Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

11/2024

SPIS TREŚCI

Scam w mediach społecznościowych

Media społecznościowe obecnie stały się prawdopodobnie głównym, globalnym kanałem komunikacji międzyludzkiej. Służą do nawiązywania oraz do podtrzymywania kontaktów, wymiany danych prywatnych czy publikowania informacji o naszych osiągnieciach zawodowych. Media te, wykorzystywane są także, jako platforma sprzedażowa, reklamowa i portal informacyjny w jednym. Zdecydowana większość z nas posiada kilka kont w różnych sieciach społecznościowych. *DataRePortal.com* w swoim raporcie informuje, że na świecie jest ponad 5,17 miliarda unikalnych użytkowników ww. mediów, co stanowi ok 63.7% światowej populacji. Liczby te mogą robić wrażenie. Technologiczni giganci, tak jak i specjaliści od marketingu internetowego sprawinie potrafią wykorzystać drzemiący w sieciach potencjał do maksymalizacji swoich zysków, jednocześnie dostarczając nam sprofilowany pod odbiorców *content* wpływający na nasze emocje i zachowania. W większości takie działania są etycznie akceptowalne oraz często stanowią formę rozrywki pobudzając nasze zmysły.

Cyberoszustwa inwestycyjne - Komisja Nadzoru Finansowego - www.knf.gov.pl

Niestety, jak to w życiu. Wzrost popularność nowych produktów i usług, sprawia że rośnie także zainteresowanie nimi przez przestępców i oszustów, próbujących zyskać na szkodzie innych. Media cyfrowe stanowią do tego doskonałą platformę. Posiadanie przez przestępców podstawowej wiedzy z zakresów działania organów ścigania, funkcjonowania socjotechniki oraz dysponowanie właściwymi kwalifikacjami technicznymi sprawia, że prowadzone złośliwe kampanie odbywają się przy zachowaniu praktycznie całkowitej anonimowości działań przestępców, co często uniemożliwia efektywną reakcję odpowiednich służb.

Forma nadużyć w sieciach internetowych przyjmuje zwykle formę tzw. „scamu", czyli oszustwa prowadzonego z zamiarem kradzieży środków finansowych. Wg. raportu NASK, CERT Polska w walce z oszustwami komputerowymi w 2023 r. obsłużył ponad 500 tysięcy zgłoszeń o cyberzagrożeniach i zablokował ponad milion wiadomości od oszustów dzięki wzorcom SMS oraz zablokowano 75 milionów prób wejścia na fałszywe strony internetowe. Należy zaznaczyć, że do najpopularniejszych form ataków od

Scam często pojawia się jako strona sponsorowana w popularnych wyszukiwarkach internetowych czy mediach społecznościowych.

kilku lat zalicza się te same grupy: *phishing*; *fałszywe sklepy internetowe*; *oszustwa na portalach ogłoszeniowych*; *fałszywe inwestycje*.

Scam w mediach społecznościowych posiada zmienną intensywność. Wykorzystuje socjotechnikę, aby zwabić potencjalne ofiary. Zwykle można zauważyć rosnącą intensyfikację kampanii oszustów w czasie zwiększonego użytkowania sieci społecznościowych przez odbiorców. Związane to jest z globalnymi wydarzeniami sportowymi, zdarzeniami incydentalnymi jak katastrofy naturalne czy głośne wypadki, kampaniami wyborczymi, czy okresami wzmożonych zakupów typu *blackweek* lub zakupy przedświąteczne.

Przykład oszustwa internetowego – porównaj go z matrycą KNF powyżej.

Niestety mimo wysiłków Ministerstwa Cyfryzacji, NASK, CBZC czy KNF, wciąż nie ma idealnego sposobu, aby przeciwdziałać *scamowi* w sieciach internetowych. Najefektywniejszą metodą zabezpieczenia swojego dobytku jest zdrowy rozsądek i zachowanie higieny cyfrowej.

Ponadto warto przestrzegać kilku podstawowych zasad:

- **Zachowaj wzmożoną ostrożność przy klikaniu linków** - unikaj wchodzenia w podejrzane linki w e-mailach, SMS-ach czy na stronach internetowych.
- **Nie udostępniaj danych osobowych oraz innych**, takich jak numery kart kredytowych, hasła czy dane logowania, nieznajomym osobom ani na podejrzanych stronach internetowych.
- **Używaj silnych, unikalnych haseł do różnych kont i włącz dwuskładnikowe uwierzytelnianie** (jak klucze szyfrowania, tokeny aplikacji, czy SMS) tam, gdzie to możliwe.
- **I najważniejsze - edukacja i świadomość**. Ucz się rozpoznawać różne rodzaje *scamów*, takie jak *phishing*, *smishing* czy *vishing*, i informuj o nich swoich bliskich!

