pl,
- kolejne moduły wykrywające podatności typu Local File Inclusion, Server-Site Request Forgery, Server-Side Template Injection, Remote Code Execution itd.,
- moduł wykrywający możliwość ominięcia blokady dostępu przez kod odpowiedzi 403 Forbidden,
- moduł sprawdzający, czy do systemu można zalogować się prostym hasłem,
- moduł sprawdzający, czy domena kieruje na niewykorzystywany adres IP, co może skutkować tym, że ten adres IP zostanie wykupiony przez innego użytkownika, a w konsekwencji w danej domenie będą hostowane treści kontrolowane przez inną osobę,
- liczne zmiany zwiększające szybkość i stabilność skanowania.

Duży wpływ na rozwój systemu Artemis miało publiczne udostępnienie przez CERT Polska serwisu moje.cert.pl, w którym wszyscy chętni mogą skorzystać z bezpłatnego skanowania swoich domen i sieci za pomocą tego systemu. W związku z tym konieczne było przyspieszenie działania systemu i dostosowanie go do wymagań serwisu, ponieważ liczba wykrywanych podatności wzrosła ponad dwukrotnie.

W 2025 roku CERT Polska stale prowadził cykliczne skanowania instytucji publicznych, takich jak szkoły, szpitale czy uczelnie, dlatego ważnym obszarem naszych działań były czynności związane z administracją systemem, rozwiązywaniem powstających problemów i odpowiadaniem na pytania skanowanych instytucji. Szczegółowe statystyki dotyczące prowadzonych skanowań prezentujemy w dalszej części raportu (→ s. 123–125).

System Artemis jest oprogramowaniem open source, dostępnym w serwisie GitHub pod adresem https://github.com/CERT-Polska/Artemis. Dzięki temu jest on wykorzystywany przez inne zespoły CSIRT, zarówno krajowe, jak i zagraniczne, i może być rozwijany przez zewnętrznych kontrybutorów. Najważniejszym z nich w 2025 roku był Abhinav Karn, który rozwijał system w ramach programu Google Summer of Code i jest autorem części modułów wymienionych powyżej.

W 2025 roku system Artemis prezentowaliśmy na licznych konferencjach, zarówno krajowych, jak i zagranicznych, m.in. na konferencji Black Hat Europe w Londynie, FIRST w Kopenhadze i Oh My Hack w Warszawie.

Snitch

Dostępność w internecie urządzeń OT/IoT może rodzić poważne konsekwencje dla cyberbezpieczeństwa instytucji, w których są one stosowane. Dotyczy to również systemów IT, na które regularnie pojawiają się nowe podatności. Snitch pozwala automatycznie monitorować ekspozycję z wykorzystaniem serwisów Shodan, Zoomeye, FOFA i n6. Następnie raportuje drogą mailową oraz zapisuje w bazie n6, powiadamiając osoby odpowiedzialne za te systemy.

Nowe źródła danych kontaktowych

W roku 2025 system Snitch zaczął wykorzystywać nowe źródła kontaktów. Oprócz bazy RIPE wykorzystywane są baza kontaktów CERT Polska oraz dane z serwisu moje.cert.pl. Pozwala to dotrzeć do administratorów odpowiedzialnych za wykryte podatne systemy. A zwłaszcza do tych, którym zależy na byciu informowanym.

Jeżeli chcą Państwo otrzymywać powiadomienia z systemu Snitch, zalecamy zweryfikować swoją podsieć w serwisie moje.cert.pl. Będą wtedy Państwo informowani bezpośrednio ze Snitcha mailowo, a powiadomienia będą widoczne także w widoku „Zdarzenia sieciowe” w moje.cert.pl.

Statystyki raportowania

W 2025 roku nasz zespół wytworzył wiele nowych reguł wykrywających najpopularniejsze rozwiązania IT/OT oraz takie, które zawierały podatności krytyczne publikowane w ciągu roku. Dla systemów OT liczba reguł wzrosła o 50%, a dla systemów IT – o 170% względem stanu na koniec roku 2024. Jeśli porównamy liczbę wysłanych powiadomień, dla OT wynik był wyższy o 90%, podczas gdy dla IT wynik wzrósł o 420%. Dzięki zwiększonej liczbie reguł dla systemów IT udało się zidentyfikować znacznie więcej podatnych usług. Nie zostało to uwzględnione w statystykach dotyczących powiadomień wysłanych przez Snitcha z uwagi na częściowe wysyłanie powiadomień dotyczących IT przez inne systemy CERT Polska.

TABELA 4. Statystyki Snitcha z podziałem na systemy OT i IT

Liczba	OT	Różnica*	IT	Różnica*	Unikalna suma*
Reguły	**90**	1,5	**194**	2,7	284
Unikalne hosty	**8367**	1,9	**42 856**	1,6	50 997
Unikalne usługi	**10 135**	1,5	**47 146**	1,7	57 280
Wysłane powiadomienia	**22 045**	1,9	**21 739**	5,2	43 784

* Różnica względem roku 2024. W statystykach są hosty, które równocześnie należą do kategorii IT i OT, stąd dodatkowa kolumna z unikalną sumą.

Średnia arytmetyczna przyrostów w roku 2025 wynosi 2,2 w porównaniu z rokiem poprzednim.

AIPITCH

Projekt AIPITCH (AI-Powered Innovative Toolkit for Cybersecurity Hubs), w którym CERT Polska uczestniczy z ramienia NASK–PIB, ma na celu wytworzenie narzędzi wykorzystujących sztuczną inteligencję do lepszej ochrony polskiej cyberprzestrzeni. Jest to projekt trzyletni, a prace prowadzone w jego ramach rozpoczęły się w 2025 roku.

Konsorcjum, do którego oprócz NASK–PIB należą także: Narodowe Centrum Badań Jądrowych (NCBJ), nasz odpowiednik w Luksemburgu – CIRCL (Computer Incident Response Center Luxembourg), włoski ABI Lab oraz Fundacja Shadowserver, prowadzi badania, których rezultatem ma być usprawnienie działań zespołów operacyjnych odpowiedzialnych za cyberbezpieczeństwo poprzez integrację nowych funkcji zapewnianych przez AI z kluczowymi narzędziami i procesami.

AIPITCH koncentruje się na budowie narzędzi wspierających kluczowe zadania operacyjne, w szczególności wczesne wykrywanie zagrożeń i usprawnienie procesów analitycznych. Projekt obejmuje m.in. opracowanie systemów wczesnego ostrzegania przed nowymi atakami na usługi dostępne w internecie czy przed phishingiem, przeprowadzanie automatycznej analizy dużych wolumenów danych z różnych źródeł informujących o zagrożeniach z zakresu cyberbezpieczeństwa, a także prace nad chatbotem AI ułatwiającym użytkownikom zgłaszanie incydentów. Istotnym elementem jest także integracja narzędzi wykorzystujących AI z wewnętrznymi systemami monitorowania sieci i platformami wspierającymi reagowanie na incydenty.

Pierwsze narzędzia wytworzone w projekcie wejdą do użycia w 2026 roku.

Projekt jest współfinansowany przez Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), program „Cyfrowa Europa”, numer grantu: 101190545.

Dofinansowane przez Unię Europejską

PERUN

W październiku 2025 roku rozpoczął się projekt PERUN (Protecting Sensitive Cyber Ecosystems from Upcoming Next Generation and AI-generated Malware Threats). Projekt jest ukierunkowany na wykrywanie i zwalczanie złośliwego oprogramowania, w tym malware generowanego przez AI, które omija tradycyjne mechanizmy detekcji oparte na sygnaturach. W ramach projektu zostaną opracowane metody i narzędzia na wysokim poziomie dojrzałości technologicznej, przeznaczone do praktycznego wdrożenia m.in. w jednostkach typu SOC, CSIRT oraz w sieciach badawczo-edukacyjnych. Rozwiązania zostaną pilotażowo wdrożone w podmiotach należących do sektorów kluczowych, takich jak energetyka.

Międzynarodowe konsorcjum składa się z jednostek badawczych i firm z Niemiec, Polski, Rumunii, Francji, Włoch, Hiszpanii, Belgii i Szwajcarii. Główne zadania naszego zespołu to rozwój narzędzia DRAKVUF Sandbox oraz testowanie i integracja rozwiązań wspomagających analizę złośliwego oprogramowania opracowanych przez partnerów. Prace w ramach projektu są zaplanowane na 3 lata (2025–2028), a ich efekty zostaną wykorzystane w pracy operacyjnej CERT Polska.

Projekt jest współfinansowany przez Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), program „Horyzont Europa”, numer grantu: 101225653. Wyrażone poglądy i opinie są wyłącznie poglądami autorów i nie odzwierciedlają oficjalnego stanowiska UE ani ECCC. Unia Europejska ani instytucja udzielająca grantu nie ponoszą za nie odpowiedzialności.

Dofinansowane przez Unię Europejską

FETTA

Zespół CERT Polska w 2025 roku kontynuował prace w ramach projektu Federated European Team for Threat Analysis (Europejski Zespół Analizy Zagrożeń, FETTA). Realizujemy go wspólnie z zespołem będącym naszym odpowiednikiem w Luksemburgu – CIRCL (Computer Incident Response Center Luxembourg). Głównym celem projektu jest dostarczanie dokładniejszych informacji o zagrożeniach cyberbezpieczeństwa (ang. Cyber Threat Intelligence, CTI), które będą służyć podmiotom w Polsce, Luksemburgu, a także – poprzez Sieć CSIRT – w innych krajach Unii Europejskiej. W zakres projektu wchodzi opracowanie nowych i udoskonalenie już istniejących raportów sytuacyjnych oraz rozwój narzędzi do zbierania i analizy danych związanych z cyberbezpieczeństwem.

