Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

04/2026

SPIS TREŚCI

Infrastruktura krytyczna, czyli co?

W kontekście zagrożeń hybrydowych i cyberbezpieczeństwa termin „infrastruktura krytyczna" odmieniany jest przez wszystkie przypadki. Jednak szafowanie tym pojęciem często jest błędem w odniesieniu do tego czym jest, a czym nie jest infrastruktura krytyczna. Warto więc powiedzieć na temat słów klika pokazać jaki jest związek IK z Krajowym Systemem Cyberbezpieczeństwa (KSC).

System ochrony infrastruktury krytycznej w Polsce został umiejscowiony w ramach systemu zarządzania kryzysowego, określonego ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (ustawa o zk). Zgodnie z ustawą o zk infrastrukturą krytyczną są wskazane na podstawie tej ustawy systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Również operatorzy infrastruktury krytycznej są wyznaczenie na podstawie ustawy o zk. Infrastrukturą krytyczną nie koniecznie musi więc, będzie coś, co się komuś wydaje, że nią jest.

Wyznaczeni na podstawie tej ustawy operatorzy infrastruktury krytycznej muszą realizować obowiązki wynikające z tejże ustawy (m.in. art. 6 oraz opracowywany na podstawie art. 5b Narodowy Program Ochrony Infrastruktury Krytycznej). Obecnie w parlamencie procedowany jest projekt nowelizacji ustawy o zk, który wdroży w Polsce unijną dyrektywę CER[1], co znacząco wzmocni system ochrony infrastruktury krytycznej, w tym poprzez postawienie szeregu wymogów, które będą musieli spełniać operatorzy IK, zarówno w wymierzę fizycznym jak i cyberbezpieczeństwa (projektowane nowe art. 6ze - 6zj).

Bytem odrębnym od systemu ochrony IK jest Krajowy System Cyberbezpieczeństwa, określony ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, której fundamentalna zmiana, polegająca m.in. na wdrożeniu dyrektywy NIS 2, weszła w życie w kwietniu 2026 roku. W ramach KSC funkcjonują Podmioty Kluczowe i Podmioty Ważne (które wraz z wejściem w życie nowelizacji ustawy o KSC zastąpiły Operatorów Usług Kluczowych i Dostawców Usług Cyfrowych).

W związku z tym Podmioty Kluczowe i Podmioty Ważne obecnie zobowiązane są zapewnić spełnianie odpowiednich wymogów cyberbezpieczeństwa, określonych w art. 8-16a, w szczególności poprzez wdrożenie systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniającym szereg określonych elementów określnych w art. 8.

Warto jednocześnie wskazać, że w ustawie o KSC przewidziano rozwiązania zapewniające synergię pomiędzy systemem ochrony IK a KSC, np. w zakresie wspólnego nadzoru (art. 53f), czy informowania organów właściwy do spraw podmiotów krytycznych przez CSIRT-y poziomu krajowego o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny (art. 26 ust. 16).

Źródło: opracowanie własne.

[1] Numer z wykazu prac legislacyjnych Rady Ministrów: UC47.

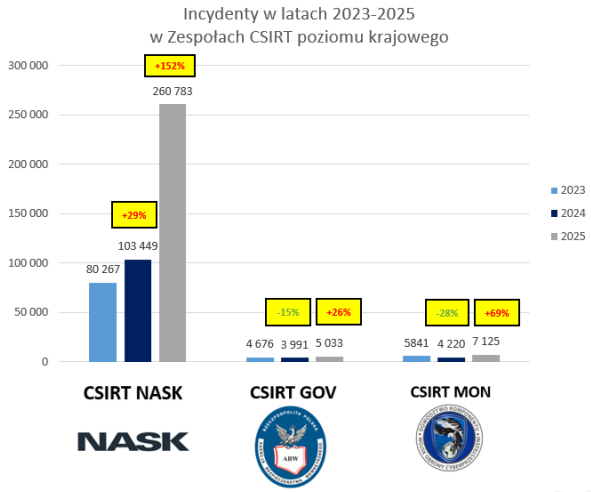
Rok bezprecedensowych wyzwań: Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2025 r.

W dniu 16.04.2026 r. Minister Cyfryzacji, a zarazem Pełnomocnik Rządu ds. Cyberbezpieczeństwa, pan Krzysztof Gawkowski, w trakcie konferencji prasowej w Ministerstwie Cyfryzacji opublikował Sprawozdanie Pełnomocnika za rok 2025. Ten coroczny dokument prezentuje w sposób obszerny stan bezpieczeństwa, poziom wyzwań i zagrożeń instytucji tworzących Krajowy System Cyberbezpieczeństwa (KSC), kreśląc obraz polskiej cyberprzestrzeni jako obszaru ścierania się nowoczesnych metod ochrony z coraz bardziej wyrafinowanymi formami agresji cyfrowej.

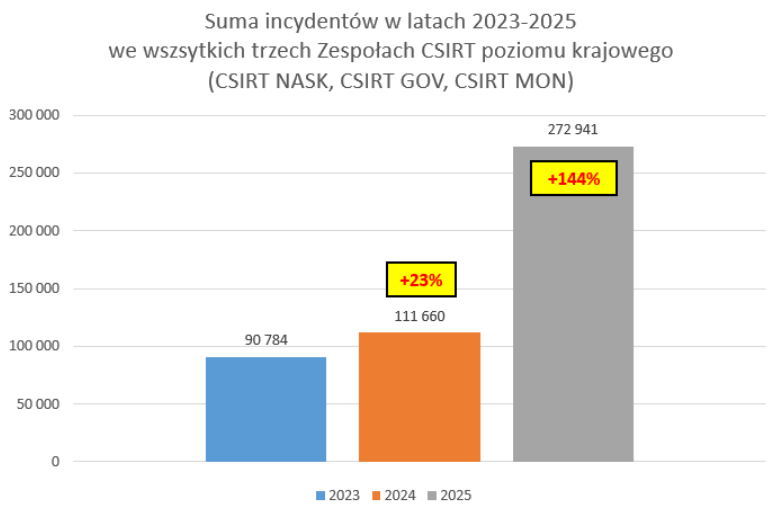
Miniony rok zapisał się w historii polskiej administracji jako czas wyjątkowej próby dla KSC. Z opublikowanego właśnie sprawozdania wyłania się obraz państwa znajdującego się pod stałą, rosnącą presją ze strony cyberprzestępców oraz obcych służb specjalnych. Dynamiczna ewolucja zagrożeń, napędzana postępem technologicznym i niestabilną sytuacją geopolityczną, wymusiła na instytucjach publicznych nie tylko wzmożoną czujność operacyjną, ale przede wszystkim głęboką refleksję nad modelem ochrony infrastruktury krytycznej.

