Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

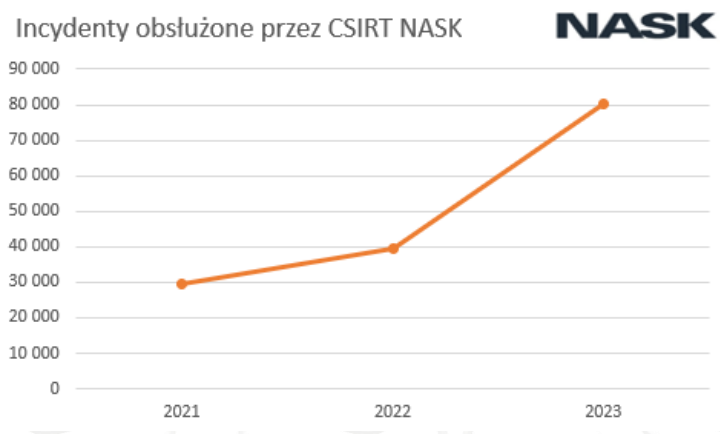
03/2024

SPIS TREŚCI

Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023 - podsumowanie

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na Pełnomocnika Rządu ds. Cyberbezpieczeństwa obowiązek przedkładania Radzie Ministrów corocznych sprawozdań. W tym roku po raz pierwszy udostępniliśmy ten dokument szerszej publiczności na stronie Ministerstwa Cyfryzacji. Sprawozdanie zostało opracowane przez Ministerstwo Cyfryzacji, pełniące centralną rolę w Krajowym Systemu Cyberbezpieczeństwa (KSC) oraz obsługujące Pełnomocnika. Dokument przedstawia aktualny krajobraz bezpieczeństwa polskiej cyberprzestrzeni, dane statystyczne oraz opis realizowanych przedsięwzięć podnoszących poziom cyberbezpieczeństwa w Polsce. Jednocześnie z uwagi na charakter niektórych informacji mających szczególne znaczenie dla bezpieczeństwa państwa, opracowano także niejawny załącznik (w myśl ustawy o ochronie informacji niejawnych), który nie podlega upublicznieniu.

Dane z ub.r. pokazują utrzymujący się wysoki poziom zagrożenia w cyberprzestrzeni oraz wzrastającą skalę cyberataków, tak w wymiarze ilościowym, jak i jakościowym. Obserwowana była wysoka aktywność grup APT, grup haktywistycznych oraz cyberprzestępczych powiązanych z państwami-adwersarzami. Na cyberbezpieczeństwo coraz większy wpływ mają nowe technologie (np. sztuczna inteligencja, rozwiązania chmurowe) i związane z nimi nowe zagrożenia, choć technologie te dają też nowe możliwości zwiększania odporności. Na nasze bezpieczeństwo wpływ ma także postępująca cyfryzacja życia oraz zmiana środowiska bezpieczeństwa międzynarodowego. Szczególne znaczenie ma wojna Rosji z Ukrainą oraz wsparcie Polski dla Ukrainy, nie tylko jako donator sprzętu wojskowego, ale też państwo istotnie wspierające ukraińską cyberobronę. Ponadto, z uwagi rolę Polski jako hubu wsparcia Zachodu dla Ukrainy, celem rosyjskich cyberataków stała się polska infrastruktura transportowa, choć działania te nie zakłóciły w istotnym stopniu systemu transportowego kraju. Wpisuje się to w rosyjskie, ale też białoruskie i ze strony innych państw działania hybrydowe, których znaczna część ma miejsce w cyberprzestrzeni. Między innymi wzmożona aktywność wrogich aktorów obserwowana była w związku z październikami wyborami parlamentarnymi, jednak nie udało im się zakłócić procesów wyborczych.



Źródło: Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok.

Zachęcamy do zapoznania się z całością dokumentu. Przedstawia on nie tylko działania realizowane przez Pełnomocnika i Ministerstwo Cyfryzacji będące środkiem ciężkości krajowego systemy cyberbezpieczeństwa, ale także działania Zespołów CSIRT poziomu krajowego (NASK, GOV, MON), organów właściwych ds. cyberbezpieczeństwa (Ministerstwo Cyfryzacji, Ministerstwo Klimatu i Środowiska, Ministerstwo Infrastruktury, Komisji Nadzoru Finansowego, Ministerstwa Obrony Narodowej) i dwóch sektorowych zespołów cyberbezpieczeństwa (CSIRT KNF i CSIRT CeZ), służb specjalnych (Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego), organów ścigania i wymiaru sprawiedliwości odpowiedzialnych za zwalczanie cyberprzestępczości (Centralne Biuro Zwalczania Cyberprzestępczości Policji, Ministerstwo Sprawiedliwości, Centralne Biuro Antykorupcyjne), jak również szereg innych przedsięwzięć wzmacniających krajowego cyberbezpieczeństwa (rozdział 2.)