Rozwój platformy n6

Istotną częścią projektu jest rozwój n6: naszej platformy do dystrybucji danych o zagrożeniach i incydentach cyberbezpieczeństwa, której kod udostępniamy na otwartej licencji. Główna instancja n6, utrzymywana przez CERT Polska, posiada ponad tysiąc zarejestrowanych podmiotów, które bezpłatnie otrzymują informacje dotyczące swoich sieci. Oprócz tego dane są również udostępniane poprzez serwis moje.cert.pl.

Najważniejszym rezultatem prac prowadzonych w 2025 roku było wzbogacenie portalu o kontekstową informację, tak aby użytkownicy mogli szybciej zinterpretować zdarzenia dotyczące ich infrastruktury i reagować na nie bez konieczności ręcznego przeszukiwania zewnętrznych źródeł. Dla zdarzeń zawierających identyfikatory CVE dodano integrację z European Union Vulnerability Database (EUVD) w celu prezentowania wiarygodnego opisu podatności, a w przypadkach, kiedy dostępne są rekomendacje CERT Polska – zapewniono szybkie przejście do właściwych komunikatów technicznych w serwisie moje.cert.pl. Równolegle uruchomiono w portalu bazę wiedzy obejmującą setki najczęściej występujących typów zagrożeń, m.in. podatności, malware, błędne konfiguracje, ataki na usługi sieciowe.

Pozostałe prace objęły rozszerzenie i utrzymanie źródeł danych, usprawnienia użyteczności portalu (filtrowanie, wyszukiwanie, eksport), ulepszenie funkcji Single-Sign-On (SSO), co pozwoliło na integrację z systemami wykorzystywanymi przez europejską Sieć CSIRT (platforma narzędzi MeliCERTes), aktualizacje dokumentacji oraz optymalizacje wydajności i zwiększenie niezawodności.

Statystki dotyczące zdarzeń przetworzonych przez platformę n6 przedstawiliśmy w ostatniej części niniejszego raportu (→ s. 126–142). Publiczne wydania n6 dostępne są w serwisie GitHub: https://github.com/CERT-Polska/n6.

Pozostałe działania

W 2025 roku kontynuowaliśmy rozwój produktów CTI, w szczególności raportów cyklicznych dotyczących bieżących zagrożeń (APT, ransomware, haktywiści). Przygotowaliśmy z CIRCL pierwszy wspólny raport CTI na temat najistotniejszych podatności za rok 2024, metodyki ich oceny oraz o sposobach identyfikacji narażonych instancji i udostępniliśmy go Sieci CSIRT. Natomiast we współpracy z Centrum Badań i Rozwoju NASK–PIB przeprowadziliśmy analizę krajobrazu botnetów IoT/Linux.

Przeprowadziliśmy również szereg warsztatów eksperckich dla analityków z obu zespołów, które przełożyły się na wymianę know-how i informacji operacyjnych, a także na nakreślenie wspólnych kierunków badań i rozwoju narzędzi.

Projekt jest współfinansowany przez Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), program „Cyfrowa Europa", numer grantu: 101128030. CERT Polska jest liderem konsorcjum. Wyrażone poglądy i opinie są wyłącznie poglądami autorów i nie odzwierciedlają oficjalnego stanowiska UE ani ECCC. Unia Europejska ani instytucja udzielająca grantu nie ponoszą za nie odpowiedzialności.

DNS4EU

W grudniu 2025 roku zakończyliśmy prace w projekcie DNS4EU, którego celem było uruchomienie bezpiecznego europejskiego serwera DNS. Projekt był współfinansowany przez Komisję Europejską i odzwierciedlał jej dążenia do zapewnienia suwerenności cyfrowej Unii Europejskiej.

Projekt realizowało międzynarodowe konsorcjum tworzone przez Whalebone (Czechy, lider), CZ.NIC (Czechy), Politechnikę Czeską w Pradze (Czechy), Time.lex (Belgia), deSEC (Niemcy), HUN-REN Sztaki (Węgry), ABILAB (Włochy), DNSC (Rumunia) oraz NASK–PIB (Polska).

Głównym rezultatem projektu było uruchomienie w czerwcu 2025 roku publicznej usługi DNS. Jest ona ogólnodostępna i darmowa. Zapewnia 5 różnych konfiguracji bezpieczeństwa.

Są to:

- Ochrona przed złośliwymi domenami,
- Ochrona przed złośliwymi domenami + Ochrona dzieci,
- Ochrona przed złośliwymi domenami + Blokowanie reklam,
- Ochrona przed złośliwymi domenami + Ochrona dzieci + Blokowanie reklam,
- DNS bez filtrowania.

W ramach projektu NASK–PIB opracował rozwiązania wykrywające domeny phishingowe w celu zapewnienia większego poziomu bezpieczeństwa użytkowników usługi. Zadanie te realizował CERT Polska wspólnie z Centrum Badań i Rozwoju. W naszych pracach skupiliśmy się na dwóch koncepcjach detekcji domen phishingowych: przez wykorzystanie danych z rejestru .pl oraz przez analizę zapytań DNS od użytkowników. Opisaliśmy obie koncepcje w raporcie rocznym za 2024 rok, poniżej prezentujemy podsumowanie uzyskanych wyników.

Wykrywanie domen phishingowych na podstawie danych z rejestru domen

W listopadzie 2024 roku uruchomiliśmy system wczesnego wykrywania domen phishingowych w domenie .pl oparty na uczeniu maszynowym. Stał się on częścią naszego środowiska detekcji phishingu, które jest odpowiedzialne za identyfikację domen wpisywanych na Listę Ostrzeżeń. Nasz system wykorzystuje dane z rejestru domen .pl do identyfikacji podejrzanych domen chwilę po ich rejestracji w celu skrócenia czasu reakcji naszego zespołu.

Dzięki monitorowaniu nowych rejestracji domen niemal w 80% przypadków nasz system był w stanie zidentyfikować domeny phishingowe szybciej niż inne źródła informacji, z których korzystaliśmy. Dodatkowo ok. 14% domen phishingowych, znalezionych przez system, nie powtórzyło się w innych źródłach, co świadczy o tym, że system umożliwia uzyskanie unikalnych informacji operacyjnych. Zaobserwowaliśmy również, że system pomaga odkryć domeny, które zostały przeoczone przy stosowaniu innych metod, np. ze względu na brak dowodów na obecność zawartości phishingowej. W tych przypadkach identyfikacja przez nasz system umożliwiła wytypowanie domen do powtórnej, pogłębionej analizy.

Opracowany system wczesnego wykrywania identyfikuje domeny phishingowe, które po weryfikacji trafiają na Listę Ostrzeżeń. Chronią tym samym internautów w Polsce dzięki integracji Listy przez głównych polskich dostawców internetu, ale także użytkowników w dowolnym miejscu na świecie korzystających z serwerów DNS4EU.

Analiza zapytań DNS

Analiza zanonimizowanych zapytań DNS do serwerów DNS4EU zaowocowała opracowaniem dwóch systemów detekcji domen phishingowych. Pierwszy system analizuje nazwy domenowe pod względem językowym, natomiast w drugim badane są zależności czasowe zapytań. System detekcji bazujący na nazwach domenowych wykorzystuje różne modele językowe do tworzenia tzw. zanurzeń (embeddings), czyli reprezentacji słów w postaci zrozumiałej przez algorytmy uczenia maszynowego: FastText[47] i Llama[48]. Pierwszy model jest używany do szybkiej filtracji domen, natomiast to drugi zapewnia wysoką jakość detekcji.

Drugi z systemów detekcji analizuje zależności czasowe między zapytaniami DNS w celu odkrycia współwystępowań pomiędzy znanymi domenami phishingowymi a innymi domenami. Identyfikacja silnych zależności umożliwia wykrycie nieznanych wcześniej domen phishingowych. Testy potwierdziły skuteczność tego podejścia w odnajdywaniu nieznanego phishingu.

Głównym wyzwaniem dla obu systemów jest fakt, że dla wielu zidentyfikowanych domen trudno znaleźć dowód na to, że są używane do phishingu. Niestety często wytypowanie samej domeny nie wystarczy, by jednoznacznie określić, czy są na niej złośliwe treści. Na przykład bez pełnego adresu URL – którego nie można zaobserwować na poziomie DNS – zazwyczaj nie da się odnaleźć treści phishingu, a tym samym w pełni potwierdzić, czy domena została poprawnie zaklasyfikowana przez nasze systemy.

Więcej o projekcie

Aktualności oraz szczegółowe informacje o DNS4EU, w tym instrukcja konfiguracji usługi, znajduje się na oficjalnej stronie projektu: www.joindns4.eu.

Mimo zakończenia głównej części projektu kontynuujemy współpracę w ramach DNS4EU – analizujemy dane z zapytań DNS i przekazujemy informacje o wykrytych złośliwych domenach.

