WRZESIEŃ 2025

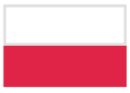
Podsumowanie Miesiąca CERT POLSKA CSIRT NASK

Nr 1/2025

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA / CSIRT NASK



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki zarejestrowanych zagrożeń

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki zawarte w niniejszym rozdziale obejmują dane o liczbie zarejestrowanych zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 30 września 2025 r. Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

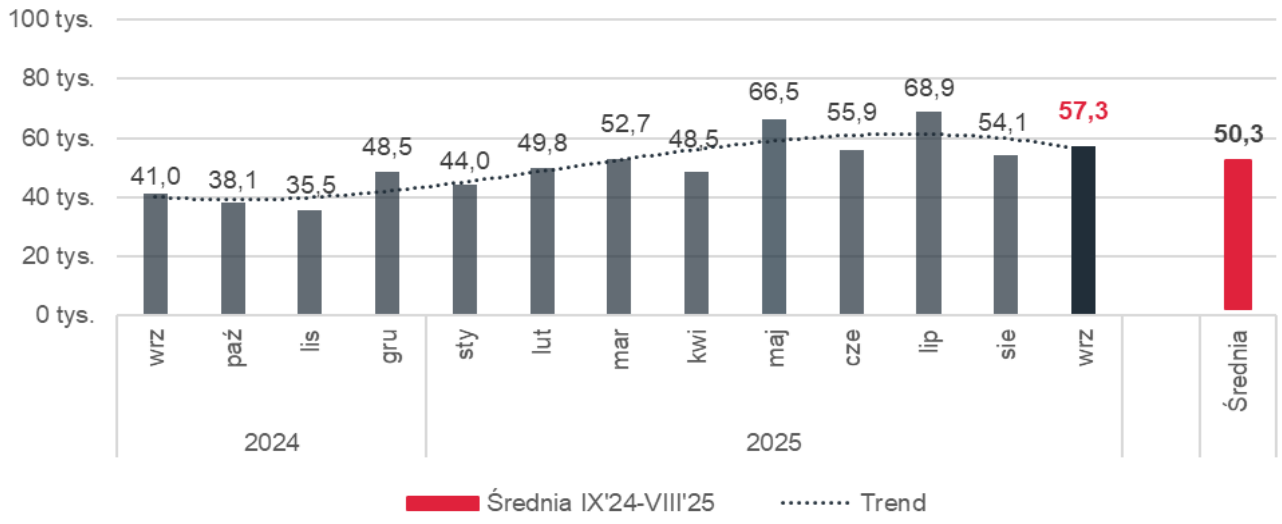
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – IX 2025

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 30 września 2025 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**57,3 tys.**
w tym zarejestrowane (obsłużone) incydenty	**26,4 tys.**

We wrześniu 2025 r. CSIRT NASK otrzymał łącznie **57,3 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **26,4 tys.** incydentów bezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na cyberbezpieczeństwo. Dotyczą one konkretnych kategorii zagrożeń, np. szkodliwych stron wyłudzających poufne informacje (ang. *phishing*), spamu czy ataku z użyciem szkodliwego oprogramowania. W wielu przypadkach jeden incydent był powiązany z kilkoma zgłoszeniami.

Zarejestrowane zgłoszenia cyberbezpieczeństwa od IX 2024 do IX 2025

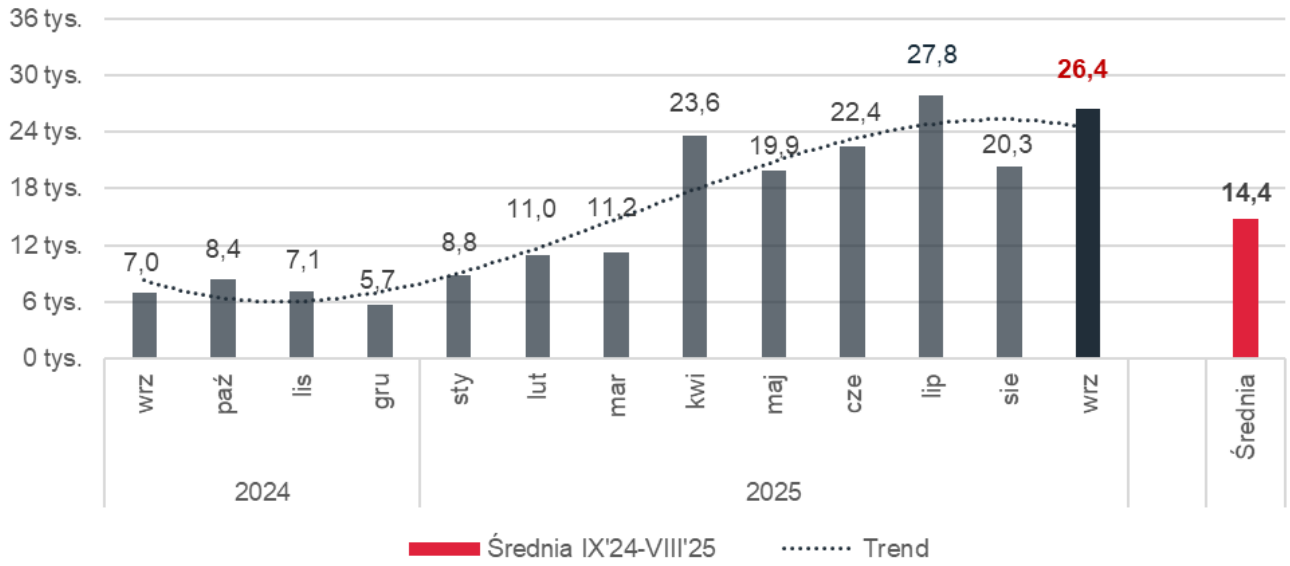


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.09.2024 do 30.09.2025. Źródło: CERT Polska / CSIRT NASK.

