MAJ 2026

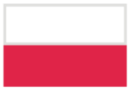
# Podsumowanie Miesiąca CERT POLSKA

Nr 5/2026

CERT.PL NASK

CSIRT NASK

# PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR



Autor: zespół CERT Polska

# SPIS TREŚCI

# Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów

## Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki przedstawione w tym rozdziale obejmują dane o liczbie zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 31 maja 2026 r. Wybrane dane ujęto również w szerszym horyzoncie czasowym, aby umożliwić obserwację zmian zachodzących w dłuższym okresie.

W dniu 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC), która zmieniła definicje ustawowe, wprowadziła nowe kategorie podmiotów – podmioty kluczowe oraz podmioty ważne – a także rozszerzyła zakres raportowania o potencjalne zdarzenia dla cyberbezpieczeństwa (art. 2 pkt 11e), cyberzagrożenia (art. 2 pkt 4a) oraz poważne cyberzagrożenia (art. 2 pkt 11f). Nowelizacja zmodyfikowała również zasady klasyfikacji incydentów oraz poszerzyła katalog sektorów i podmiotów objętych ustawą. W konsekwencji dane publikowane od kwietnia 2026 r. mogą nie być w pełni porównywalne z danymi z okresów wcześniejszych.

### Zgłoszone zagrożenia oraz zarejestrowane incydenty – V 2026

**Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 31 maja 2026 r.**

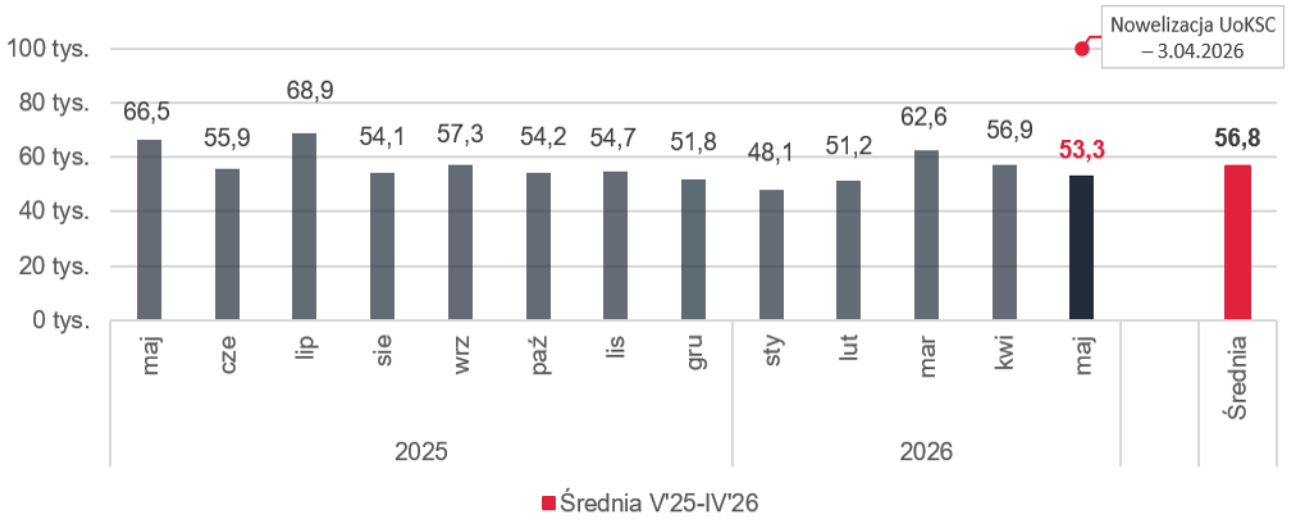
| Zgłoszone zagrożenia i zarejestrowane incydenty | Liczba |
|---|---|
| Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa* | 7,4 tys. |
| Zgłoszenia cyberzagrożeń* | 34,4 tys. |
| Zgłoszenia incydentów | 10,2 tys. |
| Zgłoszenia poważnych cyberzagrożeń* | 1,3 tys. |
| **Razem zgłoszenia** | **53,3 tys.** |
| **Zarejestrowane incydenty**** | **21,9 tys.** |

* Nowe kategorie zgłoszeń raportowane od kwietnia 2026 r. ** Incydenty zostały zarejestrowane na podstawie zgłoszeń incydentów, zgłoszeń cyberzagrożeń, zgłoszeń poważnych cyberzagrożeń oraz zgłoszeń potencjalnych zdarzeń dla cyberbezpieczeństwa.