Skokowy wzrost liczby incydentów

Dane operacyjne przedstawione w raporcie są alarmujące. W 2025 roku zespoły CSIRT poziomu krajowego obsłużyły łącznie blisko **273 tysiące incydentów**, co stanowi drastyczny wzrost o **144,4%** w stosunku do roku ubiegłego.



Przytłaczająca większość zdarzeń (ok. 95%) została zarejestrowana przez zespół **CSIRT NASK**, który obsłużył ponad 260 tysięcy incydentów (wzrost o 152%). Aż 97% tych spraw stanowiły oszustwa komputerowe, w tym masowe kampanie phishingowe uderzające w obywateli i samorządy. Wyraźne wzrosty aktywności odnotowały także pozostałe zespoły: **CSIRT MON** obsłużył 7 125 incydentów (wzrost o 69%), a **CSIRT GOV** – 5 033 (wzrost o 26%).



Główne trendy: AI jako „mnożnik siły”

Krajobraz zagrożeń w 2025 roku zdominowało złośliwe wykorzystanie sztucznej inteligencji (AI), która stała się dla adwersarzy potężnym narzędziem automatyzacji kampanii socjotechnicznych. Modele językowe umożliwiły generowanie bezbłędnych językowo wiadomości phishingowych, a technologia deepfake służyła do podszywania się pod urzędników w celu manipulacji.

Polska infrastruktura znajdowała się pod stałą presją grup APT powiązanych ze służbami Rosji i Białorusi. Najpoważniejszym przykładem był skoordynowany atak z końca grudnia, wymierzony w sektor energii, gdzie wykorzystano oprogramowanie niszczące dane (wiper) przeciwko farmom wiatrowym, fotowoltaicznym oraz elektrociepłowni. Niepokojącym trendem stały się także uderzenia w łańcuchy dostaw – atakujący coraz częściej obierali za cel słabiej zabezpieczonych podwykonawców usług IT/OT, aby uzyskać dostęp do systemów administracji rządowej.

Kryzys kadrowy i wyzwania NIS2

Raport wskazuje, że największą słabością systemu jest **krytyczny niedobór wykwalifikowanych specjalistów** oraz ograniczenia finansowe w sektorze publicznym. Problem ten sklasyfikowano w rejestrze ryzyka jako jedyne zagrożenie o najwyższym stopniu krytyczności (16 pkt).

Jest to sytuacja szczególnie trudna w obliczu implementacji unijnej dyrektywy **NIS2**. Nowelizacja ustawy o KSC skokowo zwiększy liczbę podmiotów kluczowych i ważnych, włączając do systemu tysiące nowych instytucji (np. w sektorze ochrony zdrowia czy samorządach) o często niskiej dojrzałości cyfrowej. Istnieje realne ryzyko przeciążenia organów nadzorczych oraz powstawania struktur czysto „fasadowych”, niezdolnych do realnej obrony.

Plan działań na rok 2026

Odpowiedzią na te wyzwania ma być dalsza centralizacja i automatyzacja procesów obronnych. Do kluczowych planów na rok 2026 należą:

- **Sformalizowanie PCOC** - Połączone Centrum Operacyjne Cyberbezpieczeństwa stanie się oficjalnym organem pomocniczym Pełnomocnika, pełniąc rolę „jednego okienka” dla całego ekosystemu KSC.
- **Rozwój CSIRT-ów sektorowych** -budowa nowych zespołów dla infrastruktury, cyfry i energii.
- **Modernizacja technologiczna** - rozbudowa systemu **S46** o moduł bezpiecznej samorejestracji podmiotów oraz rozwój portalu **cyber.gov.pl**.

- **Inwestycje w NASK - p**race nad fizycznym Centrum Cyberbezpieczeństwa NASK (CCN) o wartości 310 mln zł.

Rok 2025 udowodnił sprawność reagowania polskich służb na bieżące kryzysy. Jednak sprostanie wyzwaniom przyszłości będzie bezwzględnie wymagało zwiększenia finansowania etatów eksperckich oraz silnej automatyzacji analizy zagrożeń.

Pełne Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa jest możliwe do pobrania pod adresem: *https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025*

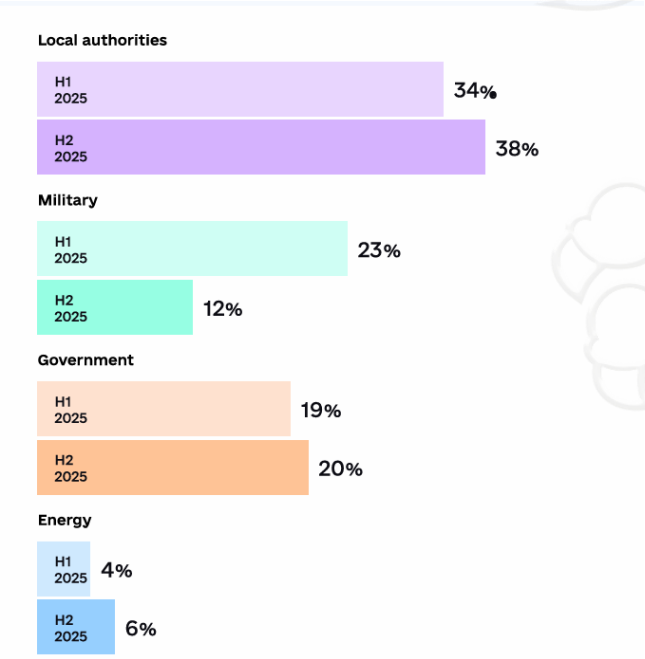
Rosyjskie cyberoperacje – analiza CERT-UA

CERT UA opublikował w kwietniu dwa raporty analityczne „*Cyber Threats: Ukraine. Analytics for the H2 2025" i „2025 Annual Report. Vulnerability Detection and Cyber Incident/Cyber Attack Response System*". Raporty te są kompleksowym podsumowaniem działań w ukraińskiej cyberprzestrzeni, stanowiącej dziś nieodłączny komponent współczesnych działań wojennych. Dokumenty rzucają dogłębne światło na nieustannie zmieniający się krajobraz zagrożeń, analizując ewoluujące podejście adwersarzy, pojawienie się nowych klastrów aktywności hakerskich oraz wdrażanie zmodernizowanych taktyk, technik i procedur.

