STYCZEŃ 2026

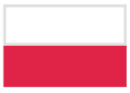
Podsumowanie Miesiąca CERT POLSKA

Nr 1/2026

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki zarejestrowanych zagrożeń

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki prezentowane poniżej obejmują dane o liczbie zarejestrowanych zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez zespół CERT Polska w okresie od 1 do 31 stycznia 2026 r.
Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

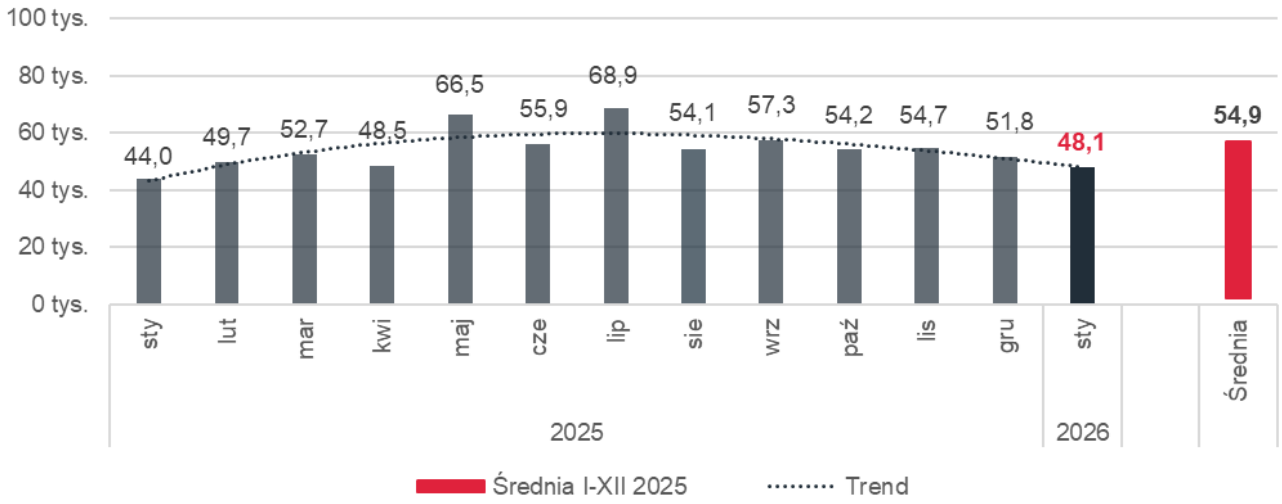
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – I 2026

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 31 stycznia 2026 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**48,1 tys.**
w tym zarejestrowane (obsłużone) incydenty	**19,4 tys.**

W styczniu 2026 r. zespół CERT Polska otrzymał łącznie **48,1 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **19,4 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 I 2025 do I 2026

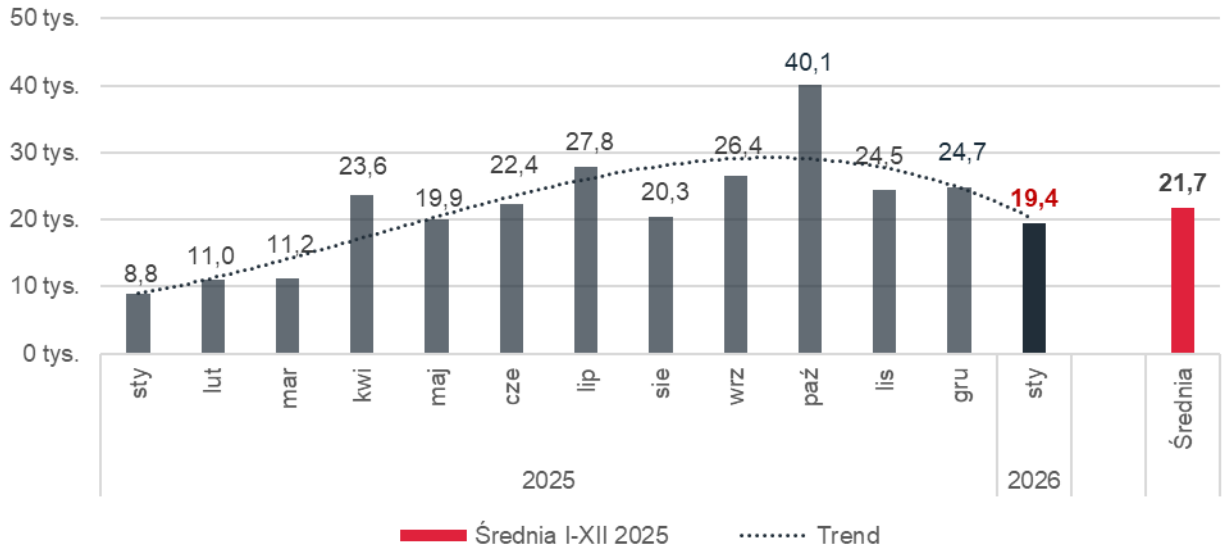


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.01.2025 do 31.01.2026. Źródło: CERT Polska / CSIRT NASK.