[1] Zgłoszenia przesyłane są za pośrednictwem formularza dostępnego na stronie https://incydent.cert.pl lub są wysyłane na adres zgłoszeniowy cert@cert.pl. Rejestrowane są także powiadomienia otrzymywane bezpośrednio od przedstawicieli sektora publicznego oraz prywatnego. Otrzymane informacje o zagrożeniach cyberbezpieczeństwa stanowią podstawę rejestracji nowych zgłoszeń, incydentów lub są rejestrowane wyłącznie do celów statystycznych, jako zgłoszenia niemające charakteru realnego zagrożenia.

Liczba zgłoszeń odnotowanych we wrześniu 2025 r. przekroczyła średnią liczoną z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2024 r. liczba ta **zwiększyła się o 40%**. W stosunku do sierpnia 2025 r. był to **wzrost o 6%**.

Zarejestrowane incydenty cyberbezpieczeństwa od IX 2024 do IX 2025



Wykres 2. Liczba zarejestrowanych incydentów od 01.09.2024 do 30.09.2025. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych we wrześniu 2025 r. wyniosła **26,4 tys.** W porównaniu z analogicznym miesiącem 2024 r. liczba incydentów we wrześniu 2025 r. **zwiększyła się o 278%** i pozostawała powyżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do sierpnia 2025 r. liczba zarejestrowanych incydentów **zwiększyła się o 30%**.

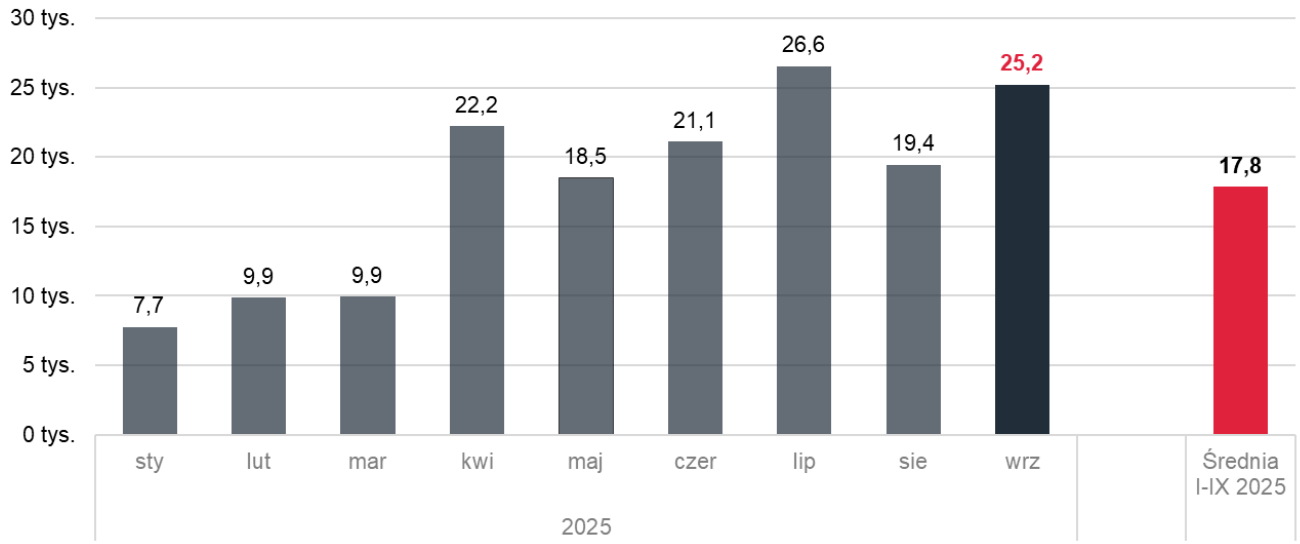
Rodzaje zarejestrowanych zagrożeń – IX 2025

Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 30 września 2025 r. Źródło: CERT Polska / CSIRT NASK.

W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**26,4 tys.**) stanowiły one **97%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). We wrześniu 2025 r. łącznie odnotowano **11,4 tys.** tego typu incydentów.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–IX 2025

CERT Polska prowadzi Listę Ostrzeżeń przed niebezpiecznymi stronami. Na listę wpisywane są domeny, które wprowadzają użytkowników w błąd oraz wyłudzają od nich dane. Szkodliwe domeny są blokowane na 6 miesięcy. Jeśli po upływie tego czasu nadal zawierają niebezpieczne treści, to zostają one dodane jako nowy wpis.



Wykres 4. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń.

Od stycznia do września 2025 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **160,6 tys.** szkodliwych domen, z czego we wrześniu 2025 r. dodano **25,2 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do sierpnia 2025 r. **zwiększyła się o 30%**.