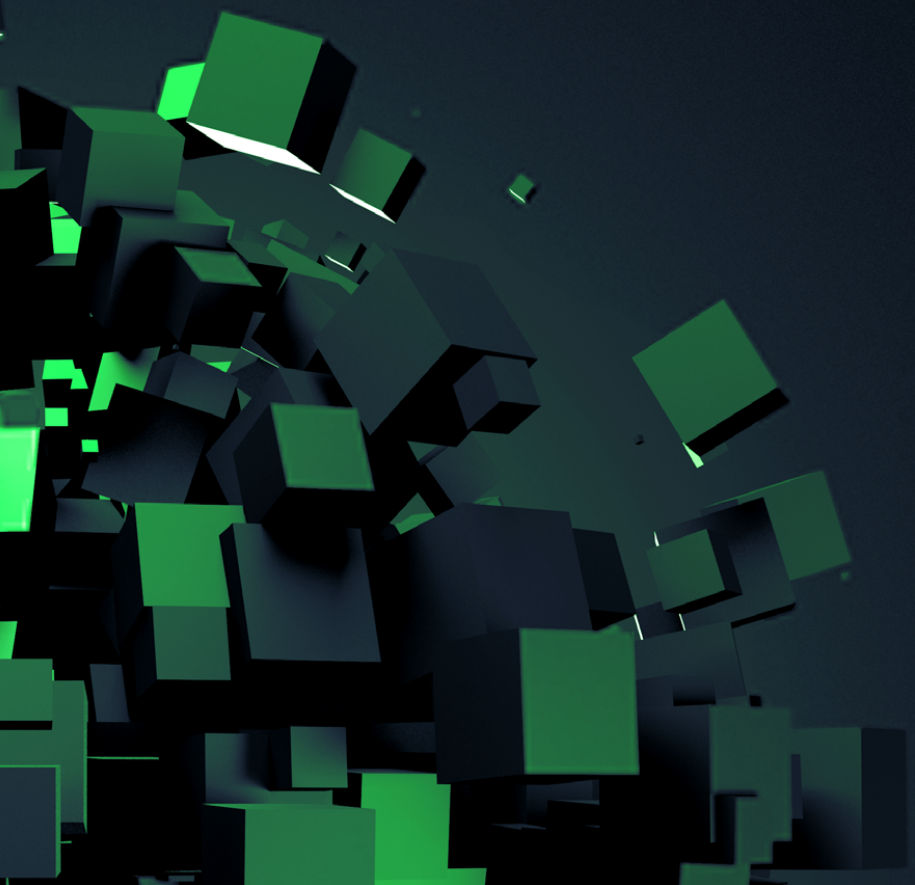
Projekt współfinansowany przez Unię Europejską. Numer grantu: 101095329 21-EU-DIG-EU-DNS, pełna nazwa projektu to: DNS4EU and European DNS Shield.

Dofinansowane przez Unię Europejską

47 https://fasttext.cc/

48 https://www.llama.com/

Statystyki



Zgłoszenia i incydenty

W 2025 roku zespół CERT Polska otrzymał 658 320 zgłoszeń, które zostały szczegółowo przeanalizowane. Na ich podstawie zarejestrowano 260 783 unikalnych incydentów bezpieczeństwa. Są to zdarzenia, które miały lub mogły mieć negatywny wpływ na poziom cyberbezpieczeństwa.

W porównaniu z 2024 rokiem liczba zgłoszeń w 2025 roku wzrosła o 10%, natomiast liczba zarejestrowanych incydentów cyberbezpieczeństwa w 2025 roku zwiększyła się aż o 152% w stosunku do roku poprzedniego. Od wielu lat obserwujemy utrzymującą się tendencję wzrostową liczby rejestrowanych incydentów w skali roku. Wzrost liczby zgłoszeń oraz zarejestrowanych incydentów cyberbezpieczeństwa wynika m.in. z rosnącej świadomości społecznej w zakresie zagrożeń, a także z roli zespołu CERT Polska w monitorowaniu i analizowaniu incydentów cyberbezpieczeństwa oraz reagowaniu na nie. Ważnym czynnikiem wpływającym na świadomość społeczną są prowadzone działania informacyjne dotyczące występujących zagrożeń. W tabeli 5 przedstawiliśmy liczbę incydentów w latach 2018–2025.

Zgłoszenia trafiają do nas poprzez:

- formularz dostępny na stronie https://incydent.cert.pl – zgłoszenie incydentu,
- formularz dostępny na stronie https://incydent.cert.pl/domena – zgłoszenie złośliwej domeny,
- SMS pod numer 8080 – zgłoszenie podejrzanej wiadomości SMS,
- aplikację mObywatel – zgłoszenie złośliwej strony internetowej, oszustwa lub innego zdarzenia (usługa Bezpiecznie w sieci),
- e-mail: cert@cert.pl,
- tradycyjną pocztę na adres NASK–PIB.

Najczęstsze typy incydentów w 2025 roku

Oszustwa komputerowe

Najliczniejszą kategorią incydentów zarejestrowanych w 2025 roku były oszustwa komputerowe. Odnotowano 253 238 takich incydentów, co stanowiło 97% wszystkich obsłużonych zdarzeń. W porównaniu z rokiem poprzednim liczba oszustw komputerowych wzrosła o 158%.

Najczęściej występującym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, takich jak loginy i hasła do poczty elektronicznej,

serwisów bankowych, portali społecznościowych czy innych usług online (phishing). W 2025 roku odnotowano 78 391 tego typu incydentów, co stanowiło 30% wszystkich zarejestrowanych zdarzeń. Na liście oszustw komputerowych znalazły się m.in. fałszywe sklepy internetowe oraz oszustwa inwestycyjne, w których przestępcy podszywali się pod koncerny paliwowo-energetyczne, firmy, instytucje, wykorzystywali też wizerunki znanych osób. Wśród najczęściej wykorzystywanych kampanii phishingowych znalazły się przypadki nieuprawnionego użycia wizerunku serwisów sprzedażowych OLX – 28 462 zdarzenia, Allegro – 22 513 zdarzeń oraz próby pozyskania poświadczeń do skrzynek elektronicznych – 2519 zdarzeń.

Szkodliwe oprogramowanie

Drugą najczęściej występującą kategorią zagrożeń w 2025 roku było szkodliwe oprogramowanie. Zarejestrowano 3438 incydentów tego typu, które obejmowały m.in. infekcje systemów informatycznych oraz próby nieuprawnionego dostępu z wykorzystaniem szkodliwego kodu. Wśród tych zdarzeń odnotowano 179 przypadków oprogramowania szyfrującego typu ransomware, które mogło prowadzić do utraty dostępności danych lub systemów oraz generować istotne ryzyko dla ciągłości działania podmiotów dotkniętych incydentem. Incydenty związane ze szkodliwym oprogramowaniem nadal stanowią istotne zagrożenie dla bezpieczeństwa teleinformatycznego i wymagają bieżącego monitorowania oraz szybkiego reagowania.

Podatne usługi

Trzecim istotnym rodzajem zagrożeń były podatne usługi. W 2025 roku odnotowano 1732 incydenty tego typu, związane z występowaniem luk bezpieczeństwa w publicznie dostępnych usługach i systemach teleinformatycznych. Incydenty te mogły umożliwiać nieuprawniony dostęp do zasobów, eskalację uprawnień lub zakłócenie działania usług. Zdarzenia związane z podatnymi usługami podkreślają znaczenie regularnych aktualizacji oprogramowania, właściwej konfiguracji systemów oraz bieżącego monitorowania stanu bezpieczeństwa infrastruktury teleinformatycznej.

W tabeli 7 przedstawiliśmy statystyki z podziałem na kategorie incydentów.

Ustawa o krajowym systemie cyberbezpieczeństwa

W 2025 roku CSIRT NASK w ramach ustawy o krajowym systemie cyberbezpieczeństwa obsłużył 27 incydentów zaklasyfikowanych jako poważne. Były to zdarzenia, które spowodowały lub mogły spowodować istotne obniżenie

jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Spośród 27 incydentów poważnych 14 dotyczyło sektora bankowości i infrastruktury rynków finansowych, 8 miało miejsce w sektorze ochrony zdrowia, natomiast 5 było związanych z sektorem transportu. W porównaniu z rokiem 2024 liczba incydentów poważnych w 2025 roku zmniejszyła się o 53%, zaś liczba incydentów poważnych z sektora bankowości i infrastruktury rynków finansowych o 68%. Spadek ten jest związany z wdrożeniem rozporządzenia DORA, które nakłada na podmioty finansowe obowiązek raportowania incydentów poważnych do CSIRT KNF. W 2025 roku nie odnotowano żadnego incydentu istotnego.

W 2025 roku CSIRT NASK obsłużył również 5111 incydentów w podmiotach publicznych, co oznacza wzrost o 48% w porównaniu z rokiem poprzednim.

TABELA 5. Zestawienie liczby incydentów obsłużonych przez CERT Polska w latach 2018–2025

Rok	Liczba incydentów
2025	260 783
2024	103 449
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6484
2018	3739

TABELA 6. Incydenty obsłużone przez CERT Polska w 2025 roku w podziale na sektor gospodarki. Oznaczenie sektorów wg wewnętrznej klasyfikacji CSIRT NASK

Sektor	Liczba incydentów	Procent
Osoby fizyczne	250 595	96,1%
Administracja publiczna	2801	1,1%
Handel hurtowy i detaliczny	2231	0,9%
Inne	1291	0,5%
Oświata i wychowanie	1258	0,5%
Ochrona zdrowia	724	0,3%
Infrastruktura cyfrowa	495	0,2%
Usługi inne	255	0,1%
Kultura i ochrona dziedzictwa narodowego	218	0,1%
Bankowość	179	0,1%
Transport	140	0,1%
Wodociągi	95	0,0%
Produkcja	93	0,0%
Budownictwo i gospodarka nieruchomościami	78	0,0%

Sektor	Liczba incydentów	Procent
Media	60	0,0%
Energetyka	52	0,0%
Logistyka i dystrybucja	36	0,0%
Infrastruktura rynków finansowych	35	0,0%
Gospodarka odpadami	31	0,0%
Rolnictwo	29	0,0%
Hotele, restauracje, catering	23	0,0%
Kultura fizyczna	18	0,0%
Poczta i usługi kurierskie	13	0,0%
Turystyka	10	0,0%
Działalność ubezpieczeniowa	9	0,0%
Wyznania religijne i mniejszości narodowe	5	0,0%
Izby gospodarcze i handlowe	5	0,0%
Rybołówstwo	4	0,0%
Razem	**260 783**	**100,0%**

TABELA 7. Incydenty obsłużone przez CERT Polska w 2025 roku w podziale na kategorie

Kategoria zagrożenia	Liczba incydentów	Procent
Oszustwa komputerowe	253 238	97,1%
Złośliwe oprogramowanie	3438	1,3%
Podatne usługi	1732	0,7%
Obraźliwe i nielegalne treści	950	0,4%
Włamania	750	0,3%
Dostępność zasobów	427	0,2%
Próby włamań	139	0,1%
Atak na bezpieczeństwo informacji	76	0,0%
Inne	18	0,0%
Gromadzenie informacji	15	0,0%
Razem	**260 783**	**100,0%**

MWDB

MWDB to zaawansowana platforma analityczna stworzona przez CERT Polska, służąca do zbierania, analizowania i udostępniania informacji o złośliwym oprogramowaniu. System, który stale rozwijamy, wspiera pracę analityków cyberbezpieczeństwa w Polsce i na świecie, umożliwia bowiem wymianę wiedzy oraz efektywne śledzenie trendów w obszarze szkodliwego oprogramowania. Kod platformy jest udostępniony nieodpłatnie na licencji open source (https://github.com/CERT-Polska/mwdb-core).