[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 w styczniu 2026 r. wyniosła **48,1 tys.** i nie przekroczyła średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 9%**. W stosunku do grudnia 2025 r. był to **spadek o 7%.**

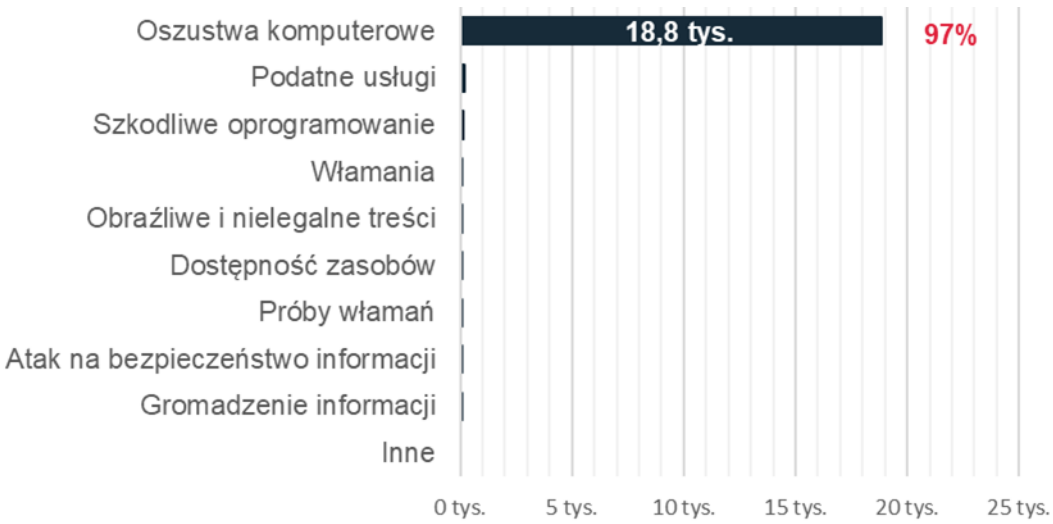
Zarejestrowane incydenty cyberbezpieczeństwa od I 2025 do I 2026



Wykres 2. Liczba zarejestrowanych incydentów od 01.01.2025 do 31.01.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w styczniu 2026 r. wyniosła **19,4 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w styczniu 2026 r. **zwiększyła się o 119%** i pozostawała poniżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do grudnia 2025 r. liczba zarejestrowanych incydentów **zmniejszyła się o 22%**.

Rodzaje zarejestrowanych zagrożeń – I 2026



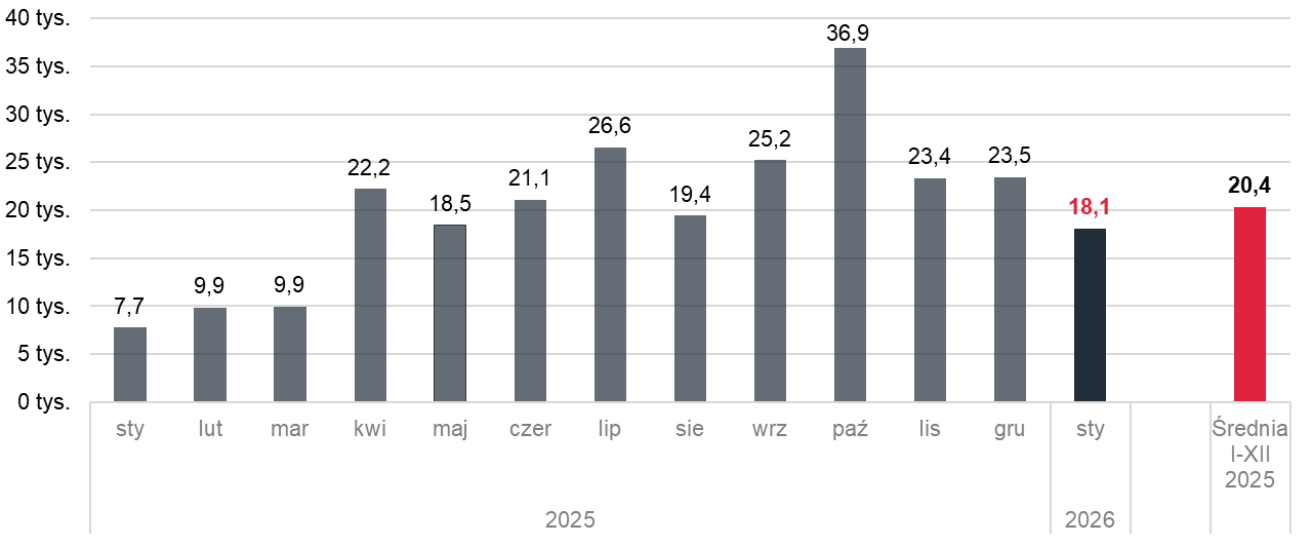
Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 31 stycznia 2026 r. Źródło: CERT Polska / CSIRT NASK.