Pamiętaj – zgłaszaj próby wyłudzeń na *zgłoś incydent* | *CERT.PL*

Wzmożona aktywność podmiotów rosyjskich w cyberprzestrzeni

Styk listopada i grudnia były niezwykle intensywnym czasem dla rosyjskich specjalistów od działań informacyjnych, dezinformacji i marketingu wpływu. W minionym okresie odbywały się geopolityczne przetasowania związane z wyborami w krajach uznawanych za nieprzyjazne Rosji (FR), jak USA, czy traktowanych jako tzw. „bliska zagranica" i strefa wpływów – Gruzja, Mołdawia, Rumunia. Ponadto zauważyć można postępujący kryzysy polityczne we Francji i w Niemczech, walki między Palestyną i Libanem a Izraelem, intensyfikacje działań na Ukrainie oraz obalenie reżimu rodu Asadów w Syrii. Wszystkie te zdarzenia łączy występowanie w lokalnych sferach informacyjnych narracji zbieżnych ze strategicznymi i żywotnymi interesami globalnymi Kremla.

Prowadzenie światowej polityki informacyjnej jest zadaniem złożonym, kosztownym i trudnym w swojej istocie. Wymaga posiadania rozbudowanych zasobów ludzkich, intelektualnych, technicznych i know-how. Tylko kto ma sobie z tym poradzić, jak nie Rosja?

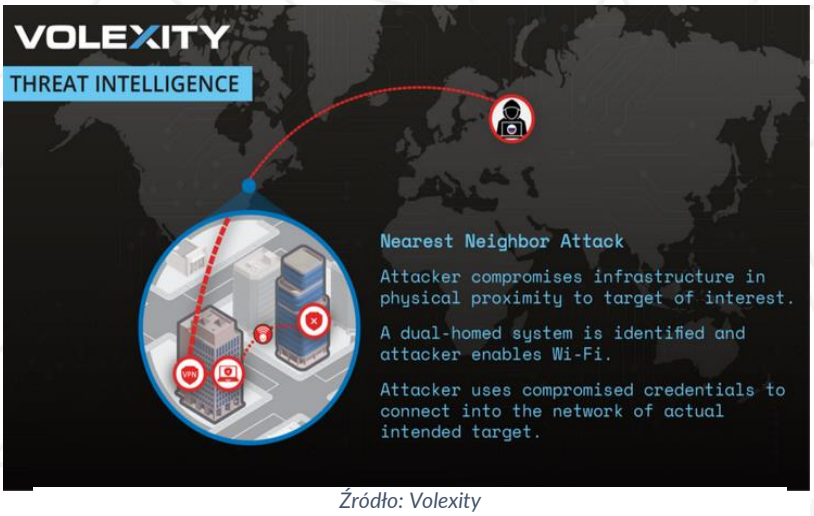
Efektywne realizacja działań poniżej progu wojny, w tym masowej dezinformacji czy kreacji narracji wymaga przede wszystkim zaangażowania najcenniejszego z zasobów, czyli czasu. Budowa zbieżnych z własnymi interesami poglądów w społecznościach lokalnych (krajowych) jest swoistym systemem programowania poglądów społecznych. Narzędzia i metody inżynierii społecznej (socjotechniki) wykorzystywane są latami do budowania kapitału intelektualnego odbiorców oraz ośrodków nadawczych często nieświadomie realizujących swoje działania przy ukrytym w cieniu soft-power FR, często wypieranym przez działania agenturalne i służby specjalne. Należy zaznaczyć, że tzw. „prorosyjskość" rzadko jest widoczna na pierwszy rzut oka. FR wspiera zwykle ruchy skrajne, poglądowo sobie sprzeczne z obu stron politycznej sceny, potęgując polaryzację społeczną będącą naturalną (do pewnego stopnia) cechą społeczeństw. Świetnym przykładem złożoności takich działań jest kampania *„doppelgänger"* upubliczniona w 2022 r. przez *EU DIsinfoLab.*

Jednakże wojna informacyjna to wycinek działalności FR w cyberprzestrzeni. Sama dezinformacja nie jest przedmiotem badań nad cyberbezpieczeństwem, które dotyczy jedynie jego technicznej strony. Należy jednak podkreślić synergiczne wykorzystanie dezinformacji wraz z podejmowanymi działaniami aktywnymi przez rosyjskich hakerów. Same maskowanie grup APT pod nazewnictwem ideologicznie usytuowanych grup haktywistycznych czy cyberprzestępczych jest metodą wprowadzania w błąd opinii publicznej, tworząc poczucie istnienia ideologicznego, anarchistycznego czy antysystemowego establishmentu w mrocznych zakątkach sieci.