Dane liczbowe:

W drugiej połowie 2025 r. odnotowano łącznie 2909 incydentów, co stanowi spadek o 4% w porównaniu do pierwszej połowy 2025 r (3018 incydentów). Nastąpił spadek incydentów o niskim, średnim i wysokim priorytecie. Głównymi celami cyberataków w H1 2025 były władze lokalne (38%, wzrost z 34%) oraz sektor wojskowy (12%, spadek z 23%).

Incidents by severity	H1 2025	H2 2025	Difference
Critical	1	0	-100%
High	6	5	-17%
Medium	2 944	2895	-2%
Low	67	9	-87%
Total	**3 018**	**2 909**	**-4%**



Raport CERT-UA Russian Cyber Operations. Analytics for H2 2025

Ważnym spostrzeżeniem z drugiej połowy 2025 roku jest gruntowna ewolucja taktyk adwersarzy, którzy nieustannie poszukują najefektywniejszych metod operacyjnych. W poprzednich okresach badacze obserwowali dominację strategii "Steal & Go", polegającej na wdrażaniu oprogramowania typu stealers w celu szybkiego przejęcia danych, przy jednoczesnym celowym skróceniu czasu przebywania w infrastrukturze ofiary, by uniknąć wykrycia. Obecnie punkt ciężkości uległ znacznej zmianie – nadrzędnym priorytetem hakerów stało

się zabezpieczanie trwałego i nieautoryzowanego dostępu do skompromitowanych systemów. Atakujący próbują zmaksymalizować długoterminową wartość ataku nadużywając legalnych narzędzi zdalnego dostępu, wykorzystując początkowe wejście jako przyczółek do głębszych operacji w sieci. Wiąże się z tym też groźne zjawisko określane jako "Comeback", polegające na wracaniu intruzów do skompromitowanych wcześniej systemów, aby sprawdzić, czy luki nadal nie zostały załatane lub czy wykradzione wcześniej poświadczenia wciąż są aktualne. Taka praktyka dobitnie ukazuje, jak istotne jest całościowe usuwanie pierwotnych przyczyn incydentów zamiast powierzchownego przywracania systemów do działania lub wybiórczego blokowania zaobserwowanej aktywności.

Działalność grup powiązanych z rosyjskimi służbami wywiadowczymi ewoluuje i staje się coraz groźniejsza. Znaczącej modyfikacji uległ główny wektor wejścia. Ponieważ klasyczny phishing z mailami i komunikatorami zaczyna tracić swoją skuteczność przez wyższą ostrożność użytkowników, przestępcy uciekają się do wysoce spersonalizowanej socjotechniki. Intruzi porozumiewają się płynnym językiem ukraińskim, wykonują połączenia wideo i audio przy użyciu lokalnych numerów operatorskich, a dzięki szczegółowej wiedzy o celu, skrupulatnie budują fałszywe zaufanie. Tego typu metody z powodzeniem stosowały takie grupy jak UAC-0001 (APT28) oraz UAC-0190 (Void Blizzard, Laundry Bear) w wymierzonych w Siły Obronne Ukrainy i przemysł zbrojeniowy atakach, w których wirus udający dokument Excel rozsyłany był na komunikatorze dopiero po odbyciu rozmowy telefonicznej.

Ciekawym przykładem była operacja grupy Sandworm wymierzona w infrastrukturę krytyczną. Po wykryciu incydentu w obiekcie i zresetowaniu haseł, analitycy zauważyli ponowne próby logowania z ukraińskich adresów IP. Śledztwo wykazało innowacyjne podejście napastników: hakerzy najpierw włamali się do niezabezpieczonych, publicznych urządzeń sieciowych (np. routerów) na terenie Ukrainy, a następnie aktywowali na nich funkcje tunelowania SOCKS oraz przekierowania SSH. Przejęte sprzęty posłużyły jako "węzły pośredniczące" (proxy). Ruch sieciowy z ataku na infrastrukturę krytyczną był przepuszczany przez całe łańcuchy tych ukraińskich urządzeń, co miało na celu całkowite zatarcie śladów i ukrycie faktu, że atak faktycznie pochodzi ze wschodu. Równolegle do wyrafinowanej socjotechniki, hakerzy nasilili wykorzystanie mechanizmów maskujących, by zapewnić sobie trwały dostęp do systemów. W drugiej połowie 2025 roku masowo wykorzystywano lukę w programie WinRAR (CVE-2025-8088), która podczas rozpakowywania archiwum potajemnie umieszczała wirusa bezpośrednio w folderze "Autostart". Aby całkowicie ukryć swoją obecność przed detekcją, grupy hakerskie powszechnie stosowały też Alternatywne Strumienie Danych (ADS) w systemach NTFS i wirtualnych dyskach VHD. Złośliwy kod pozostawał dzięki temu niewidoczny, ukryty w z pozoru pustych plikach (o rozmiarze 0 bajtów), czekając na aktywację przez skrypt.

Druga połowa 2025 r. przyniosła spadek liczby incydentów w porównaniu z pierwszym półroczem Oznacza to skuteczność wdrażanych systemów obronnych. Jednak w czasie cyberwojny nie można tracić czujności, ponieważ ogólna intensywność cyberataków utrzymuję się na stałym poziomie, a adwersarze stale modyfikują swoje działania. Wymusza to stosowanie kompleksowej strategii bezpieczeństwa, całościowym usuwaniu pierwotnych przyczyn włamań by skutecznie zablokować intruzom powrót do sieci.

Źródło CERT UA

Cyberbezpieczeństwo filarem rozwoju cyfrowego państwa – unijne fundusze na odporność infrastruktury i ochronę danych.

Cyberbezpieczeństwo staje się jednym z kluczowych elementów bezpieczeństwa państwa i stabilności administracji publicznej. 4 marca 2026 r. Komisja Europejska zatwierdziła zmiany w programie Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), wprowadzając nowy, strategiczny priorytet: FERC.04 „Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych". To odpowiedź na gwałtownie rosnącą liczbę cyberataków, a także na coraz bardziej wymagające i niestabilne otoczenie geopolityczne.