W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**19,4 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*). W styczniu 2026 r. łącznie odnotowano **6,4 tys.** tego typu incydentów.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska od I 2025 do I 2026

Na Listę Ostrzeżeń wpisywane są domeny, które wprowadzają użytkowników w błąd i wyłudzają od nich dane. Takie domeny są blokowane na okres **6 miesięcy**. Po upływie tego czasu, jeśli nadal zawierają niebezpieczne treści, zostają **ponownie wpisane na listę** jako nowy wpis.

Lista Ostrzeżeń jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do **automatycznego blokowania dostępu do szkodliwych stron internetowych**, co pozwala ograniczać skutki ataków phishingowych i innych kampanii wymierzonych w obywateli Polski.



Wykres 4. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

W styczniu 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **18,1 tys.** nazw szkodliwych domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do grudnia 2025 r. **zmniejszyła się o 23%**.

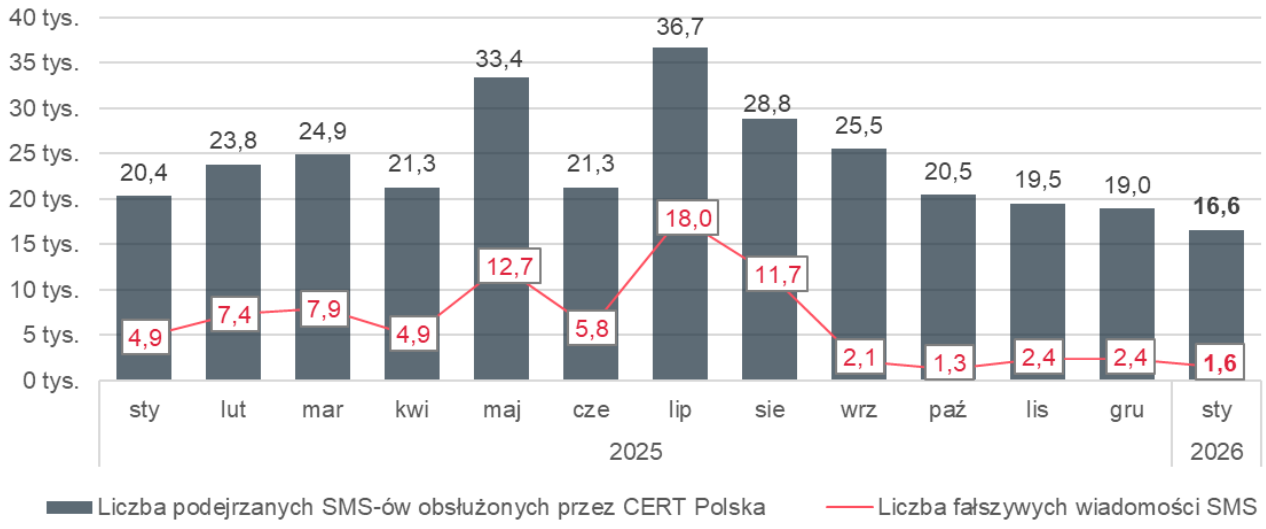
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

0lxadostawa.info; admin.booking.id0718.com; adwokat-pl.online; allegro.04805.click; allegro.oferta-4595486.sbs; alliegro.vip; disneyklienta.com; dzieci.okazja-pl.top; e-doreczenia.mc-gov.pl; edugate-ac.com; eobuwie.cccosibella-pl.sbs; e-zdrowle.pl; futureinvestwave.com; gazinvestgroup.com; globalinvestlink.com; ipko-pl-client.pro; northline-investments.com; olx.005102.com; olx.ochronakupujaceg013718391731.cfd; orlen.evmt.top; rabat-dzieci.top; santander-pl-1.top; sidebayhotel.com; smyk-pl.sbs; technologyinsport.com; topgazeta24.eu; userverif773-booking.com; vinted.195739.vu; vinted.pl-59151.pl; weryfikacja-podatki-gov.pl

Liczba zgłoszeń wiadomości SMS przyjętych przez CERT Polska od I 2025 do I 2026

W styczniu 2026 r. zespół CERT Polska zarejestrował **16,6 tys.** zgłoszeń podejrzanych SMS-ów. W porównaniu z grudniem 2025 r. był to **spadek o 12%**. Wśród ogółu SMS-ów przyjętych w styczniu 2026 r. **fałszywe wiadomości**, czyli takie, w których nadawca podszywa się pod inny podmiot, aby skłonić odbiorcę wiadomości do określonego działania – np. podania danych osobowych, przekazania pieniędzy, wejścia na stronę internetową lub instalacji oprogramowania, **stanowiły 9%**.