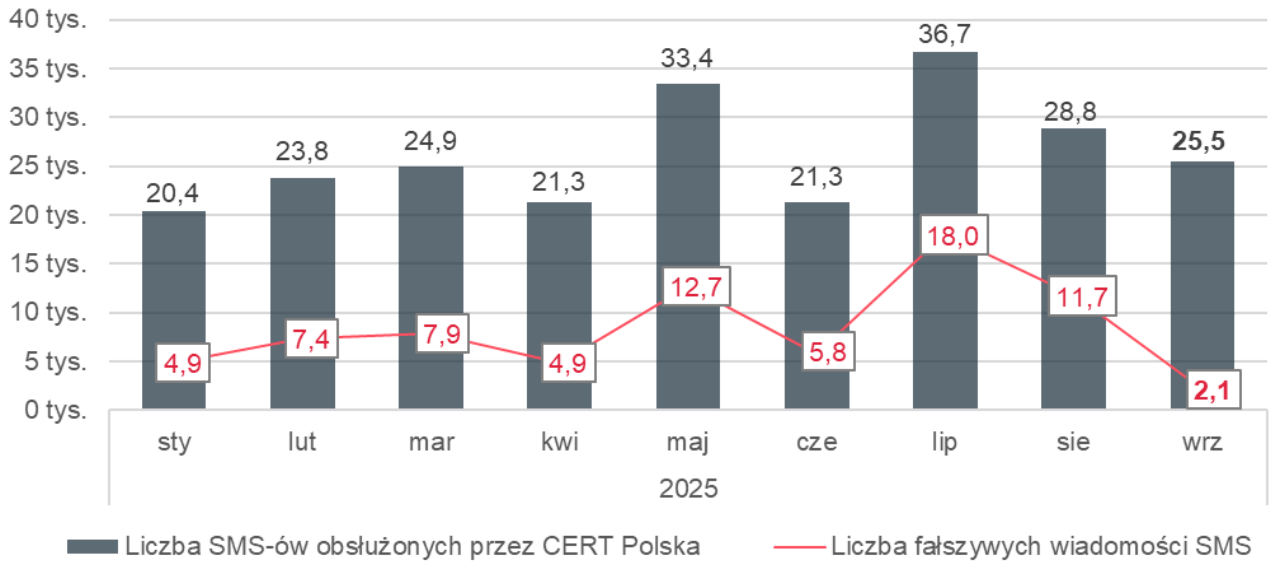
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

2authenticationtd.com; 3plk.cfd; 7462.top; alebilet.pl-kategoria2345463.pl; allegro.ochronakupuiacega39900294.cfd; dozanturix.org; dpdpaczka.idowoepq7833.icu; e-biletpl.link; ebylet-dawid-podsiadlo-pl.com; eobuwie.live; ibank.santandercommercial.com; inpost.blog; inpost.szyfrowanyprzelew24wygodnaplatforma24godziny.cfd; intelligent-invest-ai.com; ipko-support.x24hr.com; mail.kprm-gov.pl; mail-netflix.com; moj-abonament.com; mojadostawa.com; mydisneyclub.com; netflix.pl-aktualizacja.com; newseuro.live; ochnik-pl.shop; odnawialna-moc-ziemia.info; olx.74852.top; olx.ogloszenia-pozostale.com; olx.pl-oferta2347409.icu; pknorlen.com; pko-logowanie.x24hr.com; pl-smartzakupy-23174.icu; pocztex.help; polskanews.wiki; rossmann-karty.com; szkoleniajo.online; szyk-krakow.pl; taniec-online.com; testbanker.online; vinted.pl-dostaw.shop; web.teiegrnmny.com; wiadomosci24polska.pl; wydarzenia-tvn24info.com.pl; zabkonline.play-official-slots.net; zakupydlamamy.shop; zalando-on.shop; zappka.many-apps-game.com

Liczba zgłoszeń wiadomości SMS przyjętych przez CSIRT NASK I–IX 2025

Od 1 stycznia do 30 września 2025 r. zespół CERT Polska zarejestrował **236,2 tys.** zgłoszeń SMS-ów. Liczba SMS-ów otrzymanych we wrześniu 2025 r. wyniosła **25,5 tys.** W porównaniu z sierpniem 2025 r. był to **spadek o 12%.** Wśród ogółu SMS-ów przyjętych we wrześniu 2025 r. **fałszywe wiadomości SMS stanowiły 8%**.



Wykres 5. Liczba SMS-ów zgłoszonych do CSIRT NASK w danym miesiącu.

Wzorce fałszywych wiadomości SMS I–IX 2025

Zgodnie z ustawą z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej CSIRT NASK **monitoruje występowanie smishingu** i **tworzy wzorce wiadomości**, które posiadają cechy pozwalające na uznanie ich za smishing. Działania te wykonuje na podstawie zgłoszeń podejrzanych wiadomości tekstowych (SMS) otrzymanych od odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów. CSIRT NASK zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi

Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi UKE i przedsiębiorcom telekomunikacyjnym. Podejrzane SMS-y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**.