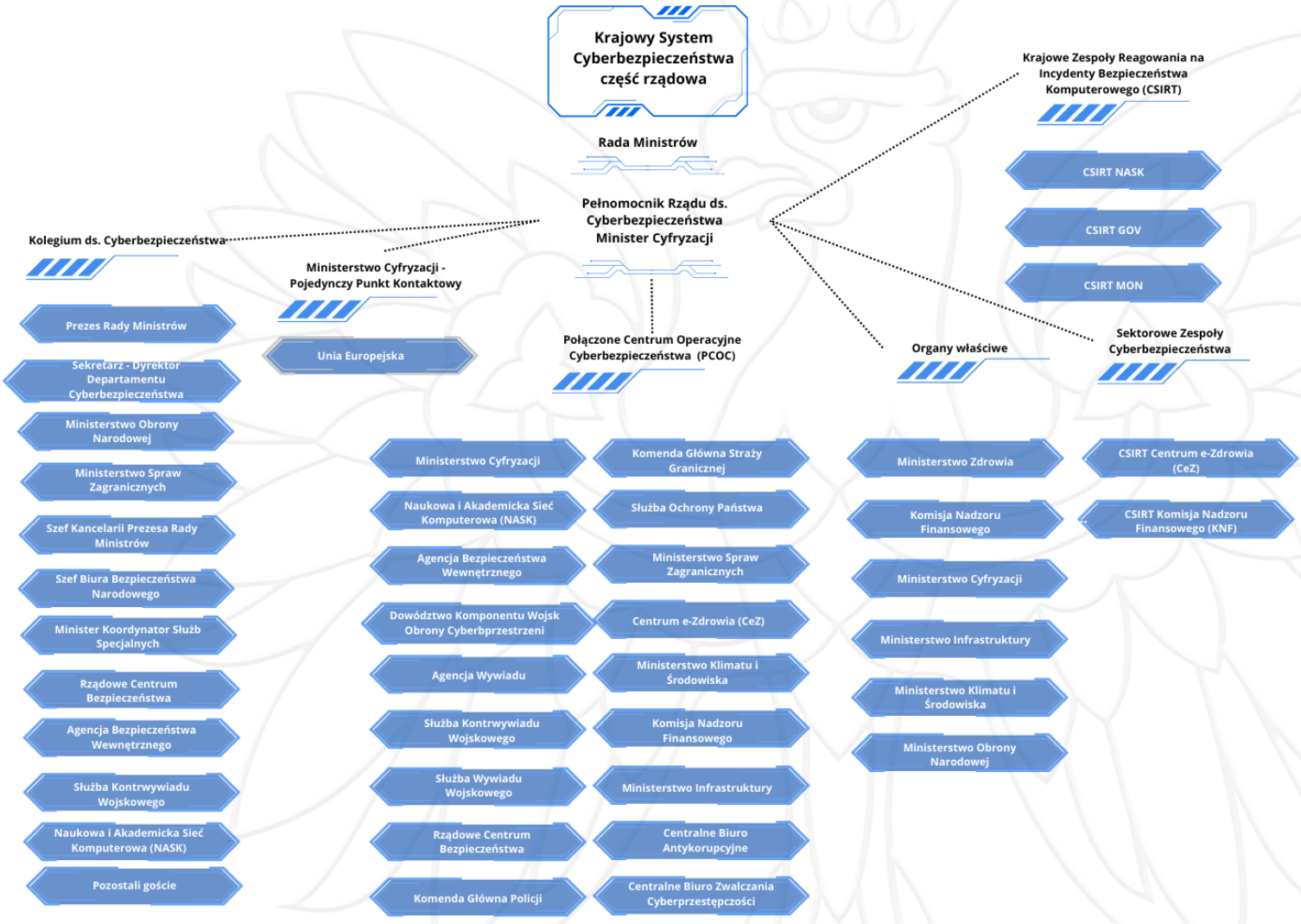
W rozdziale 2. możemy przeczytać o licznych inicjatywach, w większości realizowanych przez Ministerstwo Cyfryzacji, które wpisują się w poszczególne cele Strategii Cyberbezpieczeństwa RP na lata 2019-2024, taki jak np.:

- Nowa ustawa o krajowym systemie cyberbezpieczeństwa / wdrożenie dyrektywy NIS 2,
- Nowa Strategia Cyberbezpieczeństwa RP,
- Centrum Cyberbezpieczeństwa NASK,
- System zarządzania cyberbezpieczeństwem S46,
- Stopień alarmowy CHARLIE-CRP,
- Cyberbezpieczeństwo wyborów,
- System łączności niejawnej SKR-Z,
- Bezpieczny komunikator rządowy,
- System AntyDDoS dla administracji rządowej, służb specjalnych i Sił Zbrojnych RP zapewniany przez MC i NASK,
- Platforma CTI dla instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym,
- Portal BezpieczeneDane.gov.pl,
- Programu Współpracy w Cyberbezpieczeństwie (PWCyber),
- Projekt Cyberbezpieczny Samorząd,
- Fundusz Cyberbezpieczeństwa,
- Projekt SecureV,
- Liczne szkolenia z cyberbezpieczeństwa i higieny cyfrowej,
- Numer 8080,
- Współpraca w ramach UE, NATO,
- Współpraca międzynarodowa dwustronna,
- Wsparcie dla Ukrainy.

Działania te w istotny sposób przyczyniają się podnoszenia poziomu cyberbezpieczeństwa w kraju. Przykładowo, dzięki projektowi AntyDDoS, który Ministerstwo Cyfryzacji zleciło NASK-PIB, osłonę przed tego typu atakami zapewniamy centralnie dla 67 instytucji, w tym dla Sił Zbrojnych RP, służb specjalnych oraz urzędów centralnych. Z kolei dzięki projektom Ministerstwa Cyfryzacji takim jak SKR-Z i Komunikator stworzono narzędzia bezpiecznej łączności dla administracji rządowej i instytucji cyberbezpieczeństwa, także niejawnej. Ogromną rolę odgrywał też Fundusz Cyberbezpieczeństwa, który pozwalał zapewnić konkurencyjne zarobki specjalistom ds. cyberbezpieczeństwa w sektorze publicznym. A to tylko niewielki wycinek realizowanych w ub.r. przedsięwzięć.