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

Wzorce fałszywych wiadomości SMS – I 2026

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, np. banków, firm kurierskich, platform inwestycyjnych. CSIRT NASK zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi Urzędu Komunikacji Elektronicznej i przedsiębiorcom telekomunikacyjnym. Podejrzane SMS-y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**. W styczniu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **108,5 tys.** SMS-ów. Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

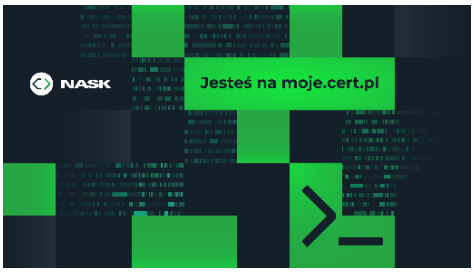
Wzorce fałszywych wiadomości SMS w 2026	styczeń
Liczba wytworzonych wzorców	**118**

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

Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił 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.

W styczniu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 512 nowych użytkowników**.



W okresie od 1 do 31 stycznia 2026 r. CERT Polska wysłał **5,8 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności lub 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 (więcej: CERT Polska/CNA). W styczniu 2026 r. zespół CERT Polska nadał **16** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. Asseco InfoMedica Plus, Kieback&Peter Neutrino-GLT oraz w aplikacji mobilnej Crazy Bubble Tea.

Lista opublikowanych podatności dostępna jest na stronie: CERT Polska/CVE

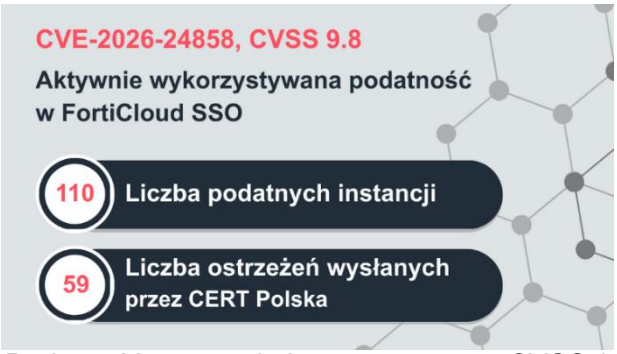
Tabela 3. Nadane numery CVE od 1 do 31 stycznia 2026 r.

Numery CVE w 2026	styczeń
Liczba opublikowanych numerów CVE	**16**

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – I 2026

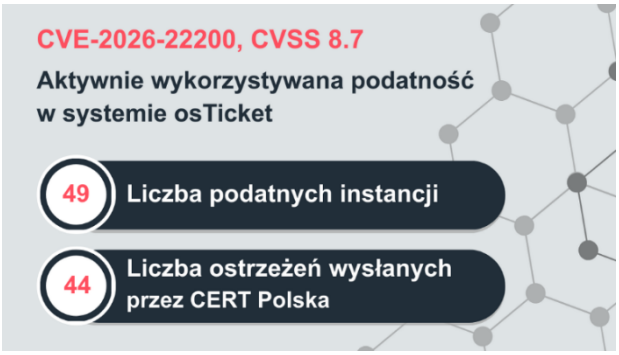
W wyniku nieprawidłowego przetwarzania jednego z parametrów żądania HTTP atakujący mógł skonstruować specjalnie spreparowane żądanie umożliwiające dostęp do wrażliwych plików systemowych, w tym plików zawierających dane niezbędne do utworzenia sesji administratorskiej. Uzyskanie dostępu do instancji n8n na tym poziomie prowadziło do możliwości zdalnego wykonania kodu (RCE). Przeprowadzenie ataku nie wymagało uwierzytelnienia ze strony atakującego. Podatność otrzymała krytyczną ocenę CVSS (ang. *Common Vulnerability Scoring System*) 10.0.

Więcej: https://www.cyera.com/research-labs/ni8mare-unauthenticated-remote-code-execution-in-n8n-cve-2026-21858



W wyniku błędnej interpretacji odpowiedzi SAML atakujący byli w stanie obejść mechanizmy bezpieczeństwa systemu SSO. Podatność ta umożliwiała nieautoryzowany dostęp poprzez manipulację treścią komunikatów uwierzytelniających. Analogiczny mechanizm zaobserwowano w przypadku podatności CVE-2025-59718, gdzie odpowiedzi SAML były wykorzystywane do omijania zabezpieczeń firewalla. Podatność otrzymała krytyczną ocenę CVSS 9.8.