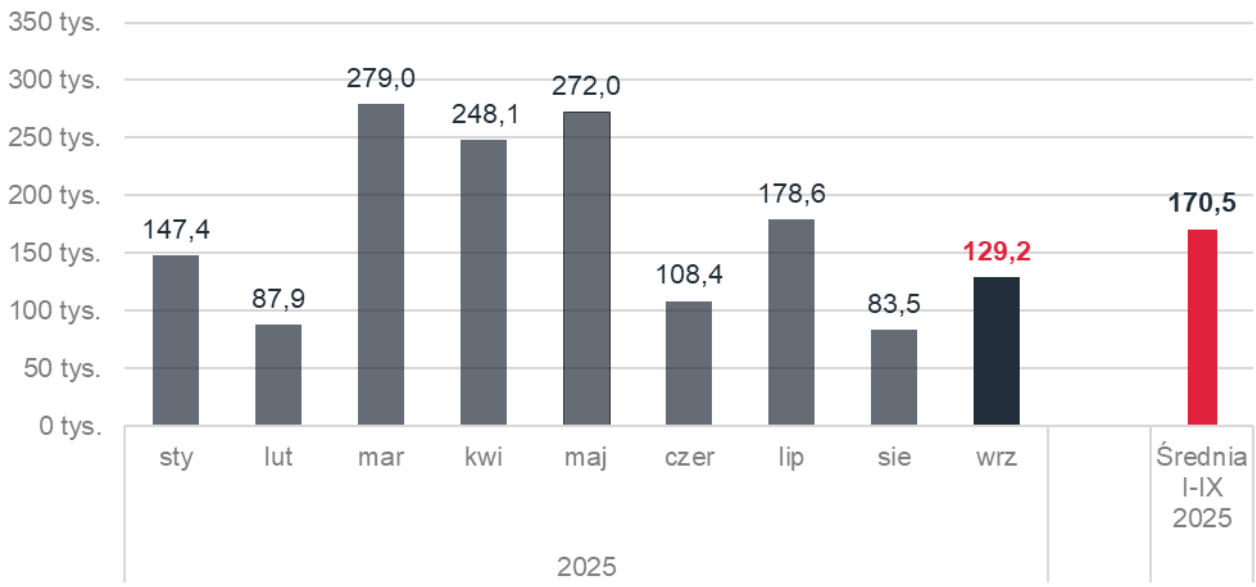
Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	Razem
Liczba wytworzonych wzorców	82	57	106	60	83	39	119	10	**43**	**599**

Wykaz wzorców wiadomości SMS znajduje się na stronie: telegraf.cert.pl

Liczba zablokowanych SMS-ów I–IX 2025

W okresie od 1 stycznia do 30 września 2025 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie ponad **1,5 mln** SMS-ów.



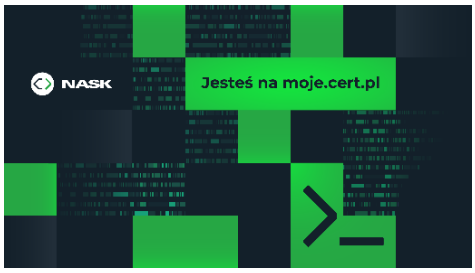
Wykres 6. Liczba SMS-ów zablokowanych na podstawie wzorców fałszywych wiadomości SMS w danym miesiącu. Źródło: CERT Polska / CSIRT NASK.

Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił szerokiemu gronu odbiorców bezpłatny serwis moje.cert.pl. Z serwisu mogą korzystać zarówno osoby prywatne posiadające stronę internetową, jak i małe firmy czy duże instytucje publiczne udostępniające wiele skomplikowanych systemów. Zarejestrowany użytkownik moje.cert.pl może zamówić bezpłatne skanowanie bezpieczeństwa wszystkich swoich domen, uzyskać informacje na temat wycieków haseł użytkowników w swojej domenie, otrzymywać informacje o infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach (ta funkcja jest dostępna dla administratorów serwerów i sieci), a także sprawdzić, czy dana sieć jest chroniona przez Listę Ostrzeżeń przed niebezpiecznymi stronami. Ponadto

w serwisie, w zakładce „Komunikaty” pojawiają się – i będą na bieżąco dodawane – ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach. Komunikaty te są dostępne na stronie także dla niezarejestrowanych użytkowników, a od sierpnia 2025 r. każdy może otrzymywać je również w wiadomości e-mail. Moje.cert.pl korzysta m.in. z systemów **Artemis** (skanowanie stron) i **n6** (informacje o zagrożeniach dla adresacji IP) – narzędzi pozwalających chronić dane i infrastrukturę.

We wrześniu 2025 r. w serwisie moje.cert.pl **zarejestrowało się 560 nowych użytkowników**.



W okresie od 1 do 30 września 2025 r. CSIRT NASK wysłał **3,5 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności i błędnych konfiguracji**. Powiadomienia o wykrytych nieprawidłowościach zostały wysłane do osób, które zgłosiły daną stronę do skanowania w serwisie moje.cert.pl, a także do ich współpracowników dodanych w serwisie.

Więcej: moje.cert.pl

Podatności CVE

Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności. We wrześniu 2025 r. zespół CERT Polska nadał **16** numerów CVE. Wśród wykrytych podatności znalazły się podatności m.in. w oprogramowaniach Sparkle, ITCube CRM oraz kamerach GALAYOU G2. Przykładami podatności wykrytych przez CSIRT NASK w ramach badań własnych były podatności w oprogramowaniu PAD CMS.

Więcej: CERT Polska/CNA; CERT Polska/CVE

Tabela 3. Nadane numery CVE od 1 stycznia do 30 września 2025 r.