Na realizację nowego priorytetu przesunięto 28 proc. całego budżetu FERC, czyli ponad 550 mln euro (około 2,3 mld zł). Środki te zostaną przeznaczone na wzmocnienie ochrony danych oraz wzmocnienie infrastruktury teleinformatycznej państwa. Szczególny nacisk położony będzie na zapewnienie ciągłości działania kluczowych systemów cyfrowych. Chodzi nie tylko o odporność na ataki hakerskie, czy operacje typu DDoS, ale także o przygotowanie na awarie energetyczne, przerwy w łańcuchach dostaw czy ekstremalne zjawiska pogodowe, które mogą zakłócać funkcjonowanie systemów informatycznych.

Fundusze z nowego priorytetu wykorzystane będą na wsparcie projektów wzmacniających cyberbezpieczeństwo państwa. Projekty obejmą m.in. ochronę infrastruktury krytycznej, kluczowych systemów administracji publicznej oraz podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Istotnym elementem będzie również dostosowanie krajowych rozwiązań do wymogów Dyrektywy NIS 2 (UE 2022/2555), wzmacniającej wspólny poziom cyberbezpieczeństwa w Unii Europejskiej.

Program FERC przewiduje także wsparcie dla samorządów, w tym rozwój kompetencji w zakresie monitorowania zagrożeń oraz reagowania na incydenty cyberbezpieczeństwa. Ważnym obszarem inwestycji to budowa i modernizacja centrów przetwarzania danych, które zapewnią ciągłość działania systemów o krytycznym znaczeniu – takich jak rejestry państwowe czy chmura rządowa, stanowiące podstawę funkcjonowania e-usług dla obywateli. W projektach tych zastosowane zostaną również unijne i krajowe regulacje dotyczące ekoprojektowania, co ma ograniczyć energochłonność i wpływ infrastruktury cyfrowej na środowisko.

Nowy priorytet jasno pokazuje, że transformacja cyfrowa nie może postępować bez równoległego wzmacniania bezpieczeństwa. Stabilne i odporne systemy informatyczne są dziś fundamentem sprawnego państwa – od obsługi obywateli, przez zarządzanie danymi publicznymi, po reagowanie w sytuacjach kryzysowych. Cyberbezpieczeństwo przestaje być wąskim zagadnieniem technicznym. Staje się sprawą publiczną, od której zależy zaufanie obywateli i odporność państwa w czasach próby.

Operacja Hellfire – uderzenie w przestępczość pedofilską. 123 zatrzymania i przejęte ponad 330 tys. plików z zabronionymi treściami.

Niemal pół tysiąca funkcjonariuszy uderzyło w przestępczość o charakterze pedofilskim, przeprowadzając działania „Hellfire". Przez dwa tygodnie trwania operacji, policjanci zatrzymali 123 osoby i przeprowadzili 175 przeszukań, w których efekcie znaleźli ponad 1500 nośników cyfrowych, na których znajdowało się ponad 330 tys. plików przedstawiających seksualne wykorzystanie osób małoletnich. 95 osób usłyszało zarzuty karne, a wobec 47 osób zastosowano środki zapobiegawcze w postaci tymczasowego aresztowania. To kolejna – już ósma operacja, przeprowadzona przez CBZC i ukierunkowana na zwalczanie przestępczości o charakterze pedofilskim.

„Hellfire", to kryptonim kolejnej operacji prowadzonej na terenie całego kraju przez Centralne Biuro Zwalczania Cyberprzestępczości. Do przeprowadzenia operacji dołączyli policjanci z komend wojewódzkich i powiatowych pod koordynacją funkcjonariuszy z Wydziału do walki z Handlem Ludźmi Komendy Głównej Policji. W sumie to niemal pół tysiąca policjantów, którzy już po raz ósmy uderzyli w przestępczość o charakterze pedofilskim, przeprowadzając na terenie całego kraju operację „Hellfire". Działania prowadzono także przy współpracy z Żandarmerią Wojskową.

W trakcie trwających działań funkcjonariusze zatrzymali 123 osoby w wieku od 19 do 94 lat. Przeprowadzili 175 przeszukań, w których efekcie zabezpieczyli ponad 1500 różnego rodzaju nośników cyfrowych, dysków, pendrive-ów telefonów, komputerów. Na zabezpieczonym sprzęcie funkcjonariusze ujawnili ponad 330 tys. plików przedstawiających seksualne wykorzystanie osób małoletnich. Wśród zabezpieczonych materiałów znajdują się również i te wytworzone przez AI.

Operacja była ściśle koordynowana z Departamentem ds. Cyberprzestępczości i Informatyzacji Prokuratury Krajowej oraz prokuraturami z terenu całego kraju. W świetle zgromadzonego materiału dowodowego 95 osób usłyszało zarzuty karne posiadania, udostępniania, ale także produkowania zabronionych treści. Decyzją sądów 47 podejrzanych zostało tymczasowo aresztowanych na okres 3 miesięcy. Funkcjonariusze zabezpieczyli mienie podejrzanych na kwotę ponad 210 tys. zł.

Wśród zatrzymanych osób znajduje się m.in. pedagog który nagrywał oraz fotografował dzieci i trafił do aresztu na 3 miesiące. Podejrzanym jest także mężczyzna, który wykorzystując mechanizm child groomingu nakłaniał osoby małoletnie do wykonywania innych czynności seksualnych, wykorzystując m.in. popularny komunikator. Względem mężczyzny zastosowano środek zapobiegawczy w postaci tymczasowego aresztowania.

W wyniku informacji otrzymanych w ramach współpracy międzynarodowej, policjanci CBZC zatrzymali też 19 latka, który – jak wynika ze wstępnych ustaleń, utrwalał treści pornograficzne z udziałem swojej małoletniej siostry przyrodniej. Sąd zastosował wobec niego areszt tymczasowy.

Kolejnych dwóch zatrzymanych mężczyzn miało zamontowane w swoich domach urządzenia monitorujące i kamerki, przy pomocy których nagrywali bliskich, członków swoich rodzin i inne osoby w trakcie czynności intymnych. Oni także trafili do aresztu.