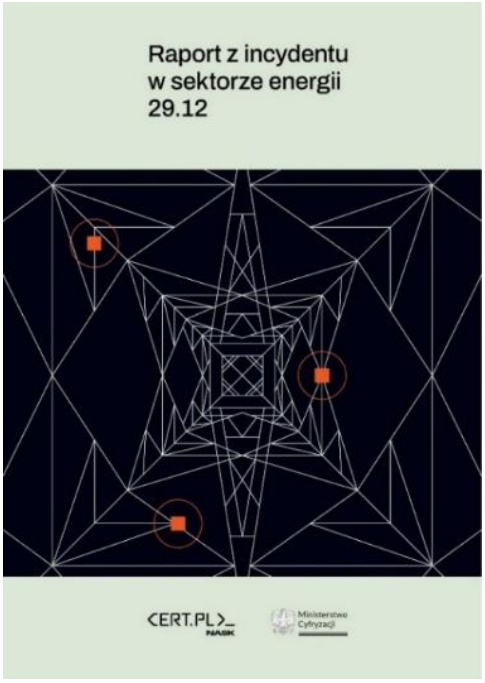
Więcej: https://www.secpod.com/blog/from-sso-to-sos-how-cve-2026-24858-gave-hackers-the-keys-to-your-fortinet-gear



Poprzez wysłanie odpowiednio spreparowanego zgłoszenia do systemu atakujący mógł wprowadzić wyrażenia z języka PHP, które z uwagi na niewystarczającą sanityzację były następnie przekazywane do modułu odpowiedzialnego za generowanie plików PDF przy eksporcie do tego formatu. Atakujący mógł dzięki temu uzyskać lokalne pliki serwerowe w postaci bitmap. Podatność otrzymała wysoką ocenę CVSS 8.7.

Więcej: https://horizon3.ai/attack-research/attack-blogs/ticket-to-shell-exploiting-php-filters-and-cnext-in-osticket-cve-2026-22200

Wybrane informacje



Zespół CERT Polska opublikował „Raport z incydentu w sektorze energii 29.12” zawierający szczegółową analizę techniczną oraz przebieg skoordynowanych ataków w polskiej cyberprzestrzeni, które miały miejsce pod koniec ubiegłego roku. Zaatakowano wówczas ponad 30 farm wiatrowych i fotowoltaicznych, spółkę prywatną z sektora produkcyjnego oraz elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców w Polsce. Zdarzenia miały wpływ zarówno na systemy informatyczne, jak i na fizyczne urządzenia przemysłowe, co jest rzadko spotykane w dotychczas opisywanych atakach. Raport pokazuje, że odnotowane ataki są znaczną eskalacją w porównaniu ze zdarzeniami obserwowanymi przez CERT Polska do tej pory.

Więcej: cert.pl/Raport z incydentu w sektorze energii z 29 grudnia 2025 roku

W styczniu wprowadzono zmiany w serwisie **moje.cert.pl** – ma on teraz nową stronę startową oraz lepiej widoczne statystyki dotyczące liczby przeskanowanych domen, subdomen i znalezionych podatności lub błędnych konfiguracji. Dodatkowo w zakładce „Komunikaty" publikowane są ostrzeżenia przygotowywane przez zespół CERT Polska oraz jego partnerów.

Więcej: moje.cert.pl

15 stycznia we Wrocławiu odbyła się konferencja „**Disinfoverse – Different Dimensions of (Un)Certainty"** zorganizowana przez CEDMO (Central European Digital Media Observatory). Podczas tego wydarzenia analizowano m.in., jak nauka, media i dziennikarstwo oraz instytucje publiczne funkcjonują w warunkach chaosu informacyjnego. Ekspert z CERT Polska w prezentacji wstępnej do panelu pt. „Cybersecurity and the influence of foreign disinformation campaigns" mówił o aktywności grup APT i dezinformacji w kontekście cyberprzestępczości w Polsce.