Na koniec polecamy uwadze rekomendacje, jak np. ta dotycząca zidentyfikowanej potrzeby powołania centrum koordynacyjnego krajowego systemu cyberbezpieczeństwa, dysponującego odpowiednią pozycją ustrojową, kompetencjami, zasobami osobowymi, budżetem i infrastrukturą, co pozwoli na zwiększenie efektywności systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni.

Źródła: Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok.



Schemat organizacyjny Krajowego Systemu Cyberbezpieczeństwa, Źródło: Opracowanie własne, Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok

Działania ofensywne w cyberprzestrzeni – problem uprawnień

W artykule powyżej omówiliśmy Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2023 r. Jedną z kwestii, która w nim wybrzmiała, był problem posiadania uprawnień do prowadzenia ofensywnych działań w cyberprzestrzeni przez wojsko.

W ramach wkładu do Sprowadzania Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) zgłosiło rekomendację, aby *dokonać stosownych zmian legislacyjnych i nadanie Dowódcy KWOC uprawnień do samodzielnego podejmowania decyzji w zakresie neutralizacji zagrożeń w cyberprzestrzeni dla resortu obrony narodowej*, co przełożyło się na zgłoszone planowane działanie DKWOC, aby *wprowadzić uregulowanie prawne niezbędne z punktu widzenia uprawnień WOC do działań aktywnych w cyberprzestrzeni*.

Odmienne stanowisko przedstawił Pełnomocnik Rządu ds. Cyberbezpieczeństwa w rozdziale z rekomendacjami (pkt 3 na str. 93). Wicepremier i Minister Cyfryzacji argumentuje, że z uwagi na obecne zrównanie wojskowych działań w domenie cyber z kinetycznymi działaniami militarnymi (w tym co do skutków prawnych), prowadzenie ofensywnych cyberoperacji przez siły zbrojne ma zbyt daleko idące skutki, aby decyzje w tej sprawie mógł podejmować dowódca jednego z komponentów Sił Zbrojnych RP, analogicznie jak dowódcy innych rodzajów sił zbrojnych i komponentów nie mogą samodzielnie decydować o zaatakowaniu innego państwa, w tym przeprowadzaniu uderzeń odwetowych. Ponieważ cyberatak przeprowadzony przez wojsko może zostać uznany za *casus belli*, decyzja w tej sprawie powinna być podejmowana na najwyższym szczeblu politycznym.

Należy zauważyć, że w polskim systemie prawnym uprawnienie do podejmowania działań ofensywnych w cyberprzestrzeni posiadają służby specjalne, co jest zgodne z przyjętą na świecie praktyką i regulacjami prawnymi. Ponadto, zgodnie z art. 34 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa CSIRT-y poziomu krajowego (czyli m.in. CSIRT MON znajdujący się w strukturze DKWOC) zobowiązane są współpracować ze służbami specjalnymi przy realizacji ich ustawowych zadań. Co więcej, to właśnie służby specjalne posiadają odpowiednie umiejętności zachowania bezpieczeństwa prowadzonych operacji (OPSEC), aby zadbać o uniemożliwienie lub utrudnienie atrybucji prowadzonych działań. Skrupulatny OPSEC jest wpisany w DNA służb specjalnych, a niekoniecznie wojska.

Loga wywiadowczych i kontrwywiadowczych służb specjalnych (ABW, AW, SKW, SWW) oraz logo DKWOC.

Reasumując, Pełnomocnik zwraca uwagę, że istnieje potrzeba uregulowania kwestii działań ofensywnych w cyberprzestrzeni, aktywnej obrony oraz rozwoju zdolności do tego rodzaju działań, w tym uszczegółowienie zadań służb specjalnych. W opinii Pełnomocnika działania jednostek Sił Zbrojnych RP wykonywane w czasie pokoju w cyberprzestrzeni powinny być

skoncentrowane na działaniach defensywnych. Natomiast kompetencje aktywne, z pogranicza działalności specjalnej, należy pozostawić instytucjom do tego powołanym (SKW, SWW, ABW, AW oraz organy ścigania), a działania podmiotów zależnych od Sił Zbrojnych RP jako wsparcie ww. instytucji. Należy także rozważyć doprecyzowanie przepisów dotyczących realizacji czynności operacyjno-rozpoznawczych uprawnionych służb celem rozszerzenia oraz doszczegółowienia ich o działania mające na celu neutralizację zagrożeń w cyberprzestrzeni.

Źródła: Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok.

Znacznie Cyber Threat Intelligence (CTI) dla zapewniania bezpieczeństwa wyborów

Sumarycznie w 2024 roku w blisko 70 krajach świata, znajdujących się na wszystkich zamieszkałych kontynentach odbędą się głosowania wyborcze. Umożliwi to oddanie swojego poparcia przez ponad 4,2 mld ludzi. Nie licząc odbytych wyborów samorządowych w Polsce, czekają nas jeszcze 9 czerwca ogólnoeuropejskie wybory do Parlamentu Europejskiego oraz z pewnością medialnie głośna elekcja na stanowisko prezydenta w Stanach Zjednoczonych.

Przeprowadzenie wyborów krajowych czy lokalnych w zdigitalizowanym świecie wiąże się z nowymi wyzwaniami dla bezpieczeństwa całego procesu wyborczego, wykraczającymi swoimi zasięgiem daleko poza geograficzne granice państw. Mowa tu nie tylko o samej procedurze elekcji, ale również o uczciwości i wiarygodności prowadzonych kampanii wyborczych. Po analizie incydentów związanych z próbami wywierania wpływu na opinię publiczną w mediach społecznościowych przez rosyjskie służby specjalne (m.in. przy wyborach w USA w roku 2016 i 2020, w brytyjskim referendum dot. *Brexitu* czy głosowaniu w sprawie autonomicznego statusu hiszpańskiej Katalonii), instytucje z całego świata podejmują działania celem niwelowania ryzyka wynikającego z incydentów w przestrzeni cyfrowej. Efektywna analiza zagrożeń w cyberprzestrzeni (ang. CTI) przez komórki i zespoły analityczne odgrywa kluczową rolę w utrzymaniu bezpieczeństwa procesu wyborczego na każdym z jego etapów.