[1] Zgłoszenia przesyłane są za pośrednictwem formularza dostępnego na stronie https://incydent.cert.pl lub są wysyłane na adres zgłoszeniowy cert@cert.pl, a także poprzez system S46. Otrzymane informacje o zagrożeniach stanowią podstawę rejestracji nowych incydentów.

W maju 2026 r. zespół CERT Polska otrzymał **łącznie 53,3 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 21,9 tys. incydentów** cyberbezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. 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.

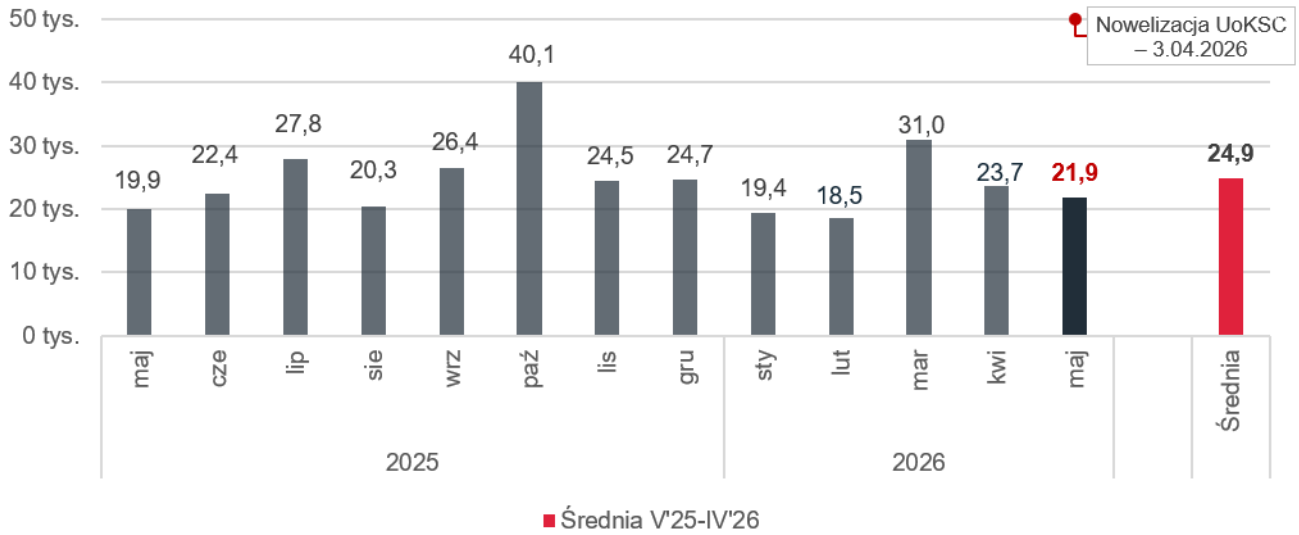
## Zgłoszenia zagrożeń od V 2025 do V 2026




**Wykres 1. Liczba wszystkich zgłoszeń od 01.05.2025 do 31.05.2026. Źródło: CERT Polska / CSIRT NASK.**

Liczba wszystkich zgłoszeń odnotowanych w maju 2026 r. pozostawała poniżej średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zmniejszyła się o 20%**. W stosunku do kwietnia 2026 r. odnotowano **spadek o 6%**.