Więcej: cedmohub.eu/Disinfoverse Different Dimensions of (Un)Certainty

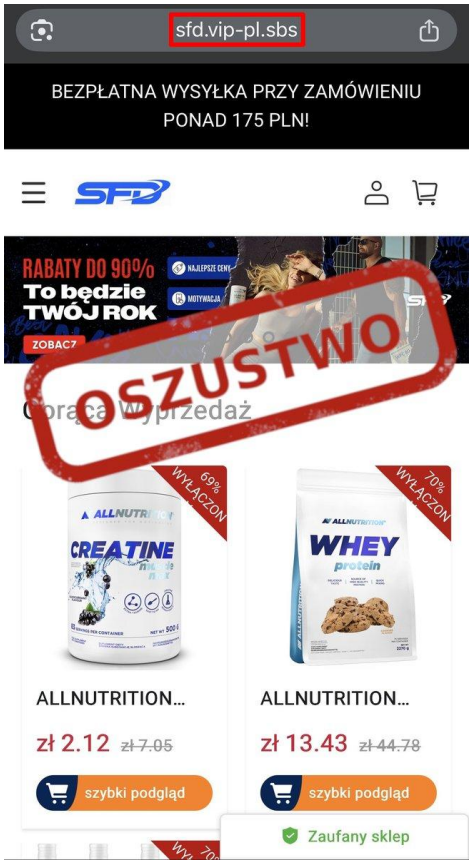
---

28 stycznia w Warszawie odbył się **Kongres Ochrony Danych i Nowych Technologii** zorganizowany przez Urząd Ochrony Danych Osobowych oraz Krajową Izbę Radców Prawnych. Uczestnicy wydarzenia, wśród których byli także eksperci z NASK-PIB, podczas wystąpień i paneli poruszali takie tematy, jak przyszłość regulacyjna sztucznej inteligencji, ochrona małoletnich w internecie, deepfake, ochrona danych w dobie cyberprzestępczości. W czasie dyskusji pt. „Cyberincydenty a naruszenia" ekspertka z NASK-PIB przedstawiła zagadnienie z perspektywy zadań zespołu CERT Polska związanych z analizą przypadków ransomware i wycieków danych, mówiła także o możliwościach ochrony domen i sieci, jakie daje serwis moje.cert.pl.

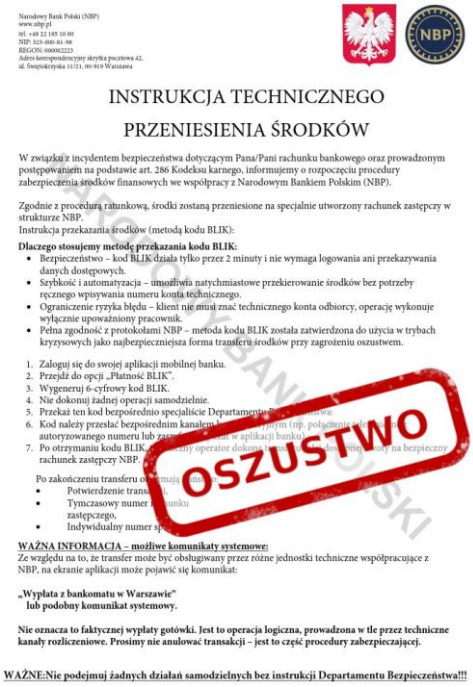
Więcej: uodo.gov.pl/Kongres Ochrony Danych i Nowych Technologii

Komunikaty o zagrożeniach

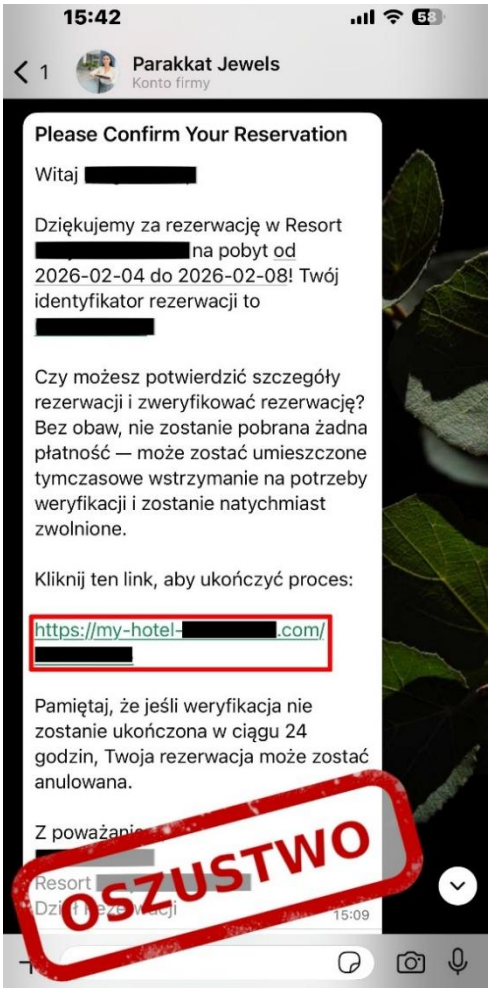
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



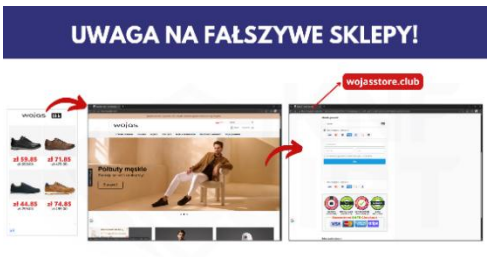
Zespół CERT Polska informował o kampanii, w której przestępcy wykupują reklamy na Facebooku dotyczące dietetycznych przekąsek, odżywek, białka oraz suplementów. Reklamy te sugerują, że oferta pochodzi ze sklepu SFD. Kliknięcie w reklamę prowadzi jednak do fałszywej strony podszywającej się pod prawdziwy sklep. Celem oszustów jest wyłudzenie pieniędzy. Warto zwracać szczególną uwagę na adres strony, a także sprawdzać regulamin sklepu i jego politykę prywatności.