Praca wymienionych zespołów polega na analizie i syntezie danych oraz informacji, wnioskowaniu, a finalnie tworzeniu materiałów stanowiących podstawę szacowania ryzyka, jak i prognostyczne scenariusze zagrożeń umożliwiających implementacje rozwiązań wyprzedzających potencjalne ataki. Odbywa się ona na wszystkich poziomach zarządzania (strategicznym, taktycznym, operacyjnym).

Aby uzyskać te informacje zespoły ds. bezpieczeństwa realizują swoją działalność na poziomie informacyjnym i technicznym. Prowadzą nie tylko stałą analizę mierników zagrożeń umożliwiającą określanie trendów, atrybucji grup APT czy badania wskaźników kompromitacji (IOC). Dokonują również ciągłej wymiany informacji w zakresie współpracy międzynarodowej, międzyinstytucjonalnej, partnerstwa publiczno-prywatnego oraz wykorzystują komercyjne, jak i publiczne opracowania z zakresu analizy zagrożeń w cyberprzestrzeni.

Szczęśliwie światowa społeczność CTI hojnie dzieli się wytworami własnej pracy, dostrzegając efekt synergii. Udostępniane treści stanowią kluczowe i zarazem podstawowe źródło wiedzy o zagrożeniach. Ze względu na sieciocentryczność i unifikację stosowanych systemów i narządzi powstaje ogrom danych możliwych do zastosowania we własnych materiałach analitycznych i rozwiązaniach technologicznych. Pozwala to skokowo zwiększając poziom bezpieczeństwa własnej infrastruktury. Jednakże ilość przetwarzanych zbiorów danych wymaga efektywnych narzędzi do zarządzania, przetwarzania, weryfikacji, analizy i dystrybucji informacji oraz przede wszystkim wykwalikowanego personelu o odpowiednich kompetencjach do ich obsługi.

Scam w mediach społecznościowych

Ogólna definicja scamu (oszustwo internetowe) mówi, że jest to forma oszustwa przy wykorzystaniu socjotechniki polegająca na nawiązaniu relacji osobowej opartej na zaufaniu miedzy przestępcą, a ofiarą zwykle z zamiarem kradzieży danych osobowych lub wyłudzenia środków finansowych, rzadziej wiąże się z wyciekiem danych czy przejęciem systemów.

Na przestrzeni ostatnich lat, te niechciane zjawisko stało się obok phishingu największą zmorą w sieci internetowej, a w szczególności w portalach społecznościowych, randkowych, skrzynkach mailowych i platformach handlu lokalnego – czyli wszędzie tam, gdzie można wejść w interakcję międzyludzką na odległość bez fizycznego kontaktu.

Przeglądając swoje „tablice", czy pierwsze wyniki wyszukania w popularnych przeglądarkach praktycznie każdego dnia możemy dostrzec wiadomości od „nigeryjskiego księcia", „amerykańskiego żołnierza", dotyczące „spadku po wujku z Ameryki" czy „sponsorowane" posty zawierające niewiarygodnie intratne oferty inwestycyjne lub zakupowe wsparte zdjęciem i opinią popularnych polityków, sportowców, dużych przedsiębiorstw, inwestorów czy powszechnie znanych celebrytów… niewiarygodnie intratne, ale dla osób o zwiększonej świadomości. Scam przy swojej masowości cechuje się wysoką skutecznością, niskimi kosztami i prostotą przeprowadzenia takiego ataku.

Czytając opublikowane po raz pierwszy przez Ministerstwo Cyfryzacji Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023, możemy dowiedzieć się, że w minionym roku sam NASK obsłużył przeszło 370 tys. Zgłoszeń, w tym ponad 80 tys. incydentów bezpieczeństwa, z czego gros stanowiły oszustwa internetowe. Natomiast z informacji pochodzących od CERT Polska, tylko w 2023 roku w Polsce wpisano na listę ostrzeżeń ponad 32 tysiące adresów stron internetowych o złośliwym charakterze.

incydent.cert.pl

Jak walczyć z internetowymi oszustwami?

Kluczowym w tym zakresie jest zachowanie każdego z nas. Możemy wesprzeć bezpieczeństwo internetowej spółczesności czyli nas samych w bardzo prosty sposób. W sytuacji napotkania na podejrzane ogłoszenie, reklamę, portal lub post w mediach społecznościowych – zgłośmy je na stronie Zgłoś incydent | CERT.PL>_ prowadzonej przez NASK. Każde zgłoszenie jest weryfikowane przez zespół analityków pracujących 24/7 – i spotyka się z weryfikacją zgłoszenia przez pracowników CERT Polska. Jeśli domena np. wyłudza dane, podszywa się pod znany podmiot, trafi na aktualizowaną w pięciominutowych cyklach listę ostrzeżeń. Stanowi ona podstawę dla operatorów telekomunikacyjnych do blokowania dostępu do niebezpiecznych i szkodliwych treści.