## Zarejestrowane incydenty cyberbezpieczeństwa od V 2025 do V 2026



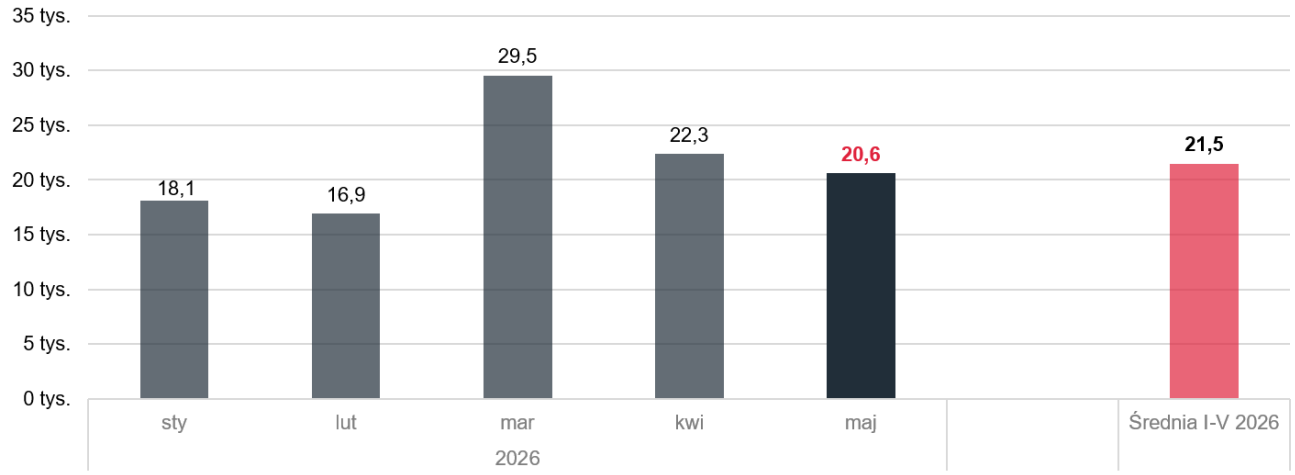

**Wykres 2. Liczba zarejestrowanych incydentów od 01.05.2025 do 31.05.2026. Źródło: CERT Polska / CSIRT NASK.**

Liczba incydentów zarejestrowanych w maju 2026 r. wyniosła **21,9 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w maju 2026 r. **zwiększyła się o 10%** i pozostawała poniżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do kwietnia 2026 r. odnotowano **spadek liczby incydentów o 7%**.

## Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–V 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.

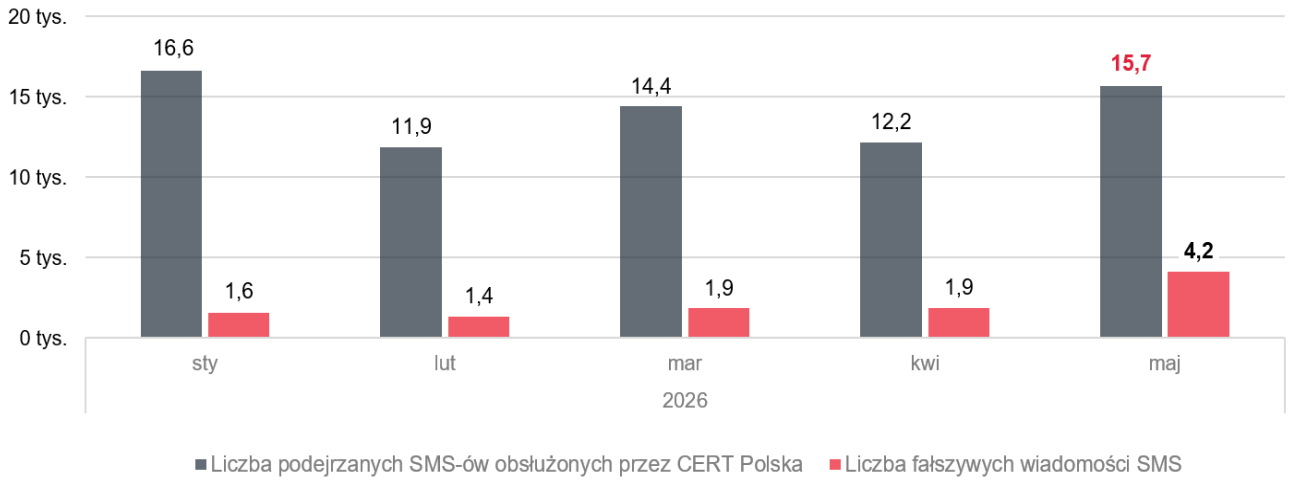



**Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.**

Od 1 stycznia do 31 maja 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **107,5 tys.** szkodliwych domen, z czego w maju 2026 r. dodano **20,6 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do kwietnia 2026 r. **zmniejszyła się o 8%**.