Działań przypisywanych do „niezależnych" aczkolwiek prorosyjskich grup hakerskich w ostatnim czasie było sporo. Do przykładów takich operacji zaliczyć można odkryte przez badaczy z *Aqua Nutilus* kampanię DDoS prowadzoną przez grupę *Matrix* wykorzystujące nowatorskie podejścia do omijania systemów antyprzeciążeniowych. Ataki wysoce profesjonalnej i świetnie zorganizowanej grupy haktywistycznej *CyberVolk* wykorzystującej specjalistyczne narzędzia i oprogramowanie ransomware do atakowania celów strategicznych w krajach zachodnich, czy pro rosyjską grupę *RomCom* używającej uważanych za najbardziej intratne podatności typ zero-day w przeglądarkach *Firefox* oraz systemach Windows do implementacji *backdoorów* w korporacyjnych sieciach firm zachodnich.

Atak Nearest Neighbor – jak Rosyjska APT wykorzystała sieci Wi-Fi

Na początku lutego 2022 r., tuż przed rosyjską inwazją na Ukrainę doszło do odkrycia przez firmę Volexity ataku, który następnie został nazwany jako **Nearest Neighbor**. Atak ten polegał na wykorzystywaniu sieci WIFI znajdujących się w bezpośrednim sąsiedztwie celu. Zgodnie z raportem Volexity atakujący uzyskał dane uwierzytelniające do usługi internetowej używanej przez Organizację A, lecz nie mógł ich użyć z powodu włączonego MFA. By ominąć zabezpieczenia atakujący włamał się do sieci Organizacji B która miała swoją siedzibę w pobliżu Organizacji A, tam hakerzy znaleźli system podłączony do sieci za pomocą połączenia przewodowego Ethernet. Za pomocą tego urządzenia, które miało również adapter Wi-Fi atakujący przeprowadził uwierzytelnienie i połączył się do Organizacji A. Wg Volexity atak Nearest Neighbor reprezentuje nowa klasę ataków, która nie była wcześniej opisana, gdzie atakujący narusza bezpieczeństwo jednej organizacji, w celu przeprowadzenia ataku na inny docelowy podmiot. Posiadanie danych uwierzytelniających samo w sobie nie zapewniało dostępu do środowiska, ponieważ zasoby wymagały od logujących się z zewnątrz użycia MFA. Jednak sieć Wi-Fi nie była chroniona MFA stąd możliwe logowanie. Atakujący w celu zatarcia śladów usunął pliki i foldery, używając natywnego narzędzia Microsoftu o nazwie Cipher.exe. Był to pierwszy raz gdy firma Volexity spotkała się z użyciem tego narzędzia. Początkowo nie można było przypisać tego ataku żadnej znanej grupie, przestępcy korzystali w tym przypadku z techniki Living off the land co dodatkowo utrudniało śledztwo. Przełom nastąpił w kwietniu 2024 r gdy Microsoft opublikował badania na temat Forest Blizzard, opisujące narzędzie GooseEgg. Microsoft szczegółowo opisał pliki i ścieżki używane przez hakerów, podobieństwo do ataków Nearest Neighbor pozwoliło określić, iż jest to grupa APT 28 (GruesomeLarch) powiązana z Rosją.