Źródło: nask.pl, cert.pl

Amerykańska Wspólnota Wywiadów formalizuje podejście do wykorzystania otwartych źródeł – strategia OSINT na lata 2024-2026

Biuro Dyrektora Wywiadu Narodowego (ODNI) i Centralna Agencja Wywiadowcza (CIA) opublikowały dwuletnią strategię przedstawiającą kompleksowe podejście do usprawnienia gromadzenia i wykorzystywania danych wywiadowczych z otwartych źródeł (OSINT).

Strategia OSINT Wspólnoty Wywiadowczej na lata 2024-2026 definiuje cztery strategiczne obszary zainteresowania:

- koordynację pozyskiwania i udostępniania danych z otwartych źródeł w całej Wspólnocie, aby zapobiec powielaniu wysiłków łącząc zasoby w celu stworzenia wspólnego zbioru danych;
- ustanowienie zintegrowanego zarządzania zbiorami danych OSINT – opracowanie mechanizmu dystrybucji w celu osiągnięcia przewagi informacyjnej;
- napędzanie innowacji z tego obszaru – angażowanie środowiska akademickiego, sektora prywatnego i zagranicznych partnerów w celu pozyskiwania nowych narzędzi i doskonalenia rzemiosła;
- inwestycje w zasoby kadrowe w zakresie OSINT oraz rozwój metodologii nowej generacji.

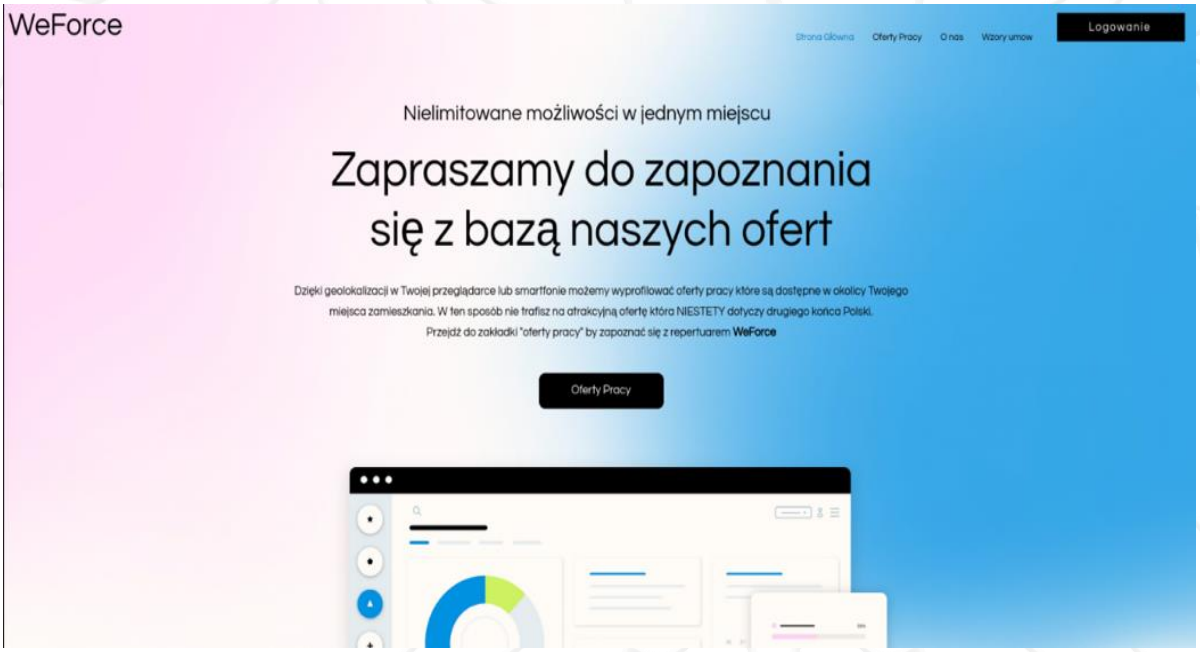
W strategii wybrzmiewa kluczowa rola CIA na tle wszystkich 18 agencji (członków Intelligence Community, czyli Wspólnoty Wywiadów) w implementacji jej założeń. Nie ma jednak wątpliwości, że to Stany Zjednoczone dysponują jednym z najbardziej rozbudowanych systemów do pozyskiwania informacji na świecie, co ma ogromne znaczenie w przypadku podejmowanych decyzji o sposobach realizacji polityki USA, kierowaniu wsparcia międzynarodowego, czy stopnia zaangażowania w politykę zagraniczną danego kraju. Wraz z publicznym uznaniem przez CIA i inne agencje wartości OSINT, ich odpowiednicy z innych krajów prawdopodobnie pójdą w ich ślady. Tym bardziej, że od czasu inwazji Rosji na Ukrainę popularność narzędzi i technik OSINT tylko wzrosła. Ponadto możemy zaobserwować znaczne zwiększenie ilości raportów dotyczących tej tematyki opracowywanych zarówno przez amatorów jak i doświadczone organizacje, co wpływa na szybszy rozwój tego obszaru.