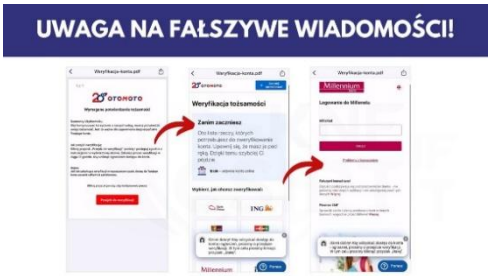
Zespół CERT Polska obserwował nawracające kampanie oszustw wykorzystujących schemat „na policjanta". Polega on na tym, że przestępcy podszywają się pod państwowe służby lub instytucje, preparują pisma, w których informują o rzekomym zagrożeniu dla konta bankowego odbiorcy wiadomości, a następnie zachęcają do wypłaty, przekazania im kodu szybkiego przelewu lub przelania środków na przygotowane konto. Oszuści chętnie korzystają z narzędzi opartych na sztucznej inteligencji, by generować wiarygodne materiały. Treść takich pism coraz rzadziej zawiera błędy językowe, gramatyczne czy ortograficzne, dlatego tak ważne jest, żeby nauczyć się rozpoznawać socjotechniki wykorzystywane przez przestępców. Elementy, które powinny wzbudzić czujność odbiorcy, to: presja czasu, obietnica kary lub nagrody, powoływanie się na autorytet instytucji czy zniechęcanie do weryfikacji nadawcy lub zastosowania innych form kontaktu.



Zespół CERT Polska obserwował wzmożone wykorzystywanie schematu oszustwa „na rezerwację noclegu". Przestępcy korzystają z przejętych kont hoteli lub z wcześniejszych wycieków danych, żeby kontaktować się z klientami, którzy wykupili nocleg. Za pośrednictwem popularnych komunikatorów wysyłają link do strony imitującej pośrednika rezerwacji. Zarówno treść wiadomości, jak i wygląd fałszywej strony są precyzyjnie dopasowane do rezerwacji odbiorcy. Celem jest wyłudzenie danych osobowych i danych karty płatniczej.



Zespół CERT Polska udostępnił ostrzeżenie CSIRT KNF przed fałszywymi sklepami na TikToku. Oszuści przygotowują spreparowane reklamy oferujące „super rabaty". Kliknięcie w link przenosi na stronę do złudzenia przypominającą sklep internetowy. Gdy użytkownik próbuje dokonać zakupu, jest przenoszony na stronę wyłudzającą dane osobowe i dane karty płatniczej. CSIRT KNF zidentyfikował ponad 300 fałszywych reklam.

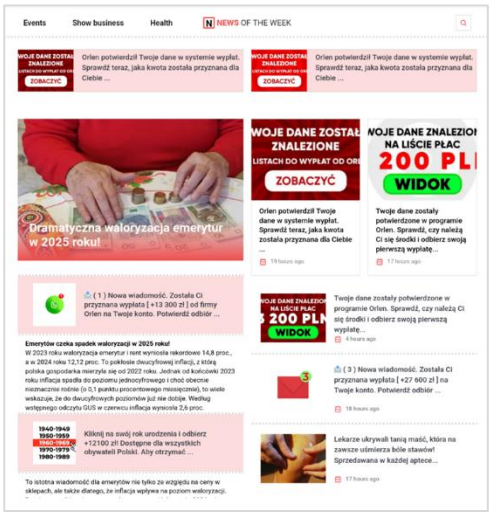


Zespół CERT Polska udostępnił ostrzeżenie CSIRT KNF przed fałszywą weryfikacją konta na OtoMoto. Oszuści wysyłają wiadomości zawierające plik „weryfikacja_konta.pdf". Dokument zawiera informację o konieczności potwierdzenia tożsamości w celu dalszego korzystania z platformy. Po kliknięciu w przycisk „Przejdź do weryfikacji" użytkownik zostaje przekierowany na stronę zawierającą logotypy banków. Następnie po wyborze banku pojawia się fałszywa strona logowania. Celem oszustów jest wyłudzenie danych logowania do bankowości elektronicznej.