Źródło: Volexity

Dlaczego ten rodzaj ataku jest tak groźny? Wiele organizacji lekceważy bezpieczeństwo sieci WiFi, szczególnie tych wykorzystywanych w urządzeniach IoT, cały czas stosowane są starsze protokoły WPA2 czy WEP mimo, że znane są ich luki, atakujący są w stanie działać niezauważenie przez dłuższy czas. W celu zminimalizowania ryzyka ataku należy zadbać o regularne aktualizowanie oprogramowania routerów, punktów dostępowych i urządzeń IoT, zaleca się stosowanie protokołu WPA 3, monitorować aktywności sieci w celu identyfikacji podejrzanych urządzeń zalogowanych do naszej sieci, zapewnić fizyczny nadzór budynków w celu uniemożliwienia zainstalowania fizycznych urządzeń. Atak Nearest Neighbor stanowi przestrogę dla organizacji i użytkowników indywidualnych. Pokazuje, jak zaawansowane grupy hakerskie potrafią wykorzystywać nieoczywiste wektory ataku do realizacji swoich celów. Raport Volexity podkreśla, że w dobie rosnącej cyfryzacji każda luka w infrastrukturze sieciowej może stać się punktem wejścia dla cyberprzestępców.

Źródło:. Volexity.com, KapitanHack.pl

Halucynacje AI

Sztuczna inteligencja (AI) jest dziś integralnym elementem wielu dziedzin życia – od medycyny, przez edukację, aż po rozrywkę. Jednym z wyzwań związanych z jej rozwojem są tzw. halucynacje AI, czyli sytuacje, w których system generuje treści lub odpowiedzi, które są błędne, nieprawdziwe lub całkowicie niezgodne z rzeczywistością.
Halucynacje AI to zjawisko, w którym modele sztucznej inteligencji generują nieprawdziwe lub mylące informacje, które nie mają oparcia w rzeczywistości. Halucynacje sztucznej inteligencji są często wynikiem ograniczeń związanych z jakością danych szkoleniowych oraz sposobem konstrukcji modeli AI. Systemy generatywne, takie jak duże modele językowe (LLM) czy generatory obrazów, są trenowane na ogromnych zbiorach danych, które zawierają zarówno rzetelne informacje, jak i błędne lub niekompletne dane. W trakcie procesu uczenia się modele analizują wzorce i zależności występujące w danych, ale nie posiadają zdolności rozumienia rzeczywistości ani weryfikacji faktów. W efekcie, podczas generowania nowych treści, mogą powielać lub wzmacniać niedokładności i błędy zakodowane w danych szkoleniowych, co skutkuje tworzeniem odpowiedzi, które wydają się wiarygodne, lecz są nieprawdziwe. Na wystąpienie halucynacji wpływa kilka czynników :

niewystarczające dane szkoleniowe- jeśli model uczony jest na niewystarczającej liczbie danych może nie posiadać informacji niezbędnych do wygenerowania dokładnych wyników.

nieprawidłowe założenia - Dane obciążone błędami. Modele mogą nieświadomie reprodukować te błędy, co prowadzi do generowania nieprawdziwych informacji.

Źródło: cybernews.com

złożoność modelu - złożone modele z wieloma parametrami mogą nadmiernie dopasować się do danych uczących, wychwytując szum i fałszywe korelacje, które prowadzą do halucynacji

prompt engineering - sposób, w jaki użytkownik formułuje zapytania do modelu, ma duży wpływ na generowane odpowiedzi. Niejasne, nieprecyzyjne lub wprowadzające w błąd podpowiedzi mogą zwiększyć prawdopodobieństwo wystąpienia halucynacji.

problemy z generalizacją - modele sztucznej inteligencji mogą mieć trudności z uogólnianiem danych szkoleniowych

Jakie są przykłady halucynacji AI?

Przetwarzanie języka naturalnego (NLP): W przypadku chatbotów lub systemów tłumaczeniowych, AI może generować odpowiedzi, które brzmią poprawnie, ale są faktycznie

błędne lub zmyślone. W obszarze wsparcia technicznego agenci AI obsługujący klientów mogą podawać nieprawidłowe kroki rozwiązania problemu, lub zasugerować nieistniejącą funkcję.

Wizualne systemy rozpoznawania: Modele rozpoznawania obrazów mogą błędnie klasyfikować obiekty. Systemy AI mogą widzieć obiekty których nie ma w rzeczywistości, systemy mogą przypisywać nieprawidłowe znaczenia obiektom np. rozpoznawać zwierzę jako pojazd.

Generowanie fałszywych obrazów - modele generowania obrazów mogą generować realistycznie wyglądające obrazy miejsc, obiektów lub osób, które nie istnieją w rzeczywistości. Systemu AI mogą generować obrazy, których detale są błędne np. ludzi z sześcioma palcami, artefakty w tle czy nienaturalną perspektywę.