Numery CVE w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	Razem
Liczba opublikowanych numerów CVE	4	9	11	15	22	3	6	36	**16**	**122**

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – IX 2025

PAD CMS (CVE-2025-7063, CVE-2025-7065, CVE-2025-8116, CVE-2025-8117, CVE-2025-8118, CVE-2025-8119, CVE-2025-8120, CVE-2025-8121, CVE-2025-8122)

Liczba podatnych instancji	961
Liczba wysłanych ostrzeżeń	350

Seria podatności w oprogramowaniu PAD CMS, wykorzystywanym w wielu polskich podmiotach publicznych (urzędach gmin, bibliotekach, szkołach) do zarządzania treściami na stronach Biuletynu Informacji Publicznej. Najpoważniejsza z podatności umożliwiała nieuwierzytelnionemu użytkownikowi umieszczenie własnego skryptu na stronie. CERT Polska powiadomił użytkowników oprogramowania o konieczności jego zmiany, a także została w tej sprawie wydana rekomendacja Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.

Więcej: Podatności w oprogramowaniu PAD CMS

Cisco (CVE-2025-20333, CVE-2025-20363, CVE-2025-20362)

Liczba podatnych instancji	427
Liczba wysłanych ostrzeżeń	154

25 września opublikowano trzy podatności w systemach Cisco Secure Firewall Adaptive Security Appliance (ASA) i Cisco Secure Firewall Threat Defense (FTD), z czego dwie oceniono jako podatności krytyczne. Podatności wykorzystują nieprawidłową obsługę zapytań do serwera oraz umożliwiają dostęp do zasobów sieciowych bez prawidłowego uwierzytelnienia. Wykorzystanie podatności pozwala na zdalne wykonywanie kodu w zaatakowanej instancji, także z poziomu root (z najwyższymi uprawnieniami). CERT Polska obserwował aktywne wykorzystywanie podatności, stąd zalecana jest natychmiastowa aktualizacja oprogramowania do wersji 9.23.1.19 w przypadku Cisco ASA i 7.7.10.1 w przypadku Cisco FTD.

Więcej: Podatności w oprogramowaniu CISCO

FortiWeb (CVE-2025-52970)

Liczba podatnych instancji	66
Liczba wysłanych ostrzeżeń	24

W oprogramowaniu Fortinet FortiWeb z powodu niedostatecznej weryfikacji danych wejściowych atakujący może wysłać żądanie, które pozwala na podszycie się pod użytkownika, który ma w danym momencie aktywną sesję. W najgorszym przypadku może to być konto administratora, co dawałoby atakującemu pełną kontrolę nad systemem.

Więcej: Podatność w oprogramowaniu Fortinet FortiWeb

FreePBX (CVE-2025-57819)

Liczba podatnych instancji	45
Liczba wysłanych ostrzeżeń	31

Podatność krytyczna w oprogramowaniu FreePBX służącym do zarządzania centralą telefoniczną umożliwia utworzenie cyklicznie wykonywanego polecenia poprzez wstrzyknięcie szkodliwego zapytania do bazy danych. Takie polecenie może zawierać instrukcje umożliwiające atakującemu zdalne wykonanie kodu lub utworzenie nowego użytkownika.

Więcej: Podatność w oprogramowaniu FreePBX

Fortra GoAnywhere (CVE-2025-10035)

Liczba podatnych instancji	3
Liczba wysłanych ostrzeżeń	3

Podatność w oprogramowaniu Fortra GoAnywhere poprzez wykorzystanie błędu w odpakowywaniu danych (deserializacji) pozwala nieuwierzytelnionemu atakującemu wysłać specjalnie spreparowany obiekt Java. Odczytanie go przez serwer może uruchomić ciąg złośliwych działań i pozwolić napastnikowi wykonać dowolne polecenia w systemie oraz umożliwić mu zdalne przejęcie kontroli nad maszyną.

Więcej: Podatność w oprogramowaniu Fortra GoAnywhere

Wybrane informacje

1 września Centrum Projektów Polska Cyfrowa ogłosiło konkurs grantowy **„Cyberbezpieczne Wodociągi”** w ramach Krajowego Planu Odbudowy i Zwiększania Odporności. Celem przedsięwzięcia jest wzmocnienie cyberodporności przedsiębiorstw działających w sektorze zbiorowego zaopatrzenia w wodę, objętych krajowym systemem cyberbezpieczeństwa. Beneficjenci programu otrzymają wsparcie finansowe na działania w trzech obszarach: organizacyjnym, technicznym i kompetencyjnym, co ma się przełożyć na ochronę danych, ciągłość działania i efektywność systemów IT oraz OT. Ponadto będą oni zobowiązani do korzystania z serwisu moje.cert.pl. Przedsięwzięcie jest realizowane przez **Centrum Projektów Polska Cyfrowa w partnerstwie z NASK-PIB**.

Więcej: nask.pl/NASK zabezpieczy wodociągi. Ponad 300 milionów złotych na cyberochronę

Zespół CERT Polska opublikował artykuł pt. **„Bezpieczeństwo twojej kieszeni, czyli jak ochronić swój telefon”**, w którym przedstawiono kluczowe informacje na temat bezpiecznego korzystania ze smartfonów. W artykule można przeczytać o zagrożeniach, wśród których jest m.in. złośliwe oprogramowanie, można też zapoznać się z rekomendacjami dotyczącymi zarówno konfiguracji urządzeń mobilnych, jak i codziennych nawyków użytkowników, które mają wpływ na odpowiedni poziom bezpieczeństwa smartfonów.