## Liczba zgłoszeń wiadomości SMS przyjętych przez CERT Polska I–V 2026

Od 1 stycznia do 31 maja 2026 r. zespół CERT Polska zarejestrował **70,8 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w maju 2026 r. wyniosła **15,7 tys.** W porównaniu z kwietniem 2026 r. był to **wzrost o 29%**. Wśród ogółu SMS-ów przyjętych w maju 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 27%**.




**Wykres 4. Liczba SMS-ów zgłoszonych do CSIRT NASK w danym miesiącu.**

## Wzorce fałszywych wiadomości SMS I–V 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 maju 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **48,7 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.**

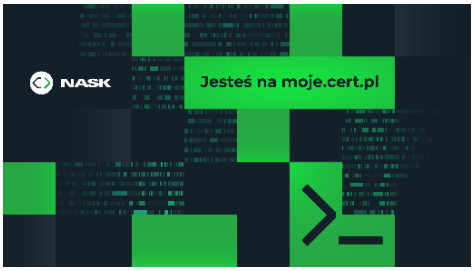
| Wzorce fałszywych wiadomości SMS w 2026 | sty | lut | mar | kwi | maj | Razem |
|---|---|---|---|---|---|---|
| Liczba wytworzonych wzorców | 118 | 97 | 85 | 80 | **105** | **485** |

**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 maju 2026 r. w serwisie moje.cert.pl **zarejestrowało się 632 nowych użytkowników**.




W okresie od 1 do 31 maja 2026 r. CERT Polska wysłał **7,7 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 maju 2026 r. zespół CERT Polska nadał **34** numery CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. QuickCMS, Lifetime, Szafir SDK, kamer Kenik. Przykładem podatności

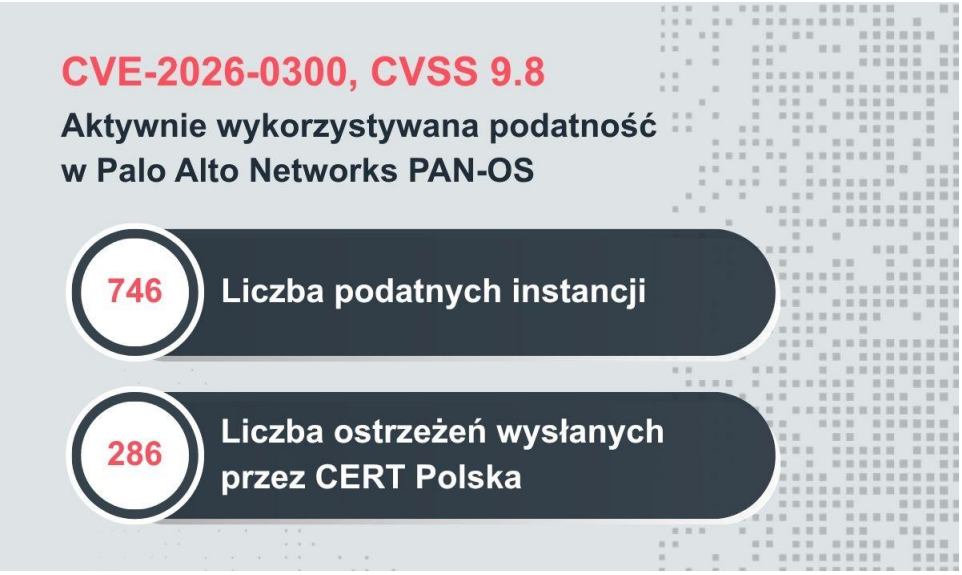
wykrytej przez zespół CERT Polska w ramach badań własnych była podatność w oprogramowaniu Request Tracker.

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

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

| Numery CVE w 2026 | sty | lut | mar | kwi | maj | Razem |
|---|---|---|---|---|---|---|
| Liczba opublikowanych numerów CVE | 16 | 12 | 32 | 21 | **34** | **115** |

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




Krytyczna podatność typu buffer overflow (CWE-787: Out-of-bounds Write) w usłudze User-ID Authentication Portal (Captive Portal) systemu PAN-OS umożliwia nieuwierzytelnionemu atakującemu zdalne wykonanie dowolnego kodu z uprawnieniami root na urządzeniach PA-Series i VM-Series poprzez wysłanie specjalnie spreparowanych pakietów.