Nieprawidłowe tłumaczenia językowe: model sztucznej inteligencji poproszony o przetłumaczenie tekstu z jednego języka na inny może dostarczyć tłumaczenie, które nie ma sensu lub jest niepoprawne gramatycznie.

Konsekwencje halucynacji AI mogą być poważne, zarówno w kontekście indywidualnym, jak i społecznym. W obszarze biznesu błędne dane generowane przez AI mogą prowadzić do strat finansowych, uszkodzenia reputacji firmy czy dezinformacji w treściach marketingowych. W zastosowaniach naukowych lub medycznych halucynacje mogą skutkować fałszywymi diagnozami, błędnymi rekomendacjami lub niewłaściwymi wnioskami badawczymi. Społecznie, generowanie fałszywych informacji przez systemy AI może przyczynić się do rozprzestrzeniania dezinformacji, podważania zaufania do technologii oraz eskalacji napięć społecznych. Dodatkowo, w sytuacjach krytycznych, takich jak zarządzanie infrastrukturą czy bezpieczeństwo, halucynacje mogą prowadzić do nieodwracalnych szkód, w tym zagrożenia życia. Te potencjalne skutki podkreślają potrzebę weryfikacji wyników generowanych przez AI oraz wprowadzania mechanizmów ograniczających błędne działanie systemów. Zapobieganie halucynacjom w generatywnej sztucznej inteligencji wymaga zastosowania odpowiednich strategii na każdym etapie tworzenia i użytkowania modeli. Jednym z kluczowych działań jest weryfikacja i poprawa jakości danych szkoleniowych. Dane powinny być zróżnicowane, reprezentatywne i pozbawione błędów, aby minimalizować ryzyko przekazywania nieprawdziwych wzorców do modelu. Istotne jest także regularne testowanie i walidacja modeli w realistycznych scenariuszach, co pozwala identyfikować i korygować potencjalne problemy, zanim zostaną wdrożone na szeroką skalę. Równie ważne jest zaangażowanie człowieka w proces oceny – użytkownicy mogą zgłaszać błędy i dostarczać informacje zwrotne, które służą do dalszego udoskonalania systemów. Równocześnie istotne jest budowanie świadomości użytkowników na temat ograniczeń sztucznej inteligencji, co pozwala lepiej zarządzać oczekiwaniami i promować odpowiedzialne korzystanie z tych technologii. Poprzez połączenie tych działań można znacznie zmniejszyć ryzyko halucynacji i poprawić jakość oraz wiarygodność generatywnej AI. Halucynacje AI to poważne wyzwanie, które wymaga zarówno postępu technologicznego, jak i refleksji etycznej. Choć sztuczna inteligencja ma ogromny potencjał, konieczne jest zachowanie ostrożności i rozwijanie systemów w sposób odpowiedzialny.

Źródła: ifirma.pl, pl.sembot.com, undetectable.ai

Wnioski z ćwiczeń KSC-EXE 2024

Pod koniec listopada odbyły się ćwiczenia krajowego systemu cyberbezpieczeństwa KSC-EXE 2024. Ćwiczenia inicjowanie są przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa na podstawie ustawy o krajowym systemie cyberbezpieczeństwa, a ich celem jest sprawdzenie działania procedur oraz weryfikacja operacyjnych zdolności podmiotów krajowego systemu cyberbezpieczeństwa (KSC) w sytuacji kryzysowej spowodowanej cyberatakiem.

Ćwiczenia KSC-EXE 2024, podobnie jak w 2020 r., zorganizowane zostały przez Ministerstwo Cyfryzacji oraz Fundację Bezpieczna Cyberprzestrzeń. Formuła ćwiczeń "Table Top Exercises" (TTX) umożliwiła symulację zdarzeń, które mogą wystąpić w rzeczywistości, a także analizę odpowiedzi organizacji na incydenty teleinformatyczne.

W ćwiczeniach udział wzięło prawie 60 przedstawicieli podmiotów krajowego systemu cyberbezpieczeństwa, w tym:

- organy właściwe: MKiŚ, MI, MZ, KNF, MC;
- zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego, czyli: CSIRT GOV, CSIRT MON, CSIRT NASK;
- przedstawiciele: MSZ, PK, RCB, UKE, CBZC.