Strategia dostępna jest pod adresem:
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

Szukasz pracy? Uważaj na fałszywe ogłoszenia i oferty od rekruterów oraz próby wyłudzenia poufnych informacji

Oszuści doskonale wiedzą w jaki sposób namówić kandydata na podjęcie działań celem ujawnienia pożądanych informacji (dane osobowe), czy wykonania określonej czynności (przekazanie środków, kliknięcie w link). **Dlatego tak ważne jest zachowanie nieustannej czujności, w tym przypadku w aspekcie wiarygodności zamieszczanych ofert pracy i aktywności w serwisach społecznościowych ukierunkowanych na nawiązywanie relacji zawodowych.**

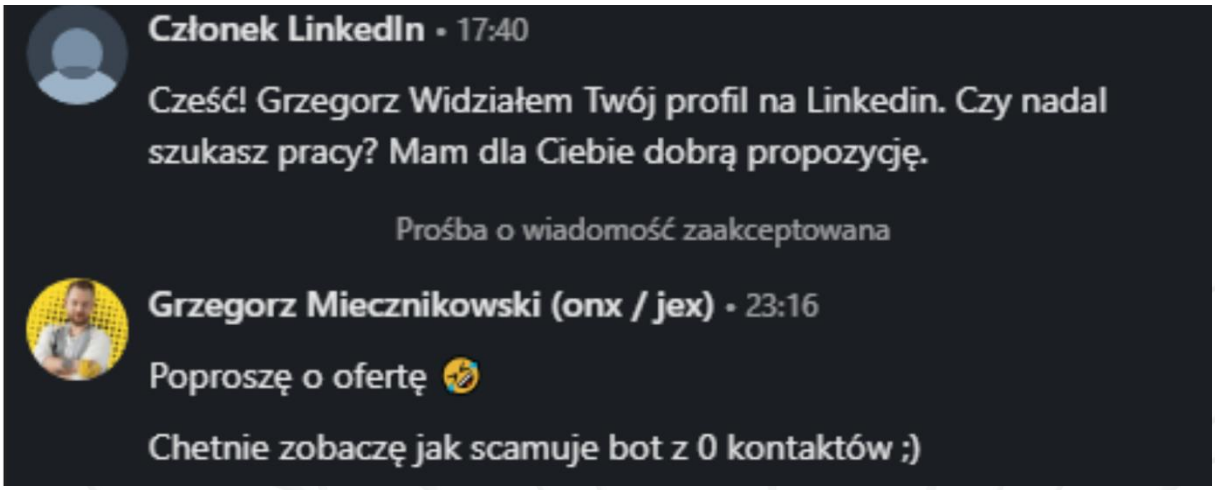
22 marca Niebezpiecznik w serwisie Twitter opublikował informację, że oszuści umawiają się na podpisanie umowy, prosząc jednocześnie o założenie „służbowego" rachunku bankowego do rozliczeń (konto zakładane jest z wysłanego przez cyberprzestępcę linku polecającego). **Podany przykład dotyczył firmy WeForce, która udawała agencję pracy (firma już nie istnieje).** W wiadomościach kierowanych do zainteresowanych ofertami, pracownica WeForce przekonywała, że konto służbowe jest niezbędne do rozliczeń, gdyż pewne czynności będą wymagały przelewów i zwrotów kosztów (motywując to korzyścią, że środki prywatne nie będą mieszały się ze służbowymi). Niebezpiecznik zwrócił uwagę, że domena WeForce[.]biz została utworzona 3 stycznia 2024 r., gdzie firma równocześnie przekonywała, że istnieje na rynku od lat i współpracuje z takimi firmami jak Auchan, McDonalds, czy Biedronka (każda z tych firm zaprzeczyła, iż współpracowała z firmą WeForce. W finale w przypadku tej właśnie firmy WeForce chodziło o to, aby kandydaci założyli „Konto Przekorzystne" w Pekao, które posiada system poleceń (system premii za polecanie kont).



Źródło: https://niebezpiecznik.pl/post/jak-rozpoznac-falszywa-agencje-zatrudnienia-pokazujemy-na-przykladzie/

LinkedIn to międzynarodowy portal społecznościowy, który został założony, by ułatwiać użytkownikom nawiązywanie kontaktów zawodowo-biznesowych, jednak tak samo jak przydatny, serwis może stać się dla nas źródłem zagrożeń ze strony cyberprzestępców. 21

marca użytkownik LinkedIn, Grzegorz Miecznikowski zamieścił wpis dot. fałszywych ogłoszeń o pracę i wyłudzeń w serwisie z przykładem próby oszustwa.



Źródło: https://pl.linkedin.com/pulse/scam-fa%C5%82szywe-og%C5%82oszenia-o-prac%C4%99-i-wy%C5%82udzenia-danych-grzegorz-nbyhf

Oprócz tego, warto mieć na uwadze, że również hakerzy z Korei Płn. wykorzystują aktualnie ChatGPT do oszustw z wykorzystaniem serwisu LinkedIn. Microsoft, który jest właścicielem LinkedIn, zauważył, że Emerald Sleet, znany również jako Kimsuky (grupa APT powiązana z Koreą Płn.), podszywał się pod "renomowane instytucje akademickie i organizacje pozarządowe, aby zachęcić ofiary do udzielania odpowiedzi dot. eksperckich spostrzeżeń i uzyskiwania komentarzy na temat polityki zagranicznej związanej z Koreą Północną". Północnokoreańskie grupy hakerskie tworzą wiarygodnie wyglądające profile rekrutacyjne w serwisach takich jak LinkedIn, a generatywna sztuczna inteligencja pomaga w wysyłaniu wiadomości, generowaniu obrazów, nowych tożsamości – wszystko czego potrzeba, aby zbudować bliskie relacje z celem.

Szukając pracy, czy nawiązując nowe relacje biznesowe, bądź po prostu przeglądając treści w mediach społecznościowych, zawsze dokładnie czytajmy treści, które otrzymujemy, sprawdzajmy linki i najpierw się zastanówmy, zanim podejmiemy jakiekolwiek czynności mające na celu udostępnienie swoich danych.