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

Opis najczęściej występujących kampanii – I 2026

Fałszywe strony oferujące wysokodochodowe inwestycje

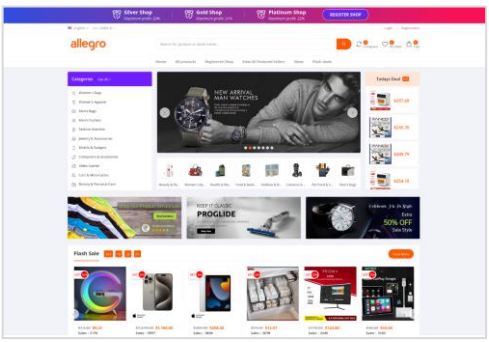


Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy, instytucje, m.in. Lotos, Tesla, PGNiG i PGE. Oszuści reklamują w mediach społecznościowych czy w wyszukiwarkach internetowych nieistniejące 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 reklamie lub 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.

Fałszywe strony kanału Polsat News

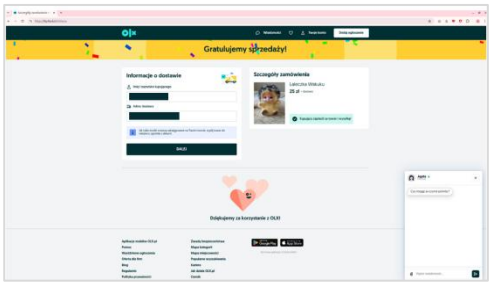
Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego Polsat News. Na fałszywych stronach internetowych umieszczają artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Fałszywe strony 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.

Fałszywe strony OLX

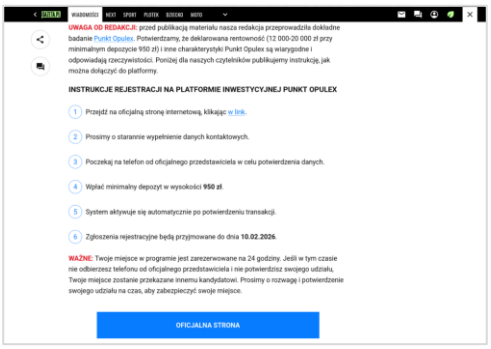


Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Oszuści kontaktują się z potencjalną ofiarą przez komunikator WhatsApp. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że zapłacili za zamówienie, 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 firmy Orlen

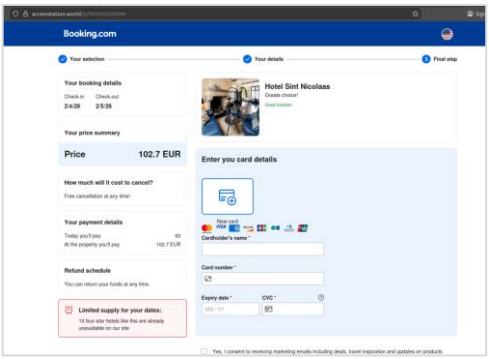
Zespół CERT Polska obserwował kampanię phishingową, w której wykorzystywany jest wizerunek Orlenu. Cel oszustów to wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

Fałszywe strony serwisu 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 rzekome inwestycje w kryptowaluty, obligacje czy akcje na platformie inwestycyjnej. Platforma ta w rzeczywistości uniemożliwia wypłatę zainwestowanych pieniędzy, a celem oszustów jest wyłudzenie środków finansowych.

Fałszywe rezerwacje serwisu Booking.com

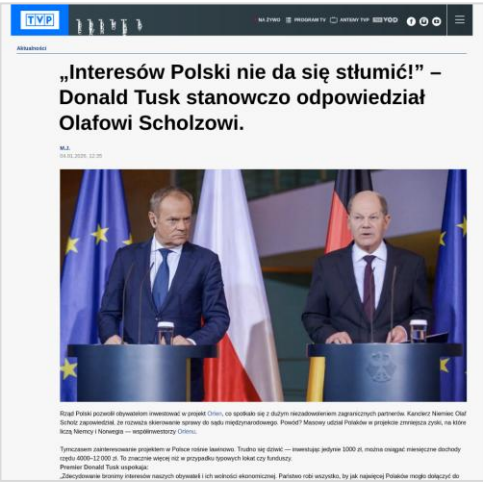


Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek serwisu Booking.com. Na fałszywej stronie internetowej znajduje się panel logowania, za pomocą którego oszuści wykradają dane osobowe i dane karty płatniczej użytkowników serwisu.

Fałszywe strony podszywające się pod serwis gov.pl

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

Fałszywe strony Telewizji Polskiej (TVP)



Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek strony internetowej Telewizji Polskiej. Na fałszywych witrynach oszuści umieszczają artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Fałszywe strony kanału 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.