Ćwiczenia KSC-EXE 2024 pozwoliły na szczegółową weryfikację procedur reagowania na incydenty oraz współpracy między podmiotami odpowiedzialnymi za cyberbezpieczeństwo. W trakcie symulacji, uczestnicy musieli podejmować decyzje w obliczu różnych scenariuszy, które miały na celu sprawdzenie ich zdolności do szybkiego i skutecznego reagowania na zagrożenia.

Tegoroczne ćwiczenia były szczególnie ważne z uwagi na nadchodzącą nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, która w 2025 roku wdroży unijne wymogi dyrektywy NIS 2. Ćwiczenia stanowią istotny element w przygotowaniach do zmian w przepisach prawnych, które wprowadzą wyższe standardy bezpieczeństwa w cyberprzestrzeni.

Wśród najważniejszych zidentyfikowanych wniosków należy wymienić:

- Powołanie centralnej instytucji odpowiadającej za cyberbezpiczeństwo na poziomie krajowy oraz dalsze wzmacnianie, instytucjonalizację i sformalizowanie działania Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), pozwoli lepiej reagować i koordynować działania instytucji KSC. Potrzebne jest też wzmocnienie kompetencji Pełnomocnika Rządu ds. Cyberbezpieczeństwa, aby lepiej koordynować działania na poziomie strategicznym. Zasadne jest także włączenie do udziału w PCOC Prokuratury Krajowej, aby usprawnić współpracę CSIRT-ów i organów ścigania.
- Również skład Zespołu ds. Incydentów Krytycznych (ZIK) należałoby rozszerzyć o organy ściągania, jak również włączyć w skład ZIK Pełnomocnika Rządu ds. Cyberbezpieczeństwa (zgodnie z procedowanym projektem nowelizacji ustawy o KSC Pełnomocnik będzie przewodniczył ZIK).
- Wprowadzenie mechanizmów polecenia zabezpieczającego ministra właściwego ds. informatyzacji oraz możliwości wykluczenia dostawcy wysokiego ryzyka (HRV), które również są przewidziane w nowelizacji, usprawniłoby i przyspieszyłoby opanowywanie sytuacji kryzysowej.
- Kluczowa jest sprawna i szybka wymiana informacji, do czego przyczyni się rozwijany system S46, który wzbogacany jest o nowe funkcjonalności, a po nowelizacji ustawy o KSC stanie się obligatoryjnym „jednym okienkiem" do zgłaszania incydentów i wymiany informacji.
- W przypadku poważnych sytuacji kryzysowych ważna jest komunikacja strategiczna, która w przypadku zdarzeń z zakresu cyberbezpieczństwa powinna być prowadzona przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa we współpracy z zespołami CSIRT oraz Centrum Informacyjnym Rządu działającym przy KPRM.

Źródła: Ministerstwo Cyfryzacji.

Prywatne telefony polityków na celowniku hakerów

Prywatne urządzenia osób sprawujących eksponowane stanowiska polityczne, takie jak smartfon, czy tablet, co raz częściej stają się celem działań hakerów, w tym tych powiązanych ze służbami wrogich państw. Dzieje się tak ponieważ na całym świecie wciąż wielu polityków wykorzystuje prywatne urządzania do celów służbowych.

W ostatnim czasie szef MSZ Francji kliknął wiadomość phishingową w komunikatorze Signal na prywatnym telefonie podczas szczytu G7 we Włoszech pod koniec listopada. Po powrocie do kraju polityk poprosił zespół swojego ministerstwa odpowiedzialnego za cyberbezpieczeństwo o sprawdzenie urządzenia. Analiza nie wykryła żadnych luk w zabezpieczeniach. Pierwsze wyniki szybko wykluczyły obecność markerów powiązanych z oprogramowaniem szpiegującym Predator i Pegasus.

Jednak jak się okazało pogłębione analizy nie mogły być niezwłocznie przeprowadzone przez francuską Narodową Agencję ds. Bezpieczeństwa Systemów Informacyjnych (ANSSI), gdyż minister odbywał serię podróży służbowych. W związku z tym miano mu zalecić rozszerzenie zwykłych procedur bezpieczeństwa stosowanych w delegacjach (podczas podróży za granicę francuscy ministrowie muszą przez cały czas korzystać z trybu samolotowego i łączyć się wyłącznie z pojedynczym routerem, aby uzyskać dostęp do Internetu). Te wyjaśnienia byłyby dalekie od rozwiania obaw ekspertów ds. cyberbezpieczeństwa. Według francuskich mediów, dopiero gdy telefon ministra wysłał podejrzaną wiadomość do jego odpowiednika w Bahrajnie, polityk zorientował się, że jednak został zhakowany. Francuskie władze zostały ostrzeżone przez dyplomację Bahrajnu, która miała być zaskoczona niedyplomatycznym tonem korespondencji. "Drogi ministrze, mam nadzieję, że czujesz się dobrze. Czy możemy do siebie zadzwonić?" – brzmiała wiadomość od rzekomego francuskiego szefa dyplomacji.