Rozwój platformy MWDB

W 2025 roku w ramach platformy MWDB przeanalizowaliśmy ponad 4,1 mln unikalnych próbek złośliwego oprogramowania. Efektem tych analiz było uzyskanie ponad 20,9 tys. nowych unikalnych konfiguracji malware (np. adresów serwerów zarządzających albo kluczy używanych do szyfrowania).

Równolegle z rozwojem bazy danych prowadziliśmy intensywne prace nad samym oprogramowaniem platformy. W 2025 roku opublikowaliśmy 4 nowe wersje MWDB[49], w których zaimplementowaliśmy istotne poprawki wydajnościowe. Część wprowadzonych zmian była efektem współpracy z zewnętrznymi kontrybutorami, co potwierdza aktywne zaangażowanie społeczności w rozwój projektu.

Dynamiczna analiza złośliwego oprogramowania – DRAKVUF Sandbox

Jednym z kluczowych komponentów ekosystemu MWDB jest projekt DRAKVUF Sandbox, wykorzystywany do dynamicznej analizy złośliwego oprogramowania. Mechanizm ten umożliwia bezpieczne uruchamianie podejrzanych plików w izolowanym i ściśle monitorowanym środowisku wirtualnym. Dzięki temu analitycy mogą śledzić rzeczywiste zachowanie próbek, w tym następstwa ich wykonania, takie jak pobranie docelowego złośliwego oprogramowania, próby połączenia się do znanych serwerów Command & Control czy próby kradzieży danych z systemu ofiary. Projekt wykorzystuje do tego celu otwartoźródłowy monitor DRAKVUF autorstwa Tamasa Lengyela (https://github.com/tklengyel/drakvuf), który obserwuje wykonanie próbek z poziomu hipernadzorcy za pomocą mechanizmów introspekcji maszyny wirtualnej (VMI). Pozwala to wykonywać analizy w sposób bezagentowy – bez konieczności instalowania dodatkowego

49 https://github.com/CERT-Polska/mwdb-core/releases

oprogramowania po stronie systemu „gościa”, które mogłoby być wykryte przez analizowany podejrzany program.

Podobnie jak MWDB projekt DRAKVUF Sandbox jest otwarto-źródłowy i jego kod jest dostępny publicznie (https://github.com/CERT-Polska/drakvuf-sandbox).

W 2025 roku projekt przeszedł gruntowną modernizację, która zaowocowała wydaniem wersji v0.19.0 i v0.20.050. Zmiany umożliwiły analizę próbek za pomocą najnowszej wersji silnika DRAKVUF i tym samym nowszej wersji systemu operacyjnego Microsoft Windows (Windows 10 22H2). Znacząco poprawiliśmy również stabilność analiz oraz jakość generowanych raportów analitycznych. W ramach prac nad DRAKVUF Sandbox wprowadziliśmy również istotne poprawki do silnika DRAKVUF.

Użytkownicy platformy MWDB

Platforma MWDB cieszy się rosnącym zainteresowaniem środowiska specjalistów od cyberbezpieczeństwa. W 2025 roku dostęp do platformy otrzymało 696 zewnętrznych użytkowników, a łączna liczba zarejestrowanych zewnętrznych kont w platformie wyniosła 2533.

Moje.cert.pl

Do końca 2025 roku w serwisie moje.cert.pl zarejestrowało się 15 156 użytkowników i dodało 18 315 domen. Serwis realnie wpływa na bezpieczeństwo polskiej cyberprzestrzeni – w 2025 roku w domenach dodanych w serwisie wykryliśmy 531 206 podatności, z czego 21 258 stanowiło wysokie ryzyko. Poinformowaliśmy użytkowników również o 3 914 212 wyciekach haseł, a także o 191 342 zdarzeniach sieciowych, takich jak np. serwery prowadzące skanowanie czy hostujące phishing. Dodatkowo w serwisie opublikowano 70 komunikatów – są one dostępne bez logowania w portalu, ale użytkownicy mogą również zgłosić chęć ich otrzymywania drogą mailową. Do końca 2025 roku z tej możliwości skorzystało 5127 osób.

Więcej na temat portalu można przeczytać w rozdziale „Moje.cert.pl” (s. 106–107).

50 https://github.com/CERT-Polska/drakvuf-sandbox/releases

Artemis

Od początku stycznia do końca grudnia 2025 roku w ramach projektu Artemis przeskanowano łącznie 92 183 domeny i adresy IP oraz 808 331 subdomen.

Skanowano m.in. instytucje wymienione w tabeli poniżej.

TABELA 8. Liczba przeskanowanych domen, subdomen i adresów IP w 2025 roku w podziale na kategorie

Kategoria	Liczba przeskanowanych domen i adresów IP	Liczba przeskanowanych subdomen
Szkoły i placówki oświatowe, m.in. strony szkół podstawowych, ponadpodstawowych oraz policealnych, domeny młodzieżowych domów kultury, przedszkoli czy poradni psychologiczno-pedagogicznych	46 018	400 994
Jednostki samorządu terytorialnego: strony gmin, powiatów, ale także np. strony spółek odpowiedzialnych za wywóz śmieci, archiwalne domeny czy systemy obsługujące pocztę	20 612	157 765
Uczelnie, np. strony uczelni, wydziałów, ale też domeny związane z konferencjami czy projektami naukowymi	7412	85 890
Instytucje kultury, np. strony teatrów, galerii czy bibliotek	6893	36 023
Zgłoszone domeny: domeny firm i instytucji, które zgłosiły je dobrowolnie do skanowania przed uruchomieniem portalu moje.cert.pl	6409	40 180
Sektor zdrowia, m.in. strony szpitali, ale też instytucji publicznych związanych ze zdrowiem	2829	17 422
Gazety i portale informacyjne	2310	84 688
Domeny .gov.pl	1789	28 390
Banki	1125	1625
Operatorzy usług kluczowych	601	17 123
Politycy i partie: strony m.in. kandydatów, posłów, senatorów i partii politycznych w kontekście wyborów np. samorządowych czy prezydenckich	591	16 998

Kategoria	Liczba przeskanowanych domen i adresów IP	Liczba przeskanowanych subdomen
Samorządy zawodowe, np. strony izb lekarskich czy adwokackich	411	3971
Domeny zgłoszone przez Ministerstwo Infrastruktury	338	477
Producenci automatyki przemysłowej	172	5576
Inne	316	12 663

W niektórych przypadkach dana domena może należeć do kilku kategorii.

Domeny z prefiksem www zostały wyłączone z powyższego zestawienia. Oznacza to, że jeśli dana strona jest dostępna zarówno pod adresem www.strona.pl, jak i strona.pl, to zostanie ona uwzględniona raz.

W 2025 roku łącznie zgłoszono 374 068 podatności lub błędnych konfiguracji, w tym 13 629 wiążących się z wysokim, 248 195 – średnim i 112 244 – niskim zagrożeniem. Stanowi to ok. 20-procentowy wzrost względem liczby podatności i błędnych konfiguracji wykrytych w 2024 roku.

Rodzaje znalezionych podatności lub błędnych konfiguracji zebraliśmy w poniższej tabeli. Skanowanie jest automatyczne, dlatego też podane liczby mogą zawierać duplikaty lub odnosić się do sytuacji, w których w rzeczywistości podatność nie występuje, ponieważ np. wykryto niepoprawnie skonfigurowane SSL/TLS w domenie, która w praktyce nie jest używana.