Więcej: cert.pl/Bezpieczny telefon

NASK

W dniach 2–4 września podczas XXXIV Forum Ekonomicznego **w Karpaczu** odbyło się **VII Forum Cyberbezpieczeństwa** organizowane przez NASK-PIB i Ministerstwo Cyfryzacji. Uczestnicy tegorocznej edycji dużo uwagi poświęcili tematyce zapewnienia kontroli nad krajową infrastrukturą krytyczną. W tym kontekście rozmawiano zarówno o fizycznych zasobach, takich jak serwery czy centra danych, jak i o budowaniu silnych, lokalnych kompetencji technologicznych w obszarze bezpieczeństwa cyfrowego. Podczas dyskusji i paneli rozmawiano także o strategicznej niezależności cyfrowej państwa oraz o dostosowaniu polskiego prawa do regulacji unijnych (NIS 2, CRA).

Więcej: nask.pl/VII Forum Cyberbezpieczeństwa

11 września w Warszawie odbyła się konferencja **SECURITY CASE STUDY 2025**, poświęcona bezpieczeństwu teleinformatycznemu. W trakcie tego wydarzenia kierownik zespołu CERT Polska oraz ekspert z CERT Orange Polska dzielili się doświadczeniami związanymi ze współpracą zespołów bezpieczeństwa z **moje.cert.pl** – od skanowania i identyfikacji podatności do kompleksowej strategii działań naprawczych.

Więcej: X/CERT Polska/SCS 2025

CERT.PL NASK

17 września zespół CERT Polska opublikował artykuł pt. **„Jak rozpoznać fałszywe strony internetowe i uniknąć phishingu”**, w którym na podstawie przykładów została przedstawiona niezawodna technika weryfikacji autentyczności witryn polegająca na analizie adresów URL. W tekście omówiono również funkcje bezpieczeństwa przeglądarek wspierające użytkowników w identyfikacji prawdziwych domen.

Więcej: cert.pl/Jak rozpoznać fałszywe strony internetowe

19 września na stronie nask.pl ukazał się artykuł pt. **„Moje.cert.pl – platforma, która przybliża cyberbezpieczeństwo”**. Zwrócono w nim uwagę na funkcjonalność dostępną także dla niezarejestrowanych użytkowników serwisu moje.cert.pl. Mowa o powiadomieniach zawierających ostrzeżenia o aktualnych zagrożeniach w polskiej cyberprzestrzeni oraz o podatnościach. Komunikaty te, przygotowane przez ekspertów z CERT Polska, można odczytywać bezpośrednio na stronie moje.cert.pl, można też otrzymywać je w wiadomości e-mail.

Więcej: nask.pl/moje.cert.pl – platforma, która przybliża cyberbezpieczeństwo

---

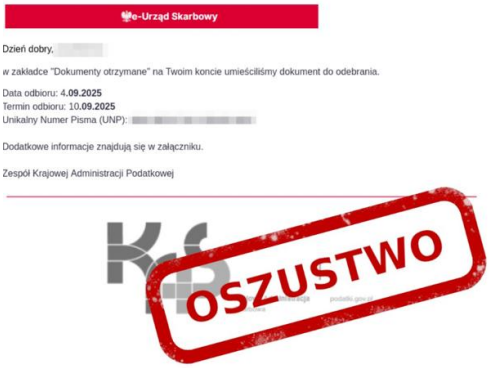
22 września zespół CERT Polska informował o **wycieku danych na publicznym kanale Telegram** oraz podpowiadał użytkownikom, jak zweryfikować, czy ich dane wyciekły, oraz jak należy postępować w takim przypadku.

Więcej: X/CERT Polska/Wyciek danych

Komunikaty o zagrożeniach

Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.

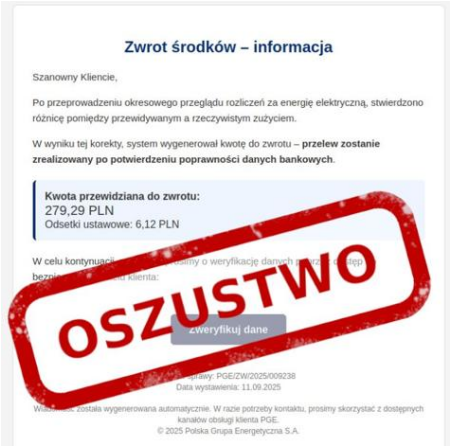
Zespół CERT Polska ostrzegał przed nowym wariantem wyłudzenia na „zwrot środków”. W tej odsłonie oszuści wykorzystują wizerunek Narodowego Funduszu Zdrowia. Spreparowane wiadomości e-mail zawierają link, który prowadzi do strony wyłudzającej dane osobowe i karty płatniczej, co umożliwia oszustom kradzież pieniędzy z konta bankowego.