Walka z rozpowszechnianiem w Internecie treści przedstawiających seksualne wykorzystanie osób małoletnich stanowi jedno z priorytetowych zadań policjantów Centralnego Biura Zwalczania Cyberprzestępczości. Działania Hellfire zostały przeprowadzone przez CBZC już po raz 8 i będą kontynuowane.

Pełny tekst artykułu dostępny pod tym linkiem.

Źródło: cbzc.policja.gov.pl

Międzynarodowa akcja przeciwko sprzedaży fałszywych leków i suplementów. CBZC i KAS zatrzymały 3 osoby i przeszukały ponad 70 lokalizacji.

W wyniku międzynarodowych, skoordynowanych działań Eurojustu i Europolu funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości oraz funkcjonariusze Wielkopolskiego Urzędu Celno-Skarbowego w Poznaniu uczestniczyli w rozbiciu grupy przestępczej, która zajmowała się wprowadzaniem do obrotu fałszywych suplementów i leków. Grupa działała na terenie całej Unii Europejskiej (UE) i poza nią. Funkcjonariusze zatrzymali 15 osób, z czego 3 na terenie Polski.

Działalność grupy przestępczej polegała na sprzedaży rzekomo legalnych leków leczących poważne choroby. Jej działalność wygenerowała straty w wysokości 240 milionów euro. Skoordynowana akcja doprowadziła do zebrania wielu dowodów, zatrzymania niektórych głównych członków grupy i przejęcia dużych zapasów suplementów. Eurojust i Europol wspierały śledztwa od samego początku, zapewniając sprawną i skuteczną współpracę między 15 krajami. 12 maja br., w wyniku śledztwa nadzorowanego przez Prokuraturę Okręgową w Warszawie, funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości, wspólnie z funkcjonariuszami KAS, przeszukali 73 miejsca na terenie Polski, m.in. w Warszawie i Krakowie. W ramach realizacji przeszukano także blisko 80 miejsc na terenie Europy, w których efekcie zlikwidowano nielegalne miejsca produkcji fałszywych produktów leczniczych wraz z linią produkcyjną służącą do ich wytwarzania. Funkcjonariusze zatrzymali 15 osób, z czego 3 na terenie Polski.

Polscy funkcjonariusze zabezpieczyli również znaczne ilości dokumentacji rachunkowej związanej z legalizacją produktów leczniczych na terenie kilkunastu państw i dokumentację związaną z legalizacją środków finansowych pochodzących z przestępstwa. Prokuratura wystąpiła o areszt wobec dwóch zatrzymanych na terenie Polski, a także o zabezpieczenie mienia w postaci hipoteki przymusowej na kwotę 8 mln zł. Dotychczas zabezpieczono mienie o wartości 3,5 mln zł.

Jak ustalono w toku prowadzonego śledztwa, grupa od 2019 r. współpracowała w profesjonalny i hierarchiczny sposób. Zakładano firmy, przez które sprzedawano suplementy i leki niedozwolone do sprzedaży. Sieć wirtualnych sprzedawców stworzyła setki stron internetowych i kont w mediach społecznościowych. Przestępcy często używali nazwisk i wizerunków znanych osób oraz fałszywych lekarzy, by wprowadzać ofiary w błąd. Grupa przestępcza szkoliła swoich partnerów w tworzeniu fałszywych kont w mediach społecznościowych oraz w sposobach sprawiania, by konta wyglądały na wiarygodne i pozostawały niezauważone przez platformy społecznościowe.

Suplementy rozpowszechniane przez grupę zawierały placebo, a nieuczciwi sprzedawcy twierdzili, że leczą różne choroby, w ten sposób wprowadzając ofiary w błąd. Bułgarska policja wykryła zakład produkcyjny nielegalnych suplementów diety oraz magazyny służące do ich przechowywania, zajmujące powierzchnię prawie 2000 m^2. Skonfiskowano dziesiątki tysięcy opakowań ponad 300 rodzajów nielegalnie produkowanych suplementów diety, które znaleziono w magazynach, a także urządzenia elektroniczne, sprzęt komputerowy i dane, znaczną ilość dokumentów księgowych, transportowych i płatniczych itp. Znaleziono maszyny

i zaawansowany technologicznie sprzęt produkcyjny, a także różne substancje i materiały różnego pochodzenia, gotowe produkty oraz przesyłki przygotowane do wysyłki do klientów.

Aby zlikwidować nielegalny proceder, niezbędna była współpraca międzynarodowa. Powstał wspólny zespół śledczy utworzony w Eurojust. Poprzez spotkania koordynacyjne w siedzibie agencji w Hadze władze 15 krajów (Rumunia, Bułgaria, Cypr, Grecja, Węgry, Włochy, Łotwa, Litwa, Polska, Słowacja, Słowenia, Hiszpania, Mołdawia i Ukraina) współpracowały, aby zaplanować i skoordynować działania.Sprawa ma charakter rozwojowy.

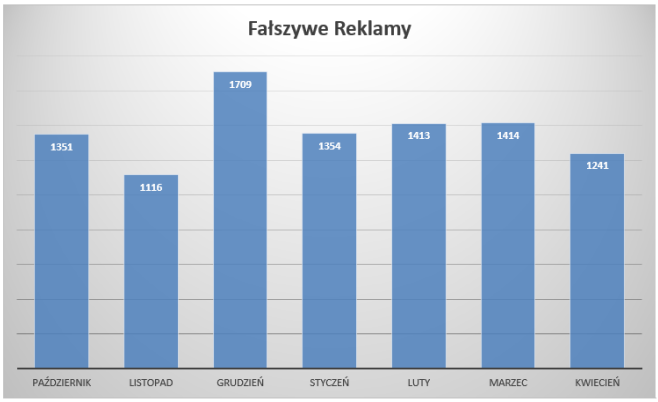
Pełny tekst artykułu dostępny pod tym linkiem.