TABELA 9. Liczba znalezionych podatności lub błędnych konfiguracji w 2025 roku i opis ryzyka z nimi związanego

Liczba wystąpień	Rodzaj podatności/ błędnej konfiguracji	Ryzyko związane z podatnością/ błędną konfiguracją
183 700	Korzystanie z nieaktualnego oprogramowania	Atak przy użyciu znanych podatności – niektóre z podatności mogą skutkować tym, że ze strony można pobrać dane, inne pozwalają zmieniać treść strony lub np. uzyskać uprawnienia administratora
58 170	Problemy z konfiguracją SSL/TLS lub podobnych mechanizmów	Przechwycenie komunikacji użytkownika ze stroną – jeżeli dane zostaną przechwycone i przestępca posiada login i hasło, to może on zalogować się do serwisu jako uprawniony użytkownik

Liczba wystąpień	Rodzaj podatności/ błędnej konfiguracji	Ryzyko związane z podatnością/ błędną konfiguracją
51 554	Błędnie skonfigurowane mechanizmy weryfikacji nadawcy poczty e-mail	Wysyłanie fałszywych e-maili – przestępca może podszywać się pod nadawcę z danej domeny
36 264	Przypadki, gdy zasób taki jak np. panel administracyjny czy panel logowania, np. do bazy danych czy usługi zdalnego pulpitu, był dostępny publicznie	Atak jest możliwy np. jeśli jedno z kont ma słabe hasło albo jeśli w usłudze występują podatności
25 684	Przypadki, gdy informacje o konfiguracji serwera, lista subdomen lub listy plików w folderach na serwerze były dostępne publicznie	Może to ułatwić atakującemu rekonesans, poznanie używanego oprogramowania lub nazw plików, które nie powinny być dostępne publicznie, a w konsekwencji także umożliwić ich pobranie
9116	Konkretne krytyczne lub poważne podatności	Na przykład przejęcie strony lub pobranie danych z bazy danych
7468	Przypadki, gdy wrażliwe dane, takie jak kopie zapasowe, kod źródłowy, zrzuty bazy danych czy dziennik zdarzeń serwera były dostępne publicznie	Pobranie wrażliwych danych
1677	Pozostałe podatności o średnim poziomie ryzyka	Na przykład Open Redirect: atakujący może spreparować w domenie podmiotu link, który przekierowuje do dowolnej innej strony, w tym np. zawierającej szkodliwe oprogramowanie
357	Serwery nadal hostujące domeny, które już nie istnieją	Atakujący może komunikować się bezpośrednio z serwerem i wchodzić w interakcje ze stroną, pomimo że jest ona uznawana za usuniętą
78	Przypadki, gdy domena zbliżała się do wygaśnięcia	Niedostępność usługi lub przejęcie domeny przez atakującego

Więcej informacji na temat projektu Artemis można przeczytać w innej części raportu (→ s. 107–109).

Bezpieczna poczta

Wysyłanie fałszywych wiadomości e-mail to technika, z której regularnie korzystają cyberprzestępcy. W związku z tym w 2023 roku stworzyliśmy serwis bezpiecznapoczta.cert.pl. Dzięki niemu organizacje mogą sprawdzać poprawność konfiguracji mechanizmów takich jak SPF, DMARC czy DKIM, które utrudniają podszycie się pod nadawcę z danej

domeny. Dodatkowo ustawa o zwalczaniu nadużyć w komunikacji elektronicznej nałożyła na podmioty publiczne obowiązek korzystania z tych mechanizmów.

W 2025 roku za pomocą serwisu sprawdzono konfigurację niemal 33 tys. domen. Stanowi to prawie 40-procentowy wzrost w stosunku do roku 2024 i świadczy o tym, że tego rodzaju narzędzie odpowiada na potrzeby podmiotów.

n6

W tej części raportu prezentujemy statystyki obejmujące dane o zdarzeniach przetwarzanych automatycznie z wykorzystaniem platformy n6. Zdarzenia dotyczą podatnych systemów, prawdopodobnych infekcji lub skutecznych ataków w polskich sieciach. Informacje zostały pozyskane z autorskich systemów CERT Polska oraz z zewnętrznych źródeł. Dane są agregowane, normalizowane i udostępniane bezpłatnie właścicielom sieci oraz odpowiednim zespołom CSIRT.

Metodyka

Dołożyliśmy starań, aby obraz sytuacji, jaki wynika z prezentowanych statystyk, trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, głównie z uwagi na specyfikę dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najlepszym przykładem są ataki ukierunkowane na konkretne podmioty lub grupy użytkowników. Ataki te, w przeciwieństwie do ataków masowych, zazwyczaj nie zostaną zarejestrowane przez nasze systemy monitorujące ani nie będą zgłoszone do naszego zespołu.

Złośliwe oprogramowanie (z MWDB)

Podobnie jak w poprzednich latach dominującym typem złośliwego oprogramowania są tzw. stealery, czyli malware, który wykrada wrażliwe informacje z systemu ofiary, np. hasła. Wśród 3438 unikalnych próbek złośliwego oprogramowania przekazanych do CERT Polska w ramach zgłoszeń incydentów nasza platforma MWDB sklasyfikowała automatycznie rodzinę w 449 przypadkach (niektóre próbki wiązały się z infekcją więcej niż jedną rodziną). Wyniki zostały przedstawione poniżej w tabeli 10.

TABELA 10. Liczba incydentów, w których zidentyfikowano poszczególne rodziny szkodliwego oprogramowania

Rodzina	Liczba zgłoszonych incydentów
remcos	131
agenttesla	127
formbook	57
xworm	43
PurelogsStealer	23
reverseloader	17
404keylogger	13
lokibot	10
asyncrat	8
expiro	7
quasar	7
mirai	3
SnakeKeylogger	6
Cobalt Strike	2
LockBit	1
Lumma Stealer	1
redline	1

Phishing

W tej części raportu uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli jedynie podszywanie się pod znane marki w celu wyłudzenia wrażliwych danych z wykorzystaniem poczty i stron WWW. Przykładowo, nie uwzględniamy w tej kategorii podszywania się pod dostawców faktur w celu dystrybucji złośliwego oprogramowania.

Phishing hostowany w polskich sieciach

W 2025 roku otrzymaliśmy łącznie 144 320 zgłoszeń phishingu tylko w polskich sieciach. Dotyczyły one 3203 adresów URL, 4430 domen, które rozwiązywały się na 1875 unikalnych adresów IP zlokalizowanych w Polsce. Spadek łącznej liczby domen phishingowych w porównaniu z analizą

z poprzedniego roku wynika ze zmiany metodyki: przy obliczaniu statystyk za rok 2025 nie uwzględniliśmy źródeł danych o niskiej pewności. W tabeli 11 wymieniliśmy 10 dostawców, którzy hostowali najwięcej stron phishingowych, a których infrastruktura znajdowała się na terenie naszego kraju. Można zauważyć, analogicznie do poprzednich lat, znaczący udział home.pl wśród dostawców wybieranych przez przestępców. Był to polski dostawca o największej liczbie domen dodanych na Listę Ostrzeżeń. Oznacza to, że kampanie phishingowe z wykorzystaniem domen dostawcy za główny cel wybierały polskich użytkowników, a więc były najczęściej zgłaszane i obserwowane przez nasz zespół.

TABELA 11. Dostawcy, u których w polskich systemach autonomicznych znajdowało się najwięcej stron phishingowych w 2025 roku

Nazwa dostawcy	Numery AS	Liczba adresów IP	Liczba domen	Liczba domen na Liście Ostrzeżeń
home.pl	12824	324	449	297
Cyber Folks	41079, 43758 29522	140	437	55
Atman	57367 15694	87	290	25
OPS PL	48707	6	254	0
Nazwa.pl	15967	89	221	48
dhosting.pl	48896	29	175	8
DATASPACE	50599	34	175	4
Akamai	20940	348	168	1
LH.pl	203417	61	158	76
OVH SAS	16276	72	148	3

Phishing, który trafił na Listę Ostrzeżeń CERT Polska

W 2025 roku na Listę Ostrzeżeń CERT Polska wpisano 244 341 domen, które rozwiązywały się na 53 544 unikalne adresy IP. Podobnie jak w 2024 roku przestępcy najczęściej wykorzystywali usługi Cloudflare do ukrycia prawdziwej lokalizacji serwera – aż 43 843 adresy IP miały prefiksy w AS13335.

Tabela 12 przedstawia najczęściej występujące cele, pod które podszywali się przestępcy. W 2025 roku najczęściej występującym celem phishingu były oszustwa inwestycyjne. Największy wzrost odnotowaliśmy dla witryn podszywających się pod telewizję TVN.

TABELA 12. Najczęściej występujące cele phishingu, które znalazły się na Liście Ostrzeżeń

Cel phishingu	Liczba domen w 2025 r.	Liczba domen w 2024 r.
Fałszywe inwestycje	98 663	42 172
OLX	28 562	9714
Allegro	22 613	4074
Orlen	16 977	972
TVN	11 644	7
Gazeta.pl	11 367	2057
Polsat News	7632	80
Telegram	5415	20
Onet	3390	866
Wprost	3189	7

W tabeli 13 umieściliśmy natomiast najczęściej występujące domeny najwyższego poziomu, które zostały dodane na Listę Ostrzeżeń w 2025 roku. Najpopularniejszymi TLD były .com, .pro i .icu. W 2025 roku przestępcy rzadziej rejestrowali domeny w .pl. Na Liście Ostrzeżeń znalazło się 2887 domen o TLD .pl.