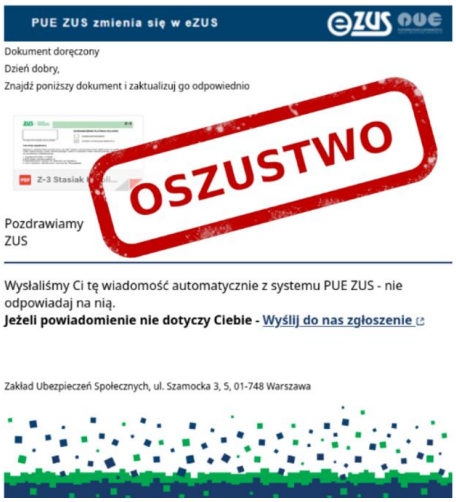
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod e-Urząd Skarbowy. Dystrybucja phishingu odbywa się za pomocą wiadomości e-mail zawierających informację o rzekomo dostępnym dokumencie do odebrania. W załączniku wiadomości znajduje się plik HTML, który po otwarciu w przeglądarce wyświetla panel logowania służący do wyłudzania danych uwierzytelniających do poczty elektronicznej. W ten sposób oszuści uzyskują dostęp do skrzynki użytkownika.

Zespół CERT Polska informował o podatności w narzędziu Omnissa Workspace ONE UEM | AirWatch MDM, która jest aktywnie wykorzystywana wobec polskich podmiotów. CERT Polska zwraca uwagę, że mogło dojść do odczytu danych przed instalacją aktualizacji, dlatego zaleca weryfikację, czy w systemie znajdują się ślady nieautoryzowanego działania. Atakujący uzyskane dane może opublikować lub zażądać okupu w zamian za ich niepublikowanie.

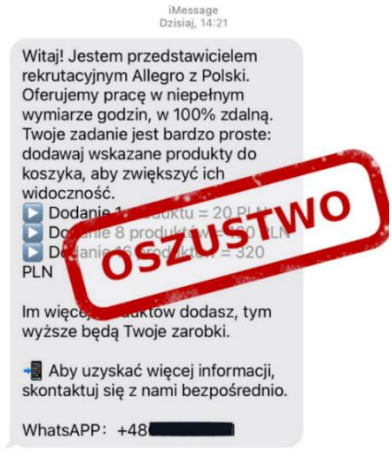
Więcej: moje.cert.pl/Krytyczna podatność w narzędziu Omnissa Workspace ONE UEM | AirWatch MDM



Zespół CERT Polska ostrzegał przed oszustwem wykorzystującym motyw okresowych przeglądów rozliczeń za energię. W tym wariancie oszuści podszywają się pod PGE i wysyłają wiadomości e-mail, w których informują o zwrocie środków w związku z nadpłatą. W wiadomości zawarty jest link prowadzący na fałszywą stronę, na której oszuści wykradają dane karty płatniczej.



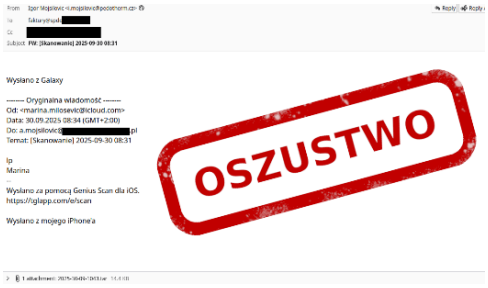
Zespół CERT Polska przestrzegał przed fałszywymi wiadomościami e-mail, w których oszuści wykorzystują wizerunek ZUS. W wiadomości pojawia się informacja o doręczeniu dokumentu i konieczności jego aktualizacji. Rzekomy dokument to w rzeczywistości obrazek udający załącznik – po kliknięciu na miniaturkę pobiera się złośliwe oprogramowanie, które może umożliwić przestępcom dostęp do zainfekowanego urządzenia, w tym m.in. wykradanie haseł do kont.



Zespół CERT Polska wraz z Allegro ostrzegał przed kolejną falą wyłudzeń, w których oszuści podszywają się pod rekruterów i w fałszywych wiadomościach SMS nie tylko proponują zdalną pracę i podejrzanie wysokie zarobki, lecz także zachęcają do dalszego kontaktu na WhatsAppie. W wiadomościach opisane są też zadania, które przyszły pracownik miałby wykonywać, takie jak ocenianie produktów na platformach sprzedażowych w zamian za niewielkie kwoty. Środki, którymi obracają oszuści na tym etapie, prawdopodobnie pochodzą z innych przestępstw, a cały schemat służy zbudowaniu zaufania. Następnym krokiem jest namawianie do fałszywych inwestycji, które prowadzą do strat liczonych w tysiącach złotych.

Zespół CERT Polska informował o oszustwie polegającym na zamieszczaniu w serwisach Facebook oraz Instagram reklam informujących o możliwości zakupu biletów np. na koncert zespołu Metallica czy Dawida Podsiadło. Fałszywe reklamy odsyłają na strony imitujące serwisy eBilet, mticket czy TicketShop. Spreparowane witryny teoretycznie oferują kilka opcji płatności, jednak aktywna jest wyłącznie płatność przez BLIK. Gdy transakcja zostanie potwierdzona, pieniądze trafią do oszustów.

Zespół CERT Polska obserwował kolejną odsłonę kampanii podszyć pod Narodowy Fundusz Zdrowia. Wiadomości e-mail rozsyłane przez oszustów zawierają link, który prowadzi do strony wyłudzającej dane osobowe i karty płatniczej. W poście, w którym został opisany ten przypadek, przypomniano użytkownikom o tym, by zawsze sprawdzali adres nadawcy wiadomości oraz adres strony internetowej, na której planują podać swoje dane.