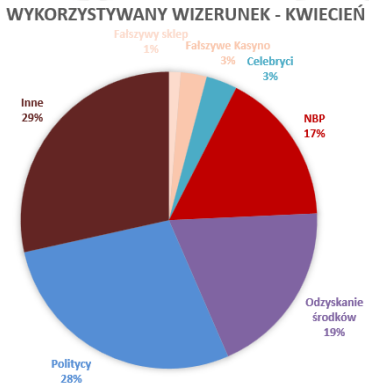
Więcej o działalności CBZC na poniższych stronach internetowych:

Podsumowanie miesiąca przez CSIRT KNF - Krajobraz zagrożeń skierowanych na klientów rynku finansowego - kwiecień 2026

W kwietniu 2026 roku CSIRT KNF wykrył i zgłosił do zablokowania 891 domen, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania CERT Polska dodał na listę ostrzeżeń 22 343 domeny. A na koniec omawianego miesiąca, na liście hole znajdowało się 131 351 domen.

Zdecydowana większość zgłoszonych domen phishingowych wykorzystywana była w scenariuszu znanym pod nazwą „fraud inwestycyjny". Schemat działania przestępców, w którym zachęcają do rzekomego inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków. Najczęstszym sposobem dystrybucji tego typu treści są reklamy w mediach społecznościowych. Poniższe wykresy przedstawiają wykryte i zgłoszone do blokady reklamy na portalu społecznościowym Facebook, w podziale na kategorie wykorzystywanego wizerunku.

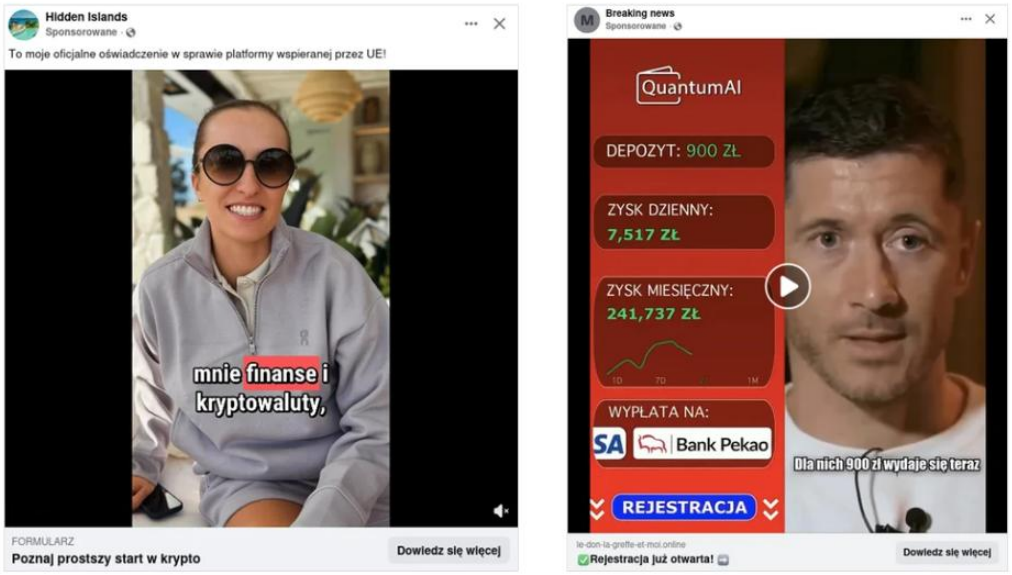




W minionym miesiącu cyberprzestępcy zamieszczali reklamy dotyczące rzekomej możliwości „odzyskania środków". To drugi etap omawianego schematu działania przestępców, w którym przestępcy publikują informację o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości, jest to ponowna próba oszukania osób, które już wcześniej dały się nabrać na ten scenariusz.

Rysunek 1 Fałszywe reklamy inwestycyjne – motywu odzyskania straconych środków

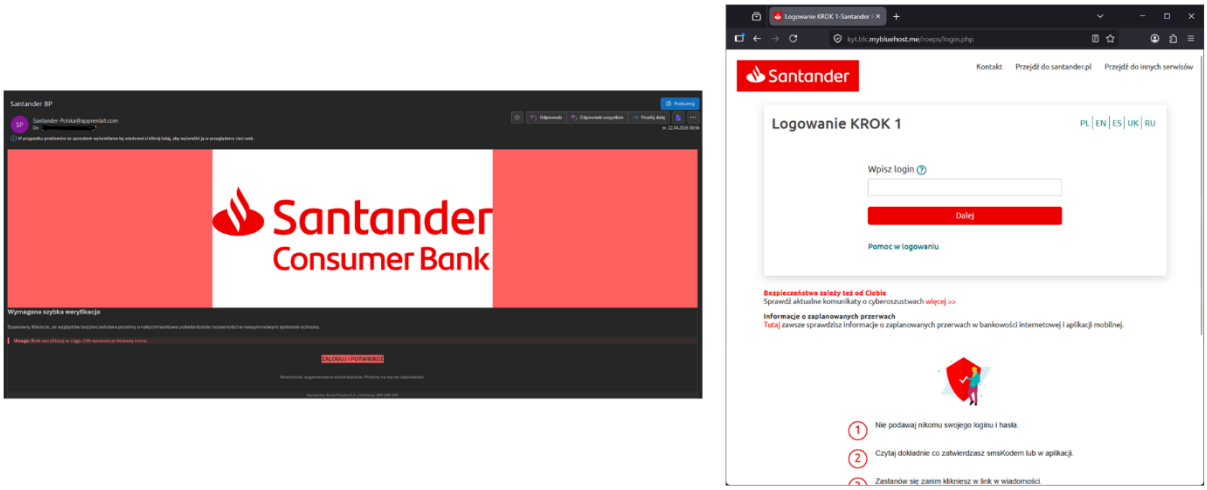
Przestępcy reklamując rzekome inwestycje wykorzystują często wizerunki znanych osób, wizerunki rozpoznawalnych firm oraz motywy rządowe. Nadal chętnie wykorzystują również technologię deepfake do tworzenia materiałów oszukańczych. Przedstawiona treść zachęca do rzekomych inwestycji.