TABELA 13. Najczęściej występujące domeny najwyższego poziomu (TLD), które znalazły się na Liście Ostrzeżeń w 2025 roku

TLD	Liczba domen
.com	77 483
.pro	28 918
.icu	18 946
.cfd	14 741
.net	10 884
.sbs	10 875
.top	8602
.shop	8386
.info	6257
.online	5039

Usługi pozwalające na prowadzenie ataków DRDoS

W roku 2025 odnotowaliśmy ponad 23 289 818 zgłoszeń dotyczących 424 947 polskich adresów IP powiązanych z publicznie widocznymi usługami, które umożliwiały przeprowadzanie rozproszonych ataków odmowy usługi ze wzmocnieniem (Distributed Reflection Denial of Service, DRDoS). Na statystykę zgłoszeń składają się przede wszystkim źle skonfigurowane usługi, realnie wpływające na bezpieczeństwo systemów teleinformatycznych. Niewielką częścią uwzględnionych zgłoszeń są systemy honeypot oraz inne usługi udostępnione celowo,

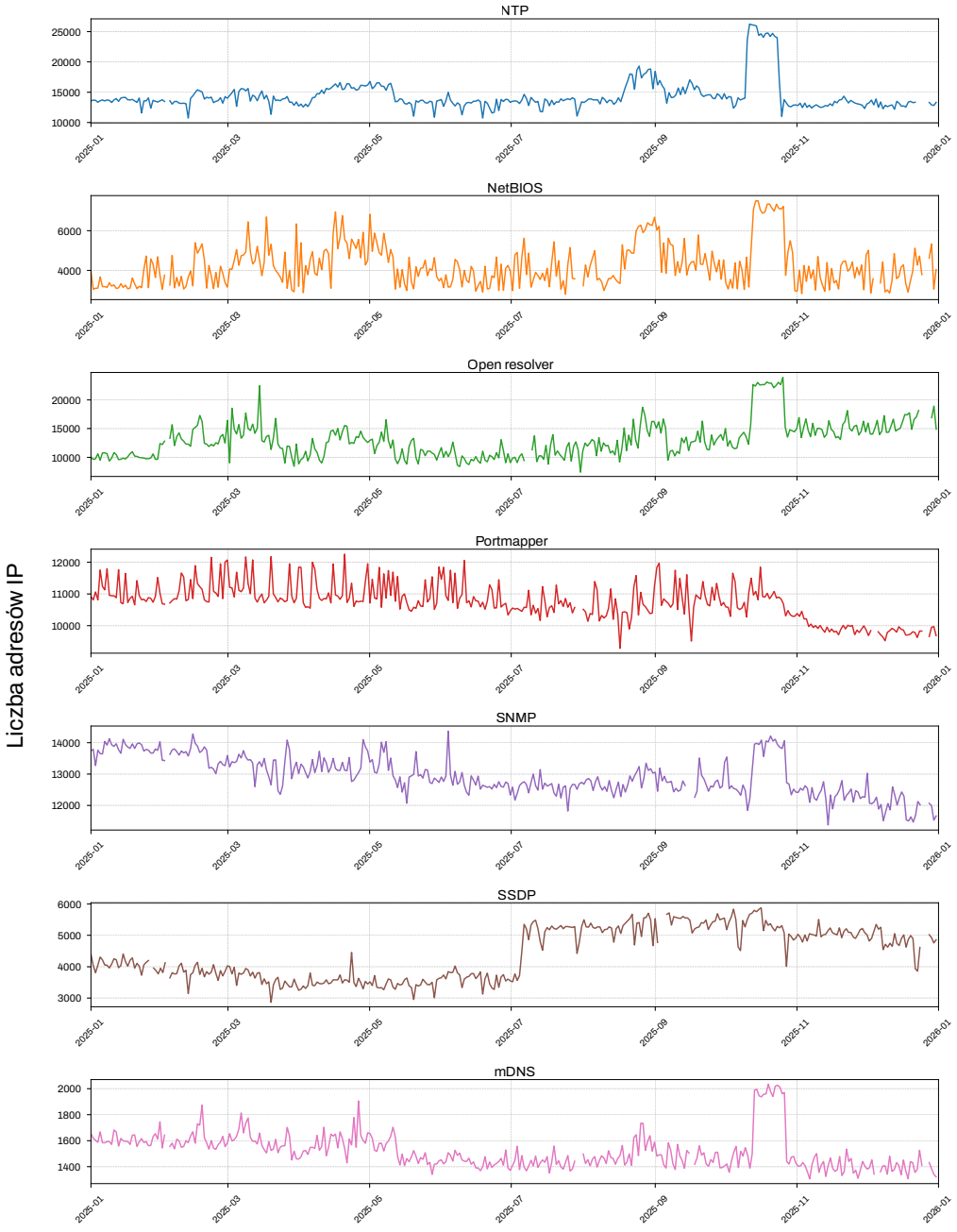
jednak odróżnienie ich na podstawie wyników ogólnego skanu jest trudne. Ich wpływ na statystykę jest minimalny. Warto zauważyć, że liczba notowanych zgłoszeń zauważalnie spadła względem roku 2024 (27 202 309 zgłoszeń), co wskazuje na spadek dostępnych usług możliwych do wykorzystania w ataku DRDoS. Rodzaj notowanych usług pozostaje bez większych zmian.

W tabeli 14 przedstawiamy zestawienie najczęściej notowanych usług, które mogły być wykorzystane do ataków DRDoS w kontekście polskich adresów IP. Zgłoszenia zostały zgrupowane w statystyki dzienne, na podstawie których obliczono statystyki roczne. Wartości zostały zaokrąglone do całości. Czas obserwacji jest procentowym przedstawieniem liczby dni w roku, w których odnotowano przynajmniej jedno zgłoszenie dotyczące danej usługi. Odchylenie standardowe dotyczy natomiast zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku.

TABELA 14. Zestawienie najczęściej występujących niepoprawnie skonfigurowanych usług możliwych do wykorzystania w atakach DRDoS

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1.	NTP	14 482	26 317	2494	99,18%
2.	Open resolver	13 013	23 960	3138	98,90%
3.	SNMP	12 944	14 383	639	99,18%
4.	Portmapper	10 731	12 258	667	98,90%
5.	SSDP	4394	5886	843	98,90%
6.	NetBIOS	4231	7532	1086	98,90%
7.	mDNS	1516	2034	155	98,90%
8.	mssql	1020	1594	132	98,90%
9.	DVR DHCPDi-scover	872	2238	445	98,36%
10.	Ubiquiti	744	962	90	99,18%
11.	CHARGEN	111	162	22	98,90%
12.	CoAP	34	41	3	98,90%
13.	QOTD	17	29	3	98,90%
14.	XDMCP	11	14	2	99,18%
15.	ARD	6	9	1	98,90%
16.	RDPEUDP	4	14	2	95,89%

RYSUNEK 41. Wykresy ukazujące zmiany liczby podatnych adresów IP w Polsce w 2025 roku w kontekście najpowszechniejszych niepoprawnie skonfigurowanych usług możliwych do wykorzystania w atakach DRDoS



Pięć najczęściej obserwowanych usług zostało dokładniej opisanych poniżej. Statystyki zgłoszeń dla tych usług ponownie zostały zgrupowane w dane dzienne z zakresu roku 2025, z dodatkowym podziałem na systemy autonomiczne.

NTP

Network Time Protocol (NTP) jest powszechnym protokołem synchronizacji czasu używanym w sieciach komputerowych. Publicznie dostępne serwery NTP, które udostępniają polecenie monlist, mogą być jednak wykorzystane do ataków DDoS. Tak jak w ubiegłym roku jest to najczęściej obserwowana usługa w tej kategorii.

Liczba zgłoszeń w ciągu roku **5 254 569**

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia **101 857**

TABELA 15. Dzienna liczba adresów, na których wykryto działającą usługę NTP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
1.	5617	Orange	2851	14226	0,26%
2.	12741	Netia	775	840	0,07%
3.	12912	T-Mobile	655	784	0,07%
4.	48956	HyperNET	429	629	12,93%
5.	43372	Telnap Telecom	287	366	5,11%
6.	199715	MSI Telekom	219	442	2,83%
7.	9085	Supermedia	216	294	0,69%
8.	59491	LiveNet	172	179	2,50%
9.	15694	Atman	170	187	0,27%
10.	8267	ACK Cyfronet AGH	164	210	0,27%

Otwarte serwery DNS

Otwarte serwery DNS (open resolver) mogą zostać wykorzystane do przeprowadzania ataków DRDoS. Pomimo kluczowego znaczenia dla działania internetu zdecydowana większość serwerów DNS nie powinna odpowiadać na zapytania z całej sieci internet, lecz tylko na zapytania z ograniczonej grupy adresów.

Liczba zgłoszeń w ciągu roku **4 769 640**

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia **171 196**

TABELA 16. Dzienna liczba adresów IP, na których wykryto otwarty serwer DNS, w podziale na systemy autonomiczne

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
1.	5617	Orange	2218	10 440	0,19%
2.	9141	P4 (Play)	1781	6841	0,42%
3.	12741	Netia	740	1496	0,12%
4.	12912	T-Mobile	562	621	0,06%
5.	201814	Mevspace	365	2659	13,32%
6.	13110	INEA	346	368	0,21%
7.	8374	Polkomtel	317	356	0,08%
8.	29314	Vectra	312	341	0,06%
9.	50599	Dataspace	279	1205	9,81%
10.	6830	Liberty Global Europe Holding BV	225	419	0,04%

SNMP

SNMP (ang. Simple Network Management Protocol) to protokół stworzony do zdalnego zarządzania urządzeniami sieciowymi. Zalecane jest używanie go wyłącznie w odseparowanych sieciach przeznaczonych do zarządzania. W sytuacji gdy usługa bazująca na SNMP jest widoczna w internecie, poza zagrożeniem nieuprawnionego dostępu do urządzenia może być ono także wykorzystane do realizacji ataków DDoS.

Liczba zgłoszeń w ciągu roku **4 688 089**

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia **49 712**

TABELA 17. Dzienna liczba adresów IP, na których wykryto działającą usługę SNMP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
1.	12741	Netia	1375	1699	0,14%
2.	20804	EXATEL	670	1189	0,49%

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
3.	8374	Polkomtel	599	697	0,16%
4.	199390	Alfa Komputer System	476	507	16,50%
5.	12912	T-Mobile	423	495	0,04%
6.	57978	Digicom	338	352	17,19%
7.	5617	Orange	305	1862	0,03%
8.	200594	SOFT PARTNER	223	307	14,99%
9.	9141	P4 (Play)	218	306	0,02%
10.	13110	INEA	188	206	0,12%

Portmapper

Portmapper to niskopoziomowa usługa typowa dla uniksowych systemów operacyjnych. Korzystają z niej protokoły wyższych warstw, w tym m.in. NFS (sieciowy system plików, ang. Network File System). Publicznie dostępny portmapper stanowi zagrożenie ze względu na możliwość jego wykorzystania w atakach DDoS.