Podatność dotyczy wyłącznie firewalli z włączonym User-ID Authentication Portal udostępnionym na interfejsie dostępnym z niezaufanych sieci. W wyniku raportowanych przypadków aktywnego wykorzystania podatności CVE trafiło do katalogu CISA KEV (Known Exploited Vulnerabilities). Atakujący może przejąć pełną kontrolę nad urządzeniem firewall, modyfikować reguły bezpieczeństwa, przechwytywać ruch sieciowy oraz uzyskać trwały dostęp do infrastruktury sieciowej.

**Więcej:** https://security.paloaltonetworks.com/CVE-2026-0300

# Wybrane informacje


13 i 14 maja w Poznaniu odbyła się **konferencja Impact'26**, jedno z najważniejszych europejskich wydarzeń poświęconych technologii, gospodarce, kulturze i tematyce społecznej. We wspólnej strefie Ministerstwa Cyfryzacji, NASK – PIB i Centralnego Ośrodka Informatyki spotykali się i dyskutowali eksperci w dziedzinie cyberbezpieczeństwa i sztucznej inteligencji, twórcy, dziennikarze. Spotkania były poświęcone takim tematom, jak ochrona infrastruktury krytycznej, cyfrowa suwerenność i odpowiedzialne wykorzystywanie danych oraz sztucznej inteligencji.
W ramach wydarzenia odbyła się także debata „Zdarzyło się w CERT – na styku zbrodni online i offline", która była okazją do rozmowy o roli ekspertów z zespołu CERT Polska w zabezpieczaniu cyfrowych śladów po ataku hakerskim na łódzki szpital w 2022 r., a także o codziennej pracy zespołu oraz o skali cyberzagrożeń.

**Więcej:** nask.pl/Anatomia cyberprzestępstw. NASK na Impact'26

---


14 maja zespół CERT Polska opublikował artykuł pt. **„Autonomiczny proces fuzzingu pod nadzorem LLM"** poświęcony projektowi badawczemu **fuzzlab**, rozwijanemu przez ekspertów z CERT Polska w ramach Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania (FUMAL). Fuzzing to technika automatycznego testowania oprogramowania, która polega na podawaniu losowych lub celowo zniekształcanych danych wejściowych w celu wykrywania błędów i luk bezpieczeństwa. To bardzo skuteczna metoda, jednak wymaga długich przygotowań przed uruchomieniem. System fuzzlab pod nadzorem LLM samodzielnie wykonuje dotychczasową pracę badaczy – od analizy kodu, przez generowanie testów, po klasyfikację znalezisk i tworzenie raportów dla twórców testowanego oprogramowania.

**Więcej:** cert.pl/Autonomiczny proces fuzzingu pod nadzorem LLM


25 maja zespół CERT Polska opublikował poradnik pt. **„Dobre praktyki zarządzania bezpieczeństwem oprogramowania”**. Opracowanie to zawiera rekomendacje obejmujące rozwiązania organizacyjne i techniczne, które mają wspomóc producentów oprogramowania i produktów z elementami cyfrowymi w wypełnianiu wymagań wynikających z rozporządzenia Cyber Resilience Act (CRA). Obowiązki producentów to m.in. ocena ryzyka w kontekście cyberbezpieczeństwa i wdrożenie uporządkowanego procesu obsługi podatności. Zgodnie z przepisami nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zespół CERT Polska, wykonując zadania CSIRT NASK, pełni funkcję koordynatora procesu ujawniania podatności. W związku z tym zespół realizuje zadania związane ze zgłoszeniami wynikającymi z przepisów CRA.

**Więcej:** cert.pl/CRA – nowe obowiązki dla producentów oprogramowania i korzyści dla użytkowników

# Wystąpienia ekspertów CERT Polska

- 13 maja – kierownik CERT Polska podczas konferencji CyberTek Tech Festival w Katowicach wystąpił z prelekcją pt. „29 grudnia: kulisy incydentu w sektorze energii”, w której omówił sam incydent, jego kontekst oraz najważniejsze wnioski i lekcje, które można z niego wynieść.

  **Więcej:** cybertek.com.pl/agenda
- 20 maja – kierownik CERT Polska przedstawił krajobraz cyberzagrożeń na podstawie raportu rocznego CERT Polska za 2025 r., konferencja CyberGov, Warszawa.