Rysunek 2 Fałszywe inwestycje – wykorzystanie technologii deepfake

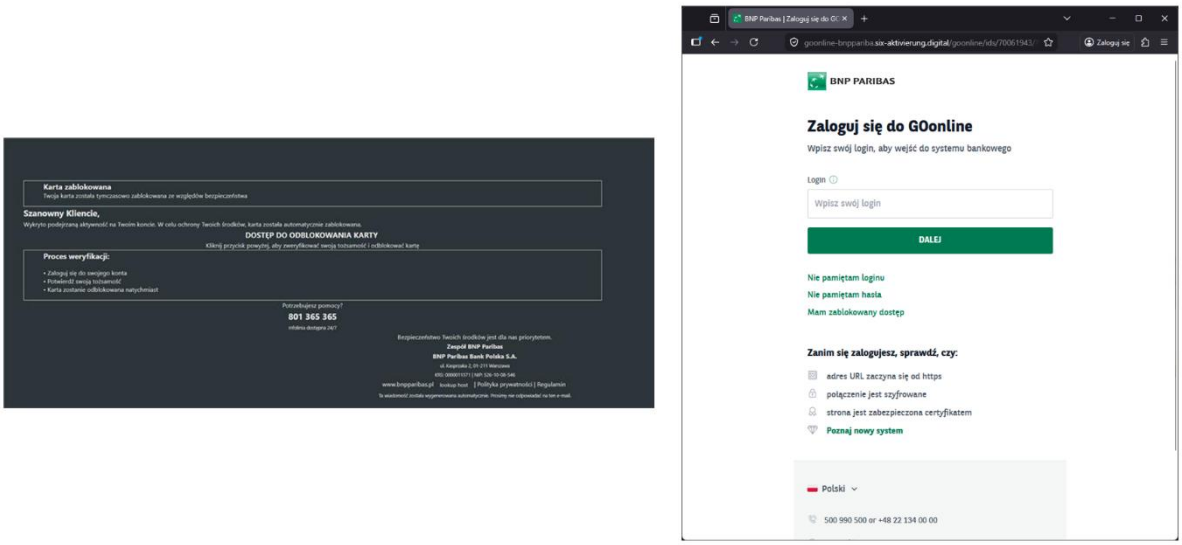
Przestępcy wykorzystują również wizerunek znanych instytucji, aby zwiększać wiarygodność kampanii phishingowych, dlatego też regularnie podszywają się pod polskie Banki. Wyłudzają w ten sposób m.in. dane osobowe, informacje o kartach płatniczych, dane uwierzytelniające do bankowości elektronicznej, czy kody BLIK. W kwietniu 2026 roku nadal wykorzystywali ten sposób. Zidentyfikowane kampanie phishingowe wykorzystywały wizerunki m.in:

- Santander Bank Polska,



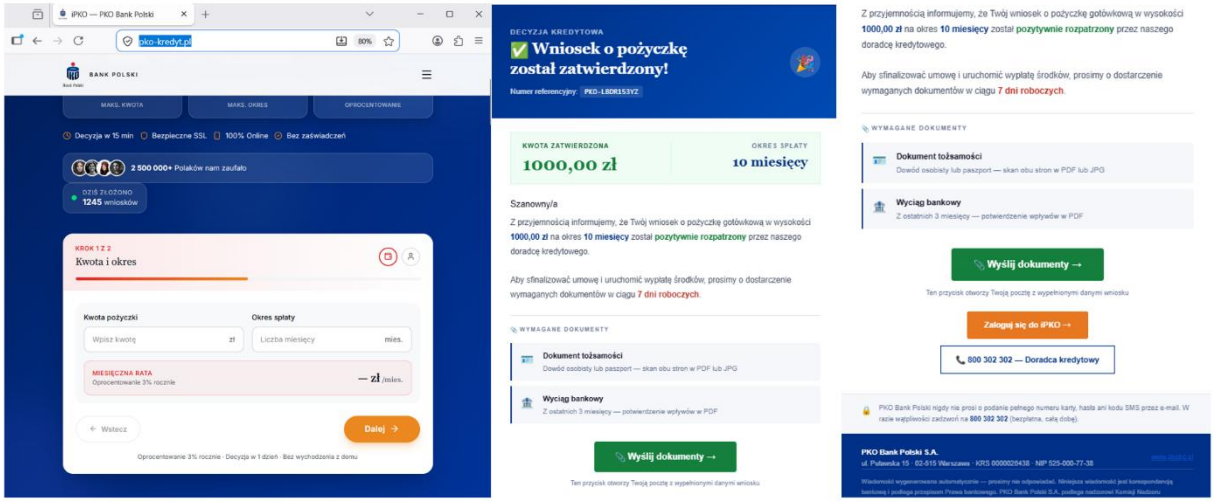
Rysunek 3 Kampania phishingowa – podszycie pod Santander Bank Polska

- BNP Paribas,



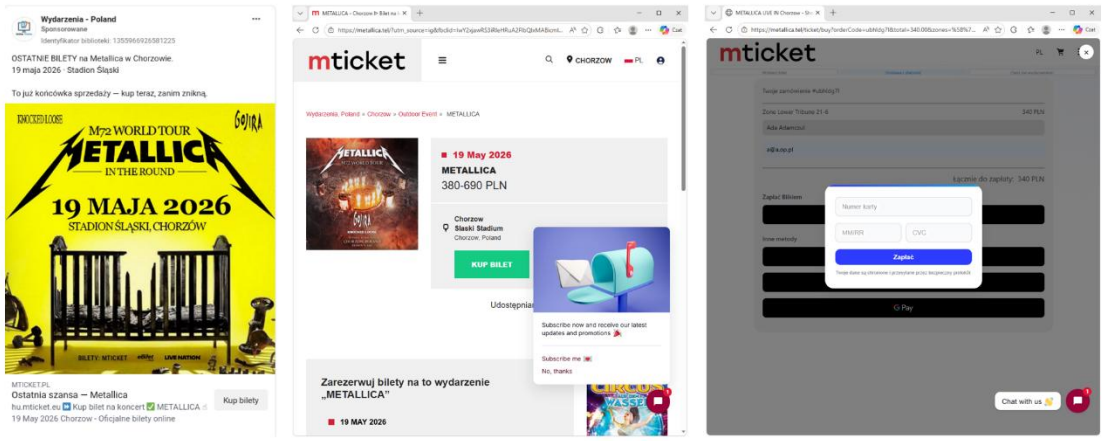
Rysunek 4 Kampania phishingowa – podszycie pod BNP Paribas