Więcej informacji nt. przypadku firmy WeForce można znaleźć na stronie:
https://niebezpiecznik.pl/post/jak-rozpoznac-falszywa-agencje-zatrudnienia-pokazujemy-na-przykladzie/

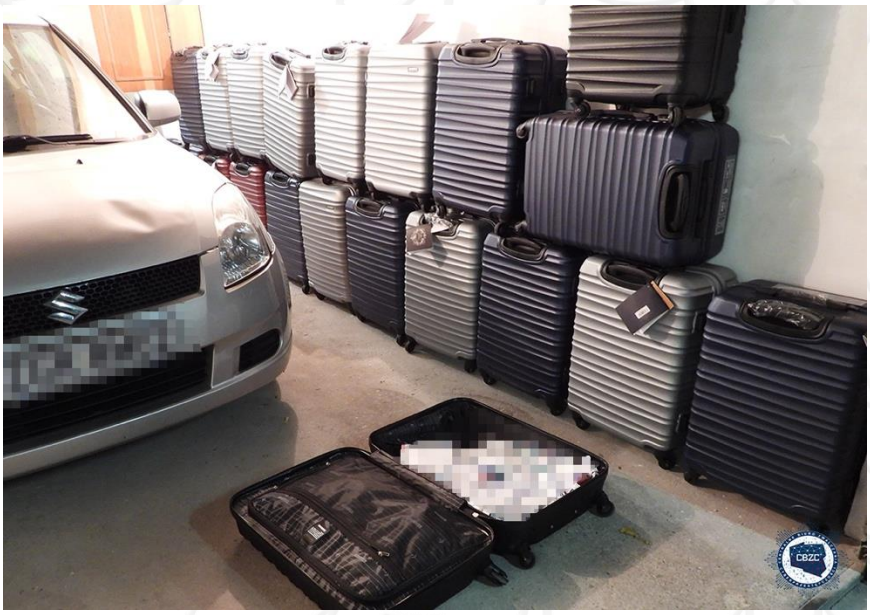
Źródła: readwrite.com, niebezpiecznik.pl

Nielegalnie sprzedawał w sieci leki – został zatrzymany przez funkcjonariuszy CBZC

Funkcjonariusze Zarządu w Poznaniu Centralnego Biura Zwalczania Cyberprzestępczości zatrzymali mężczyznę zajmującego się sprzedażą w Internecie (w tym w Darknecie) leków bez wymaganych prawem zezwoleń. Postępowanie prowadzone jest pod nadzorem Prokuratury Regionalnej w Poznaniu, a koordynowane z Departamentem do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej.

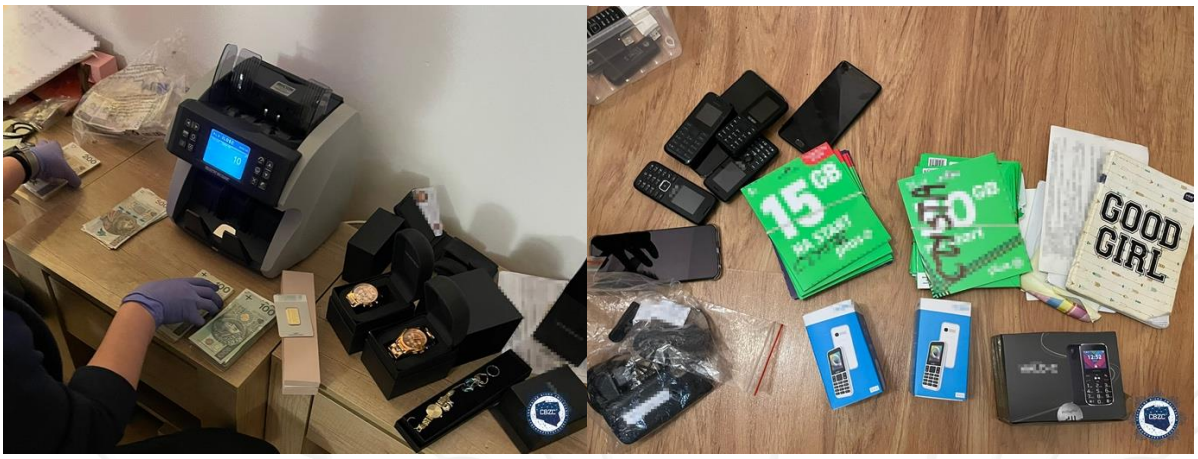
Pieniądze z przestępczego procederu trafiały na konta bankowe podstawionych osób, a sam proces składania zamówień i ich wysyłka utrzymana była przez sprzedającego w warunkach całkowitej konspiracji, celem uniemożliwienia organom ścigania wykrycia procederu, jak i zajęcia środków pochodzących z przestępstwa. Funkcjonariusze zatrzymali również osobę, która pomagała podejrzanemu w prowadzeniu nielegalnej działalności poprzez założenie na swoje dane rachunku bankowego służącego do dokonywania nielegalnych transakcji finansowych. Czynności procesowe prowadzone były pod adresami zamieszkania klientów podejrzanego oraz osób, na które były zarejestrowane telefony, które wykorzystywał podejrzany. Podczas przeprowadzonych przeszukań zabezpieczono telefony komórkowe, karty SIM, sprzęt komputerowy oraz karty bankomatowe.

Dodatkowo w trakcie czynności zabezpieczono gotowe do wysyłki klientom paczki zawierające leki, 27 walizek o pojemności 62 litry każda z lekami bądź opakowaniami po nich, przeszło 5100 opakowań i blistrów z lekami, około 20 litrów leków w substancjach płynnych, susz roślinny, gotówkę w kwocie ponad 80 tys. złotych oraz 2 sztabki złota. Na jednym z zabezpieczonych laptopów, w wyniku wstępnej analizy ujawniono komunikatory umożliwiające anonimową korespondencję, a także aplikacje zapewniające anonimowy dostęp do sieci Internet.