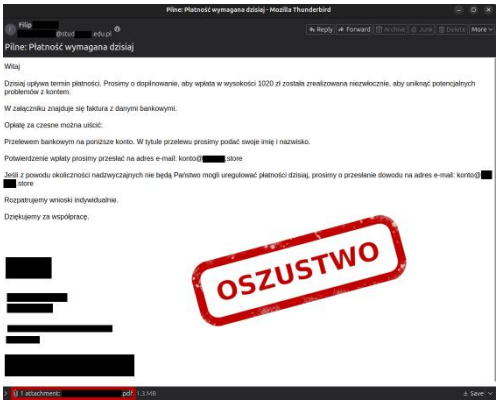
  **Więcej:** cybergov.pl

# Komunikaty o zagrożeniach

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

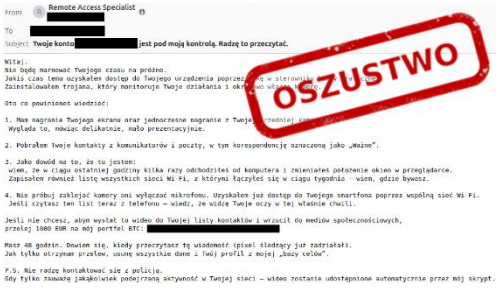

Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek firmy OpenAI. Wysyłają e-maile o rzekomej konieczności ponowienia płatności za dostęp do ChatGPT, a link zawarty w wiadomości prowadzi do strony wyłudzającej dane kart płatniczych.

---




Zespół CERT Polska informował o kampanii phishingowej wymierzonej w środowisko akademickie. Pod pretekstem zaległej opłaty za studia oszuści próbują wyłudzić pieniądze. Wiadomości przychodzą ze skrzynek mailowych w domenie uczelni. Przestępcy wykorzystują przejęte konta studentów, doktorantów i pracowników uniwersytetu, aby dotrzeć do pozostałych członków społeczności akademickiej.

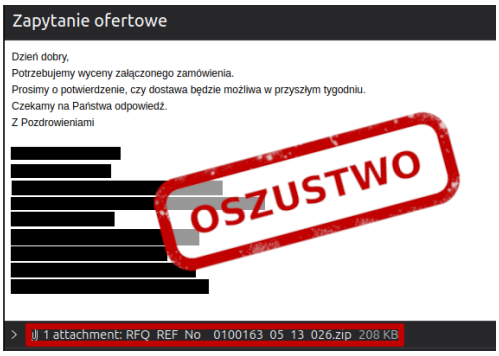
---




Zespół CERT Polska otrzymywał zgłoszenia dotyczące znanego schematu spamu opartego na szantażu. Cyberprzestępcy masowo wysyłają wiadomości e-mail, w których informują o rzekomym dostępie do prywatnych danych, nagrań z kamery, historii przeglądania lub innych materiałów z urządzenia. Następnie podają numer portfela kryptowalut i oczekują opłacenia „okupu" w zamian za niepublikowanie prywatnych danych. Kampania wykorzystuje spoofing, czyli podszywanie się pod adres nadawcy. Wiadomość wygląda, jakby została wysłana z własnej skrzynki odbiorcy lub z domeny znanej instytucji.


Zespół CERT Polska obserwował kampanię wymierzoną w pracowników firm i organizacji. Cyberprzestępcy podszywają się pod zespoły HR i informują o rzekomej aktualizacji zasad lub konieczności zapoznania się z nowymi dokumentami. Elementem fałszywej wiadomości jest kod QR, który ma umożliwiać szybkie przejście do „firmowego systemu”. Po zeskanowaniu kodu użytkownik zostaje przekierowany na stronę przypominającą portal Microsoft 365, gdzie jest zachęcany do podania hasła do swojego konta. Dane logowania trafiają następnie do cyberprzestępców i mogą zostać wykorzystane do dalszych, bardziej precyzyjnych ataków.