Liczba zgłoszeń w ciągu roku **3 874 126**

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia **39 764**

TABELA 18. Dzienna liczba adresów, na których wykryto działającą usługę portmapper na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
1.	16276	OVH	2250	2510	0,06%
2.	12876	Scaleway	631	1042	0,21%
3.	50599	Dataspace	417	1315	10,70%
4.	57367	Atman	255	298	2,16%
5.	25369	Hydra Communications	251	252	0,23%
6.	12741	Netia	217	261	0,02%

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
7.	201814	Mevspace	195	304	1,52%
8.	50840	HitMe	190	204	4,43%
9.	197155	Artnet	180	237	1,93%
10.	31242	P4 (Play)	163	197	0,17%

SSDP

SSDP (ang. Simple Service Discovery Protocol) jest protokołem wykorzystywanym do wykrywania i rozgłaszania obecności wybranych urządzeń oraz usług w danej sieci. Zwykle pozwala przede wszystkim na identyfikację urządzeń działających w oparciu o protokół UPnP (ang. Universal Plug and Play), ale dostępny publicznie, podobnie jak poprzednie opisywane usługi, stanowi zagrożenie i może być wykorzystywany do realizacji ataków DDoS.

Liczba zgłoszeń w ciągu roku **1 608 242**

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia **44 414**

TABELA 19. Dzienna liczba adresów, na których wykryto działającą usługę SSDP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne

Poz.	Numer AS	Nazwa AS	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odsetek wszystkich adresów IP w AS
1.	197697	DERKOM	1498	1698	20,73%
2.	29314	Vectra	561	790	0,13%
3.	21021	Multimedia Polska	341	734	0,12%
4.	41023	ARREKS	340	378	10,55%
5.	8374	Polkomtel	153	204	0,05%
6.	12741	Netia	145	280	0,02%
7.	12912	T-Mobile	124	147	0,01%
8.	57101	WadowiceNET	98	114	2,12%
9.	43118	East&West	90	146	0,20%
10.	5617	Orange	89	389	0,01%

Podatne usługi

W 2025 roku odnotowaliśmy 55 605 774 wydarzenia związane z obserwacją usług narażonych na ataki. Odnotowane wydarzenia dotyczyły 810 173 polskich adresów IP. Do statystyki zaliczają się zarówno usługi, w których występują aktywnie wykorzystywane podatności, jak i usługi niepoprawnie skonfigurowane, umożliwiające m.in. nieupoważniony dostęp do informacji lub zarządzania daną usługą. Liczba odnotowanych wydarzeń utrzymała się na podobnym poziomie w stosunku do poprzedniego roku (53 010 669 obserwacji).

W tabeli 20 przedstawiliśmy zestawienie usług, które mogły być zagrożone atakiem i były najliczniej reprezentowane w polskim internecie. Przyjęliśmy metodę obliczeń analogiczną do metody opisanej w sekcji dotyczącej ataków DRDoS.

Na rysunku 42 zostały pokazane zmiany rejestrowanej przez nas liczby adresów IP powiązanych z podatnymi usługami w skali roku. Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług.

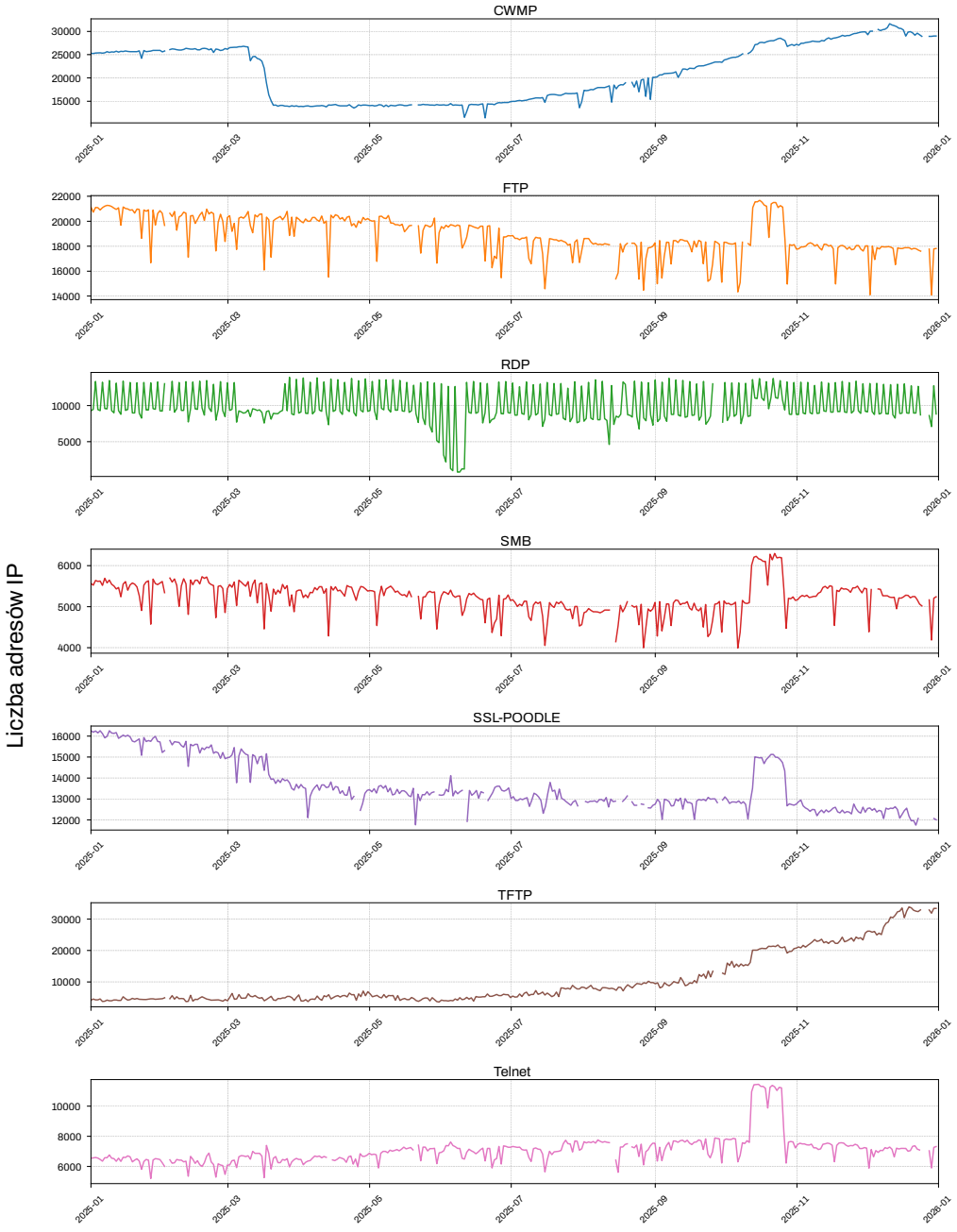
Na wykresach dotyczących CWMP oraz TFTP (na rysunku 42) widać znaczące zmiany liczby zgłoszeń na przestrzeni roku. Z analizy kwartalnej statystyk wynika, że w wypadku tych usług liczba notowanych adresów IP w większości systemów autonomicznych (AS) utrzymywała się na podobnym poziomie, a wzrost bądź spadek statystyki był spowodowany przez znaczące zmiany w pojedynczych AS. W wypadku CWMP w pierwszym kwartale na bardzo wysokim poziomie utrzymywała się liczba zgłoszeń dotyczących ASN 12741 (Netia) – średnio ponad 12 000 zgłoszeń dziennie. Od drugiej połowy drugiego kwartału liczba ta znacznie się zmniejszyła i utrzymała się na relatywnie niskim poziomie. Na przestrzeni roku wyróżnił się ASN 29314 (Vectra) – w pierwszych dwóch kwartałach notowano średnio 300 adresów IP dziennie, w trzecim kwartale 2000 adresów IP dziennie, a w czwartym ponad 9600 adresów IP dziennie. Głównie ta zmiana spowodowała stały wzrost notowań pod koniec roku. Analogicznie sytuacja wygląda w kontekście TFTP. Większość notowań utrzymywała się na stałym poziomie dla danych AS. Wyjątkiem od reguły był ASN 9141 (P4/Play), dla którego liczba notowań wzrosła znacząco ze średnio kilkudziesięciu adresów IP dziennie w pierwszej połowie roku do średnio 2000 adresów dziennie w trzecim kwartale i wyniosła średnio ponad 12 000 adresów w ostatnim kwartale 2025 roku.

Nagły spadek liczby adresów IP powiązanych z CWMP najprawdopodobniej powiązany jest z wdrożeniem aktualizacji do grupy urządzeń danego producenta, która wyłącza obsługę usługi przy domyślnych ustawieniach. Odnotowany w drugiej połowie roku stopniowy wzrost notowań CWMP oraz TFTP można natomiast powiązać z wprowadzaniem do użytku nowych urządzeń, domyślnie korzystających z tych protokołów.