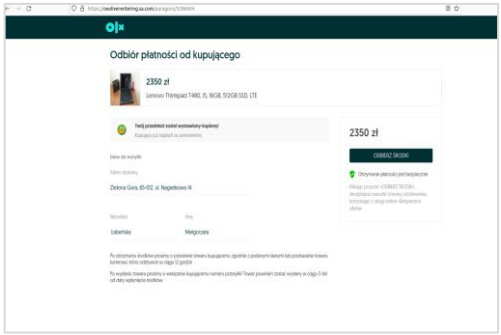


Zespół CERT Polska ostrzegał przed kampaniami dystrybucji szkodliwego oprogramowania. W wiadomościach e-mail oszuści umieszczają krótki tekst oraz załącznik. Tytuły wiadomości, m.in. „Skanowanie” czy „Dokumenty do podpisu”, sugerują, że użytkownik będzie musiał otworzyć załącznik. W tym wariancie oszuści nie podszywają się pod znane instytucje, liczą na ciekawość odbiorcy. Należy zwracać uwagę na rozszerzenia plików – formaty takie jak .tar, .exe, .js czy .7z mogą być wskazówką, że zawartość załącznika jest inna, niż sugerują tytuł i treść e-maila.

Więcej: Facebook/CERT Polska, X/CERT Polska oraz moje.cert.pl/komunikaty

Opis najczęściej występujących kampanii – IX 2025

OLX

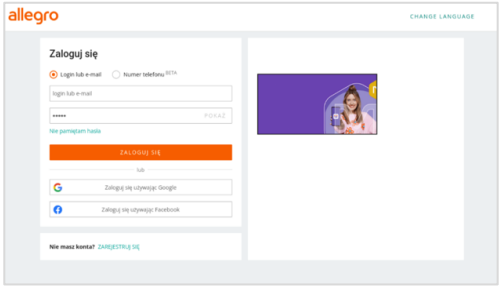


Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Oszuści kontaktują się z potencjalną ofiarą przez komunikator WhatsApp. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że zapłacili za zamówienie, a w kolejnym kroku wysyłają link do strony internetowej, poprzez którą rzekomo można wypłacić środki. Oprawa graficzna witryny przypomina stronę OLX, InPostu, DPD, DHL lub Poczty Polskiej. Znajduje się na niej fałszywy panel płatniczy. Podanie danych karty powoduje utratę środków finansowych przechowywanych na koncie bankowym.

Fałszywe strony oferujące wysokodochodowe inwestycje

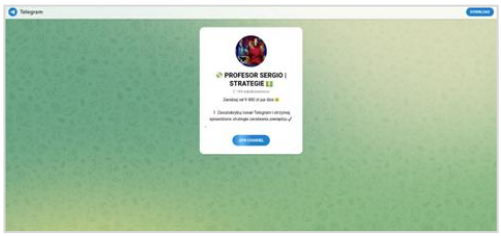
Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy, instytucje, m.in. Lotos, Tesla, PGNiG i PGE. Oszuści reklamują w mediach społecznościowych czy w wyszukiwarkach internetowych nieistniejące programy dla akcjonariuszy indywidualnych, rozsyłają wiadomości. Informują w nich o możliwości inwestowania środków z rzekomo wysokim zyskiem za pośrednictwem platform inwestycyjnych. Osoby zainteresowane dużymi zarobkami oraz inwestycjami w handel ropą, gazem czy akcje firmy są proszone o udostępnienie swoich danych osobowych i kontaktowych (w formularzu, do którego prowadzi link umieszczony w wiadomości). Następnie z użytkownikiem kontaktuje się telefonicznie osoba podająca się za konsultanta i zachęca do zainwestowania środków w kryptowaluty, obligacje czy akcje firm na platformie, która jak się okazuje, uniemożliwia wypłaty zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

Allegro



Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

Telegram Web



Zespół CERT Polska obserwował kampanię phishingową, w której wykorzystywany jest wizerunek komunikatora Telegram Web. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

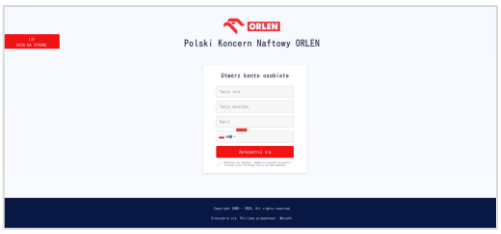
Gazeta.pl

Zespół CERT Polska rejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis Gazeta.pl. Na fałszywych stronach oszuści publikują artykuły, w których opisują inwestycje znanych osób w kryptowaluty, obligacje czy akcje na platformie inwestycyjnej. Platforma ta w rzeczywistości uniemożliwia wypłatę zainwestowanych pieniędzy, a celem oszustów jest wyłudzenie środków finansowych.

TVN

Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego TVN. Na fałszywych stronach internetowych znajdują się artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Orlen



Zespół CERT Polska w dalszym ciągu rejestrował kampanię phishingową, w której wykorzystywany jest wizerunek Orlenu. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

Polsat News

Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego Polsat News. Na fałszywych stronach internetowych umieszczają artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Baltic Pipe

Zespół CERT Polska obserwował wzmożoną kampanię phishingową rzekomo powiązaną z projektem inwestycyjnym Baltic Pipe. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

Onet.pl

Zespół CERT Polska obserwował wzmożoną kampanię phishingową, w której oszuści wykorzystują wizerunek serwisu Onet.pl do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.