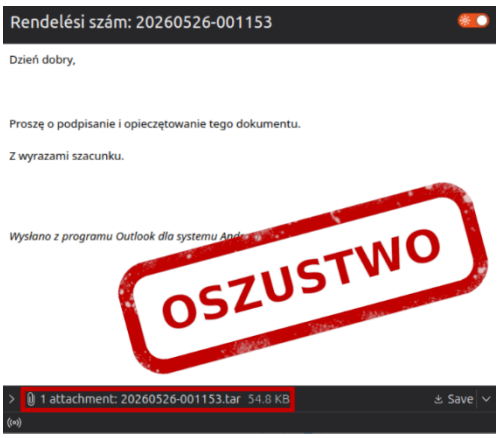
---



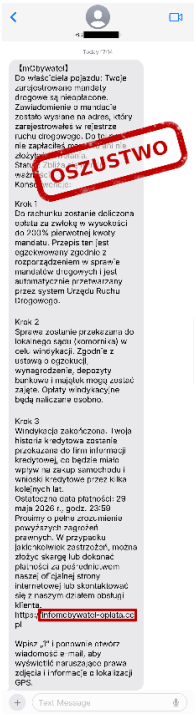

Zespół CERT Polska informował o kampanii dystrybucji szkodliwego oprogramowania, w której przestępcy wysyłają wiadomości związane z rzekomą wyceną produktów lub usług. Wykorzystują w tym celu dane prawdziwych firm i ich pracowników pozyskane ze źródeł dostępnych w internecie. Oszuści zachęcają do otwarcia załącznika pod pretekstem zapoznania się ze szczegółami zamówienia. Załączony plik zawiera szkodliwe oprogramowanie typu RAT (Remote Access Trojan). Po jego pobraniu i uruchomieniu przestępcy uzyskują zdalny dostęp do urządzenia, co pozwala na kradzież danych lub zmianę konfiguracji komputera.


Zespół CERT Polska obserwował kampanię phishingową, w której przestępcy podszywają się pod bank Erste (wcześniej Santander). Oszuści wykorzystują niedawną zmianę nazwy banku i pod groźbą ograniczenia dostępu do konta nakłaniają do rzekomej aktualizacji i weryfikacji danych teleadresowych oraz numeru rachunku. Link zawarty w wiadomości e-mail prowadzi do strony internetowej o szacie graficznej zbliżonej do oficjalnej strony banku. Na stronie znajduje się formularz wyłudzający login i hasło do bankowości internetowej, które następnie trafiają do przestępców.

---




Zespół CERT Polska informował o kampanii dystrybucji szkodliwego oprogramowania, w której przestępcy rozsyłają wiadomości e-mail zawierające prośbę o „podpisanie i opieczętowanie” dokumentu zawartego w załączniku. Do wiadomości dołączany jest plik z rozszerzeniem .tar, który zawiera szkodliwe oprogramowanie z rodziny AgentTesla. Po rozpakowaniu i uruchomieniu zawartości załącznika dochodzi do infekcji urządzenia. AgentTesla to malware służący m.in. do kradzieży danych, takich jak loginy, hasła czy informacje zapisane w przeglądarkach i klientach poczty. Dane te mogą zostać wykorzystane do dalszych ataków phishingowych, przejmowania kont czy wyłudzeń.

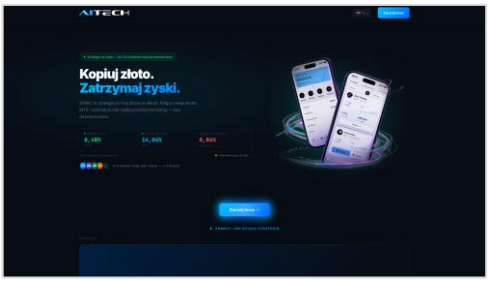



Zespół CERT Polska monitorował kampanię wykorzystującą wiadomości tekstowe, w której oszuści podszywają się pod serwis mObywatel i informują o rzekomo nieopłaconych mandatach drogowych. Fałszywe wiadomości zawierają groźby konsekwencji prawnych, dodatkowych opłat i negatywnego wpływu na historię kredytową. Schemat ma na celu wyłudzenie informacji, które mogą posłużyć do dalszych przestępstw. Link prowadzi do strony, na której użytkownik proszony jest najpierw o podanie numeru rejestracyjnego pojazdu, a następnie danych karty płatniczej. Dodatkowym elementem wywierania presji są krótkie terminy płatności oraz fałszywe informacje o dowodach wykroczenia w postaci zdjęć i lokalizacji GPS, które mają skłonić odbiorcę do szybkiego działania.