TABELA 20. Zestawienie najliczniej występujących w Polsce usług zagrożonych atakiem

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1.	CWMP	21 078	31 677	6031	98,63%
2.	FTP (dane uwierzytelniające w postaci jawnej)	18 817	21 676	1983	98,90%
3.	SSL-POODLE	13 506	16260	1272	98,90%
4.	TFTP	10 337	33 662	8250	98,90%
5.	RDP	10 045	13 941	2516	98,90%
6.	Telnet	7042	11 446	1088	99,18%
7.	SMB	5190	6283	523	98,90%
8.	VNC	2801	5006	452	99,18%
9.	RSYNC	1602	1993	295	99,18%
10.	SSL-FREAK	1187	1769	224	99,18%
11.	MQTT	1064	1364	104	99,18%
12.	MongoDB	815	919	145	99,18%
13.	AMQP	725	797	65	98,90%
14.	Redis	568	2521	665	98,90%
15.	AFP	496	746	105	98,90%
16.	NAT-PMP	435	523	45	99,18%
17.	ISAKMP	428	1117	164	78,08%
18.	IPP	335	521	47	98,63%
19.	IPMI	281	316	19	98,90%
20.	LDAP	238	273	23	99,18%
21.	Memcached	159	226	30	99,18%

RYSUNEK 42. Wykresy ukazujące zmiany liczby podatnych adresów IP w Polsce w 2025 roku w kontekście najpowszechniej używanych usług narażonych na ataki



Podobnie jak w ubiegłorocznym raporcie w ramach omawiania podatnych usług zdecydowaliśmy się dodatkowo wydzielić informacje dotyczące serwerów Exchange, usługi HTTP oraz systemów przemysłowych (ICS/OT). Dane zostały zaprezentowane poniżej w osobnych tabelach. Przyjęto metody obliczeń i oznaczenia analogiczne do metod opisanych w sekcji dotyczącej ataków DRDoS.

Exchange

W poniższej sekcji znalazły się informacje dotyczące podatnych serwerów Microsoft Exchange. Większość podatności wymienionych w tabeli to luki umożliwiające zdalne wykonanie kodu na zaatakowanym systemie (Remote Code Execution). Najnowsza z notowanych podatności, CVE-2025-53786, dotyczy eskalacji uprawnień i nie jest tak krytyczna, jak wcześniej obserwowane podatności. Zespół realizował wysyłkę powiadomień dotyczących tej podatności do właścicieli serwerów, dzięki czemu większość instancji została zaktualizowana. Z prawie 70 serwerów średnio jedynie 7 pozostaje oznaczanych jako narażone na atak związany z tą podatnością. Ogólna liczba notowanych instancji podatnych serwerów Exchange znacząco spadła w stosunku do roku 2024, co sugeruje, że komunikaty wysyłane do administratorów oraz przeprowadzone aktualizacje przyniosły pozytywny efekt.

TABELA 21. Zestawienie najliczniej notowanych podatności dotyczących serwerów Exchange w Polsce narażonych na ataki

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1.	CVE-2024-26198	7	92	14	98,63%
2.	CVE-2025-53786	7	67	10	39,18%
3.	CVE-2023-36745	3	13	3	96,71%
4.	CVE-2023-36439	3	13	3	97,81%
5.	CVE-2024-21410	3	11	2	98,63%
6.	CVE-2023-21529	3	11	2	98,63%
7.	CVE-2022-41082	3	11	2	98,63%
8.	CVE-2020-0688	2	8	2	98,08%
9.	CVE-2021-27065	2	8	2	98,08%
10.	CVE-2021-26855	2	6	1	98,63%

HTTP

Poniżej podajemy wybrane informacje dotyczące systemów wykorzystujących protokół HTTP, które mogą być narażone na ataki. Podane w tabeli podatności oznaczają:

- **Basic auth** – serwery HTTP, które używają Basic Authentication. Serwer pozwala na przysłanie danych uwierzytelniających w postaci jawnej, bez szyfrowania.
- **Basic auth (IoT)** – jak wyżej. Dotyczy urządzeń IoT.
- **Folder .git** – dostępny publicznie folder .git.

Pozostałe podatności odnoszą się do standardowego systemu oznaczeń CVE.

TABELA 22. Zestawienie najliczniej występujących w Polsce serwerów narażonych na ataki. Pozycje zostały wytypowane na podstawie zarówno średniej dziennej liczby adresów, jak i znaczącego czasu obserwacji

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1.	Basic auth	6836	7779	616	98,90%
2.	Basic auth (IoT)	3654	5002	548	98,90%
3.	Folder .git	367	439	26	98,63%
4.	Cisco CVE-2025-20333, CVE-2025-20362, CVE-2025-20363	141	286	83	24,93%
5.	React Server CVE-2025-55182	122	398	106	6,85%
6.	Fortinet CVE-2024-21762	84	501	108	98,90%
7.	Fortinet CVE-2024-55591	79	281	48	94,52%
8.	Roundcube CVE-2023-43770	75	129	51	46,30%
9.	Fortinet CVE-2023-27997	74	501	118	98,90%
10.	Fortinet CVE-2024-23113	70	501	103	98,90%
11.	Plex Media Server CVE-2025-34158	69	239	57	35,34%

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
12.	Tinyproxy CVE-2023-49606	66	238	59	98,90%
13.	Roundcube CVE-2023-5631	62	129	51	46,30%
14.	Roundcube CVE-2025-49113	45	318	58	4,11%
15.	Zimbra CVE-2024-45519	31	107	33	98,90%
16.	Zimbra CVE-2025-62763	16	30	12	18,36%
17.	VMare CVE-2025-22224	15	58	13	82,19%
18.	GLPI CVE-2025-24801	12	34	11	77,81%
19.	FreePBX CVE-2025-57819	11	27	6	29,59%
20.	VMware CVE-2025-41236	9	49	10	44,66%

Przemysłowe systemy sterowania

W poniższej sekcji znalazły się informacje dotyczące systemów ICS/OT, które są publicznie widoczne w sieci. Podczas procesu skanowania nie sprawdzano konkretnych podatności, lecz tego typu urządzenia nigdy nie powinny być widoczne i dostępne z internetu. Protokoły przemysłowe często nie wspierają uwierzytelniania, co naraża je na nieuprawnione modyfikacje i dostęp do znaczących informacji przez osoby nieupoważnione.

Poniższe zestawienie, jak w przypadku wcześniejszych statystyk, uwzględnia zarówno adresy IP, na których faktycznie dostępne są opisane usługi, jak i te, które są udostępniane celowo (np. systemy honeypot), ponieważ ich odróżnienie na podstawie danych ze skanowania jest trudne, a ich łączna liczba jest niewielka.

W porównaniu z rokiem poprzednim ogólna średnia dzienna liczba adresów IP utrzymała się na podobnym poziomie, ale wystąpiły zmiany w popularności usług, których te adresy dotyczą. Największe wzrosty wystąpiły w przypadku protokołu BACnet (średnio ok. 40 adresów więcej dziennie), natomiast największe spadki dotyczą S7 oraz Codesys (średnio ok. 20 adresów mniej dziennie). Pozostałe protokoły pozostały na bardzo zbliżonym poziomie notowań.

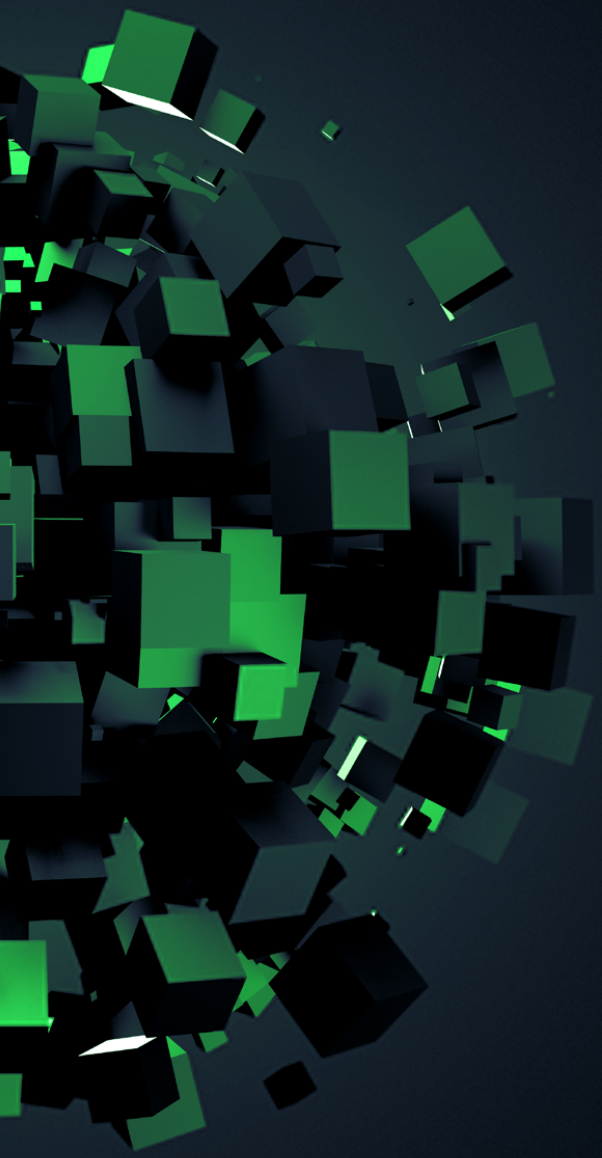
TABELA 23. Zestawienie najliczniej występujących w Polsce systemów ICS/OT narażonych na ataki

Poz.	Nazwa podatności/ otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1.	S7	157	225	19	98,63%
2.	BACnet	157	208	21	98,36%
3.	Codesys	124	181	18	98,63%
4.	Modbus	102	141	14	98,63%
5.	EtherNet/IP	60	75	6	98,36%
6.	OPC UA Binary	27	41	5	98,63%
7.	Fox	18	22	3	98,63%
8.	Unitronics	14	22	2	98,63%
9.	DNP3	9	23	3	98,36%
10.	IEC 60870-5-104	8	22	4	98,63%
11.	Omron FINS	7	14	2	98,63%
12.	PC Worx	6	9	1	97,26%
13.	GE SRTP	5	8	1	97,81%
14.	ICCP	3	6	2	95,07%
15.	MELSEC-Q	2	4	1	93,42%

Spis rysunków

Spis tabel

Spis wykresów



NASK–PIB/CERT Polska

ul. Kolska 12,
01–045 Warszawa

Recepcja

+48 22 380 82 00
+48 22 380 82 01

Sekretariat

+48 22 380 82 04
+48 22 380 82 01

info@cert.pl
cert.pl