Źródło: CBZC

Do Prokuratury Regionalnej w Poznaniu złożono wniosek o zabezpieczenie majątkowe w kwocie przekraczającej 800 tys. złotych, na które składa się gotówka ujawniona w toku przeszukania oraz dwa mieszkania należące do podejrzanego, zakupione ze środków pochodzących z przestępstwa.



Źródło: CBZC

Sąd Rejonowy Poznań Stare Miasto w Poznaniu na wniosek prokuratora prowadzącego postępowanie wydał postanowienie o tymczasowym aresztowaniu zatrzymanego na okres 3 miesięcy. Sąd podczas posiedzenia w przedmiocie rozpoznania wniosku o tymczasowe aresztowanie zauważył w uzasadnieniu, że: „Zgromadzony do tej pory w sprawie materiał dowodowy wskazuje na ogromne zaangażowanie organów ścigania w ujawnienie całej działalności przestępczej podejrzanego i innych osób w niej uczestniczących i rzeczą Sądu, na wniosek Prokuratora, jest zabezpieczenie postępowania przed możliwym działaniem podejrzanego, by ta praca mogła dalej być w sposób niezakłócony kontynuowana”.

Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – ochrona klienta

W marcu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 6 249 domen (w styczniu 6 345 domeny), które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe, etc.).
W minionym miesiącu przestępcy nieustannie stosowali, znany pod nazwą „**fraud inwestycyjny**", schemat działania. **W ramach niego podszywali się pod znane osoby oraz instytucje, celem nakłonienia potencjalne ofiary do rzekomego zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzili grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe. Przestępcy nadal wykorzystują metodę deepfake do tworzenia fałszywych treści.** Jakość przygotowywanych przez nich materiałów jest coraz bardziej wiarygodna. Zebraliśmy zbiór przykładowych fałszywych reklam do stworzenia których atakujący wykorzystali sztuczną inteligencję, zapoznać można się z nim pod adresem: *https://cebrf.knf.gov.pl/deepfake*
W prowadzonych analizach regularnie zauważamy również kampanie phishingowe podszywające się pod polskie Banki. W marcu 2024 roku przestępcy nadal wykorzystywali ten sposób działania. Podszywając się pod takie organizacje jak Santander Bank Polska, Pekao SA, PKO BP, BNP Paribas, Nest Bank, Millennium oraz ING Bank Śląski publikowali reklamy na platformie Facebook oraz wysyłali wiadomości SMS. Pod pretekstem rzekomej możliwości odebrania nagrody lub strasząc blokadą dostępu do aplikacji bankowej wyłudzali dane uwierzytelniające do bankowości elektronicznej oraz dane kart płatniczych. **W marcu 2024 roku analizowaliśmy również kampanie phishingową podszywającą się pod serwis rządowy. Cyberprzestępcy dystrybuowali poprzez wiadomość e-mail informacje o rzekomej konieczności potwierdzenia tożsamości, aby otrzymać zwrot podatku.** W rzeczywistości mieli na celu wyłudzanie danych kart płatniczych. **Na platformie Facebook zidentyfikowaliśmy również fałszywą reklamę podszywającą się pod Miasto Wrocław.** Pod pretekstem rzekomej możliwości wykupienia spersonalizowanej karty miejskiej w niższej cenie, przestępcy zachęcali do kliknięcia w link, który prowadził na stronę phishingową wyłudzającą dane. **Niektórzy z Państwa, mogli również spotkać się z wiadomością SMS, w której widniała informacja o rzekomych zaległych opłatach za przejazdy autostradą.** Wejście na stronę i podanie danych kart płatniczych, było warunkiem koniecznym do uniknięcia dalszych konsekwencji rzekomego zadłużenia. **Przestępcy przygotowali także kampanie phishingowe podszywające się pod firmy kurierskie oraz portale streamingowe.** Tym razem wykorzystywali wizerunek firm InPost, DHL, Netflix oraz HBO. Strony phishingowe dystrybuowane były poprzez wiadomości SMS oraz e-mail. Na fałszywej stronie wyłudzane były dane osobowe oraz informacje o kartach płatniczych.
W trakcie prowadzonych analiz Cyber Threat Intelligence, zespół CSIRT KNF zidentyfikował oraz przeprowadził szczegółową analizę kampanii phishingowej, w której zidentyfikowaliśmy sieć wzajemnie powiązanych fałszywych stron, które wyróżniają się globalnym zasięgiem i są dystrybuowane w rożnych krajach na całym świecie. Cyberprzestępcy w ramach tej kampanii wykorzystywali wizerunek znanych i zaufanych instytucji pocztowych, serwisów streamingowych oraz operatorów telekomunikacyjnych, co znacząco podnosiło skuteczność ich działań. Z raportem zapoznać można się pod adresem:
https://cebrf.knf.gov.pl/images/Kampania_phishingowa_PaaS_PL.pdf

Zachęcamy również do lektury naszego raportu rocznego, w którym prezentujemy podsumowanie cyberzagrożeń dla rynku finansowego w 2023 z perspektywy CSIRT KNF. W opracowaniu znajdują się m.in. statystyki z naszych działań, najczęściej spotykane cyberoszustwa oraz prognozy na rok 2024.
Raport dostępny jest tutaj: *https://cebrf.knf.gov.pl/images/Raport_roczny_CSIRT_KNF.pdf*
„Wiedza to potęga", dlatego (jak zawsze) zachęcamy także do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook.

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

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

Źródło: *https://www.linkedin.com/newsletters/biuletyn-nask-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*