**Więcej:** Facebook/CERT Polska, X/CERT Polska, moje.cert.pl/komunikaty, Linkedin.com/CERT Polska

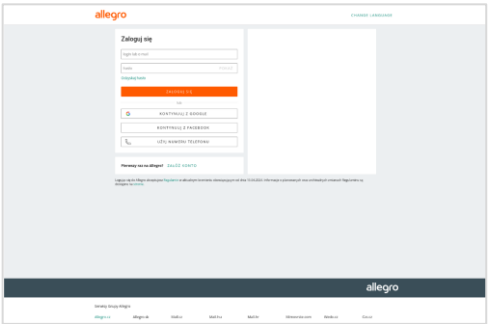
# Opis najczęściej występujących kampanii – V 2026

## 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 i instytucje, m.in. Lotos, Tesla, PGNiG, PGE, Baltic Pipe. Oszuści reklamują w mediach społecznościowych oraz w wyszukiwarkach internetowych nieistniejące programy dla akcjonariuszy indywidualnych, a także rozsyłają wiadomości, w których informują 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 później okazuje – uniemożliwia wypłaty zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

## Fałszywe strony Allegro

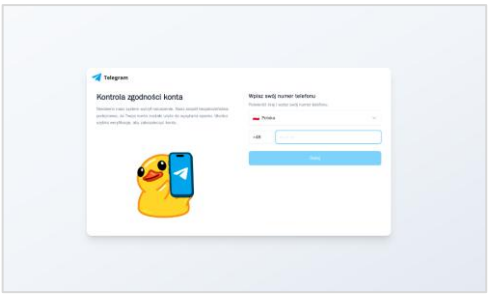



Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

## Fałszywe strony 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 wykorzystują wizerunki znanych osób do promowania inwestycji 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 komunikatora Telegram

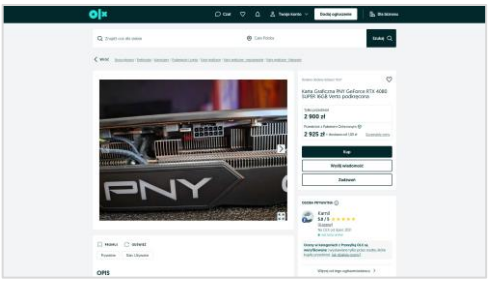



Zespół CERT Polska obserwował kampanię mającą na celu przejmowanie kont użytkowników komunikatora Telegram. Oszuści wysyłają wiadomości SMS z informacją, że konto użytkownika mogło brać udział w wysyłce spamu. Link zawarty w wiadomości prowadzi do strony internetowej, która wyłudza numer telefonu. Następnie użytkownik jest proszony o wpisanie kodu weryfikacyjnego wysłanego na jego numer – podanie go umożliwia atakującym przejęcie konta Telegram.

## Fałszywe strony serwisu gov.pl


Zespół CERT Polska rejestrował incydenty, w których oszuści na spreparowanych stronach internetowych łudząco podobnych do stron serwisu gov.pl umieszczają artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem jest wyłudzenie środków finansowych.

## Fałszywe strony OLX



Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Panel logowania do tego serwisu służy do wyłudzania od użytkowników danych uwierzytelniających.

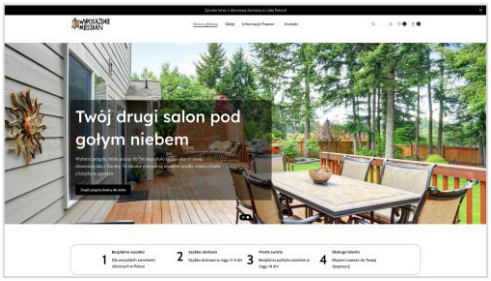
## Fałszywe strony firmy Orlen


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

## Fałszywe strony serwisu Onet.pl


Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod serwis Onet.pl i umieszczają na fałszywych stronach internetowych artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

## Fałszywe strony sklepów internetowych




Zespół CERT Polska rejestrował incydenty, w których oszuści tworzą fałszywe sklepy internetowe zawierające towary w atrakcyjnych cenach. Na tych stronach zazwyczaj nie ma możliwości zapłaty za pobraniem, a na wielu z nich jedyną metodą płatności jest karta płatnicza.

## 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, i zachęcają czytelników do rejestracji na platformie, która w rzeczywistości służy do wyłudzania środków finansowych.