- PKO BP



Rysunek 5 Kampania phishingowa – podszycie pod PKO BP

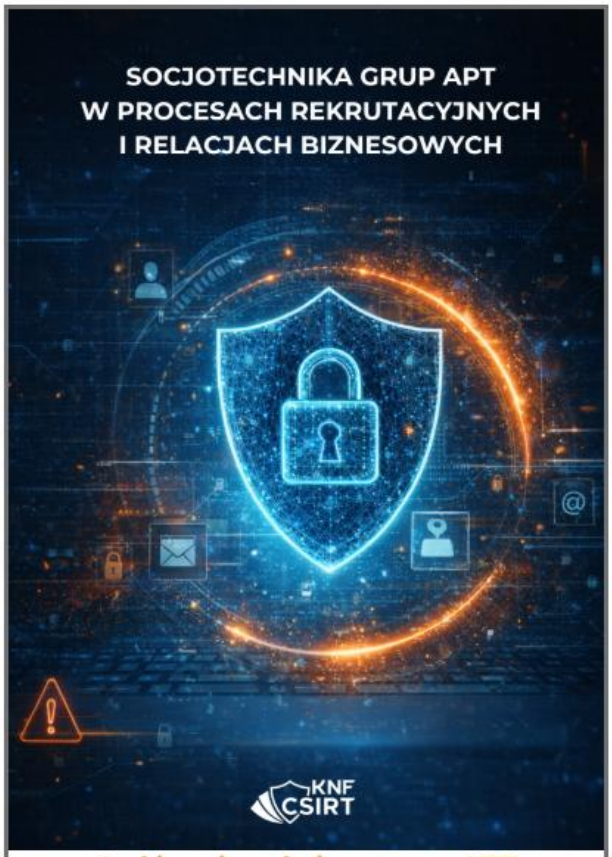
Podobnie jak w marcu 2026 roku, również w kwietniu cyberprzestępcy przygotowali kampanie phishingowe wyłudzające dane kart płatniczych. Tym razem w publikowanych przez nich reklamach na platformie Facebook zachęcali do zakupienia rzekomo ostatnich biletów na koncert zespołu Metallica i wykorzystywali wizerunek mTicket (rys. 6). Przykładem kolejnej kampanii, z jaką mieliśmy do czynienia w ostatnich tygodniach było podszycie pod PayU. Cyberprzestępcy przygotowali stronę, za pośrednictwem której można było rzekomo doładować telefon na kartę. W rzeczywistości była to strona phishingowa wyłudzająca dane kart płatniczych. Cyberprzestępcy podszywając się pod ZUS, przesyłali także fałszywe wiadomości SMS, w których informowali o rzekomym błędzie w stanie rozliczeń ubezpieczenia zdrowotnego. Oszuści zachęcali do kliknięcia w znajdujący się w wiadomości link, a w kolejnym kroku wymagali podania swojego numeru PESEL oraz informacji o karcie płatniczej.



Rysunek 6 Fałszywe reklamy na platformie Facebook, w których oszuści zachęcali do zakupienia biletów na koncert zespołu Metallica

Tak jak zaznaczamy co miesiąc, jedną z metod ochrony przed wymienionymi wyżej i innymi działaniami cyberprzestępców jest wiedza. Dlatego zachęcamy do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook.

Natomiast ze szczegółami kampanii przestępczych obserwowanych zarówno w kwietniu 2026 roku, jak i w poprzednich miesiącach zapoznać się można na naszej stronie: https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf.



Zachęcamy także do zapoznania się z materiałem dotyczącym socjotechniki grup APT w procesach rekrutacyjnych i relacjach biznesowych. Przybliżamy w nim jak współczesne kampanie zagrożeń wykraczają poza klasyczny phishing i wykorzystują m.in. fałszywe rekrutacje, podszywanie się pod kandydatów IT, spreparowane spotkania Zoom, Teams, a także długoterminowe budowanie wiarygodności w kontaktach biznesowych.

W publikacji zaprezentowane zostały:

- najczęstsze schematy działania.

- sygnały ostrzegawcze,

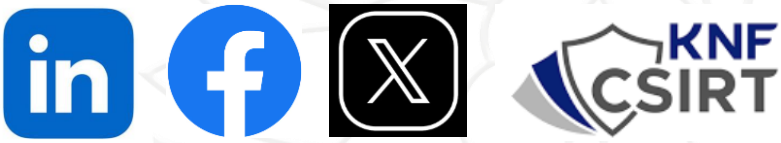
- rekomendacje dla organizacji, zespołów bezpieczeństwa oraz osób zaangażowanych w rekrutację i onboarding.

Zachęcamy do lektury i przeglądu wewnętrznych procedur bezpieczeństwa w obszarach HR, współpracy z kontrahentami i ochrony pracowników technicznych.

Z materiałem można zapoznać się pod tym adresem:

https://cebrf.knf.gov.pl/images/Raporty/Ataki_socjotechniczne_grup_APT.pdf

Więcej o działalności CSIRT KNF na poniższych stronach internetowych:



BIULETYN INFORMACYJNY MC – ZAGROŻENIA W CYBERPRZESTZRENI

„Biuletyn Informacyjny. Zagrożenia w cyberprzestrzeni" - opracowywany jest przez zespół Departamentu Cyberbezpieczeństwa MC we współpracy z CBZC i CSIRT KNF.

Ideą Biuletynu jest zwiększanie świadomości i wiedzy na szerokorozumiane tematy związane z cyberbezpieczeństwem wśród pracowników administracji publicznej, zarówno na poziomie centralnym jak i na szczeblu samorządowym.

Możliwość dołączenia do subskrypcji Biuletynu pod linkiem:

– https://www.gov.pl/web/baza-wiedzy/subskrypcja

INFORMACJA O SZKOLENIACH

Zachęcamy również do udziału w bezpłatnych szkoleniach online dla podmiotów krajowego systemu cyberbezpieczeństwa, które organizuje Departament Cyberbezpieczeństwa MC.

Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej Bazy Wiedzy cyberbezpieczeństwa na portalu *gov.pl* – pod linkiem:

– https://www.gov.pl/web/baza-wiedzy/szkolenia

BIULETYN NASK

Zachęcamy również do zasubskrybowania biuletynu NASK – jest to przegląd najważniejszych informacji nt. cyberbezpieczeństwa, edukacji cyfrowej i nowych technologii. Link do zapisów:

– https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html

Oznaczenia TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.**	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: *cert.pl*

Biuletyn został opracowany przez Wydział Analiz Cyberbezpieczeństwa Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji we współpracy z zespołami CSIRT KNF i CBZC.

Więcej o działalności MC na poniższych stronach: