Tysiące oszukanych, setki podejrzanych. Alarmujące dane

Kategoria: Aktualności
Opublikowano: wtorek, 10, marzec 2026 07:56
Alicja Cisowska

CERT Polska w 2025 roku zarejestrował 658,3 tys. zgłoszeń cyberzagrożeń oraz 260,8 tys. incydentów cyberbezpieczeństwa. Liczba zgłoszeń wzrosła o 10 proc. rok do roku, natomiast liczba incydentów zwiększyła się o 152 proc. w porównaniu z 2024 rokiem. Dane organów ścigania wskazują na rosnącą skalę przestępczości w sieci. W ubiegłym roku zarzuty karne w sprawach dotyczących cyberprzestępczości usłyszało ponad 1,3 tys. podejrzanych.

Dane procesowe Policji pokazują wzrost liczby czynności prowadzonych w sprawach dotyczących cyberprzestępczości. Z podsumowania działań Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) wynika, że w 2025 roku funkcjonariusze zatrzymali 1177 osób. Zarzuty karne przedstawiono 1374 podejrzanym, spośród których 417 decyzją sądów zostało tymczasowo aresztowanych. To wzrost we wszystkich tych kategoriach średnio o 30 proc. w porównaniu do 2024 roku.

– *W ostatnich latach liczba odnotowanych postępowań z zakresu cyberprzestępczości wzrosła. Choć nie mamy definicji cyberprzestępczości, to opieram się na danych, które sięgają nieco głębiej, nie tylko bazują na samej kwalifikacji prawnej, ale również na opisach czynów. Wzrosła liczba postępowań dotyczących na przykład hackingu czy kradzieży tożsamości, natomiast zdecydowanie dominują oszustwa. Oszustwo jako przestępstwo z art. 286 Kodeksu karnego nie jest typowym cyberprzestępstwem, ale na tym w zasadzie skupia się aktywność sprawców* – podkreśla dr hab. inż. Agnieszka Gryszczyńska, dyrektorka Departamentu ds. Cyberprzestępczości i Informatyzacji w Prokuraturze Krajowej.

Jak wskazują statystyki CERT Polska i CSIRT NASK, w grudniu ubiegłego roku zdecydowanie najczęściej występującą kategorią zagrożeń online były oszustwa komputerowe. Stanowiły one 98 proc. ogółu obsłużonych incydentów (24,7 tys.). 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).

Tego typu oszustwa znajdują się na celowniku funkcjonariuszy CBZC i Prokuratury Krajowej. Prowadzone postępowania dotyczą m.in. oszustw metodą „na pracownika banku" czy oszustw z wykorzystaniem kodów BLIK. W drugiej połowie 2025 roku policjanci z Poznania rozbili jedną ze zorganizowanych grup przestępczych, której członkowie wyłudzali pieniądze poprzez pozyskiwanie kodów BLIK. Podejrzani działali na terenie całego kraju i oszukali w ten sposób ok. 1,3 tys. osób na ponad 3 mln zł.

CBZC i Prokuratura Krajowa zajmują się również oszustwami inwestycyjnymi, polegającymi na tworzeniu i wykorzystywaniu fałszywych platform inwestycyjnych, podobnych z nazwy lub wyglądu do tych działających legalnie. Sprawcy często posługują się wizerunkami znanych osób oraz logotypami renomowanych firm, by zwabić klientów.

– *Mamy bardzo wielu pokrzywdzonych zarówno przez działania fałszywych sklepów internetowych, jak i pokrzywdzonych na bardzo wysokie kwoty w oszustwach inwestycyjnych, czyli przez strony, które stwarzają pozory inwestowania. Mamy oszustwa na legendę, na wnuczka, na policjanta. Mamy też oszustwa z kategorii love scam, czyli najpierw uwodzenie ofiary, a następnie żądanie różnego rodzaju kwot, które następnie ta ofiara przekazuje sprawcy* – wymienia dr inż. Agnieszka Gryszczyńska. – *Tylko w ubiegłym roku samych oszustw odnotowano około 160 tys., natomiast w policyjnych bazach danych już ponad połowa oszustw oflagowana jest jako popełnione online, tak więc tutaj cyberprzestępczość nam się ukrywa statystycznie.*

Kategoria: Aktualności
Opublikowano: wtorek, 10, marzec 2026 07:56
Alicja Cisowska
Odsłony: 462

Postępowania dotyczące cyberprzestępczości należą do najbardziej wymagających dowodowo kategorii spraw, ponieważ kluczowe informacje mają postać danych cyfrowych o często krótkim okresie retencji. W praktyce oznacza to konieczność szybkiego zabezpieczania logów, danych transmisyjnych oraz informacji przechowywanych przez dostawców usług, zanim zostaną one nadpisane lub usunięte.

– Mamy bardzo niską odpowiedzialność karną za przestępstwo hackingu. Przestępstwo to jest ścigane na wniosek, więc jeżeli pokrzywdzony nas nie zawiadomi, nie złoży wniosku, to w zasadzie takiego postępowania się nie wszczyna, a wszczęte umarza. Niewątpliwie problematyczne jest również to, że duża część podmiotów zawiadamia o incydencie na przykład CSIRT-y, natomiast nie składa od razu bezpośrednio po zdarzeniu zawiadomienia o podejrzeniu popełnienia czynu zabronionego – tłumaczy dyrektorka Departamentu ds. Cyberprzestępczości i Informatyzacji w Prokuraturze Krajowej. *– Nie możemy zatem na wstępnym etapie zabezpieczyć danych, a w ściganiu cyberprzestępców czas jest najważniejszy z uwagi na konieczność pozyskania danych bardzo często transgranicznie, czyli od różnych dostawców spoza Polski.*

Ważnym elementem walki z cyberprzestępcami jest zabezpieczane mienie. W 2025 roku śledczy z Centralnego Biura Zwalczania Cyberprzestępczości zabezpieczyli od podejrzanych ponad 80 mln zł. Policjanci odzyskali niemal 25 mln zł.

Prokuratura Krajowa i Centralne Biuro Zwalczania Cyberprzestępczości w kwietniu ubiegłego roku przeprowadziły wspólnie ogólnopolską operację „Fever" przeciwko rozpowszechnianiu pornografii z udziałem małoletnich w internecie. Zatrzymano wówczas 98 osób. Podobnie grudniowa operacja „Game Over", również dotycząca treści pedofilskich, doprowadziła do zatrzymania 100 osób i zarzutów dla 102 podejrzanych.

Źródło: Newseria