Szef francuskiego MSZ, były minister cyfryzacji. Źródło: RTL.

Wykorzystywanie do celów służbowych wyłącznie służbowych urządzeń i kont jest podstawową zasadą higieny cyfrowej, która powinna być także uregulowana w wewnętrznych przepisach danej organizacji. Szeregowy pracownik mógłby ponieść surowe konsekwencje za nie przestrzeganie tych zasad, a VIP-y...?

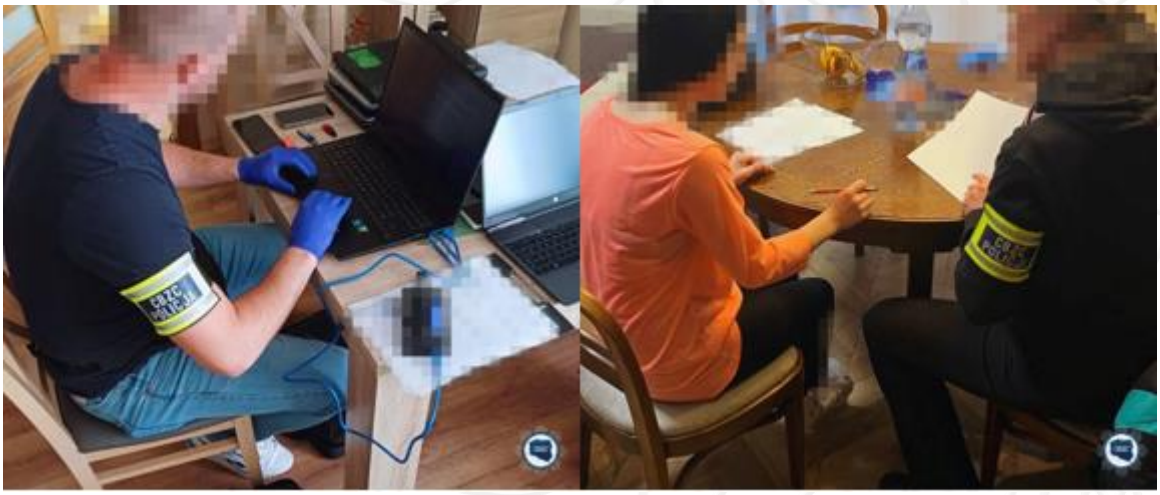
Warto jednocześnie podkreślić, że w celu zapewnienia bezpiecznych środków komunikacji dla administracji państwowej Ministerstwo Cyfryzacji uruchomiło bezpieczną aplikację Komunikator na urządzenia służbowe oraz mobilny system łączności niejawnej SKR-Z. Ministerstwo Cyfryzacji we współpracy z NASK realizuje także projekt SecureV, w ramach którego prowadzone są indywidualne szkolenia dla najważniejszych osób w państwie. Poza tym, w obliczu pojawiających tzw. pranków, Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał w tym roku komunikat z zaleceniami w sprawie oszustw w komunikacji z osobami publicznymi.

Źródła: RTL, Mediapart.

Policjanci CBZC przerwali działalność grupy internetowych oszustów

Policjanci Zarządu w Gdańsku Centralnego Biura Zwalczania Cyberprzestępczości rozbili zorganizowaną grupę przestępczą, która w Internecie zamieszczała fałszywe ogłoszenia. Pokrzywdzeni, którzy zamówili wybrane przedmioty nigdy ich nie dostali a kontakt ze sprzedającymi się urywał. Funkcjonariusze zatrzymali 9 osób, spośród których 6 osób zostało tymczasowo aresztowanych. Podejrzani usłyszeli łącznie 160 zarzutów karnych.

W wyniku czynności policjantów z Zarządu w Gdańsku Centralnego Biura Zwalczania Cyberprzestępczości ustalono, że grupa działała od dłuższego czasu na terenie Łodzi i okolic. Członkowie grupy wyłudzali pieniądze od pokrzywdzonych, w ten sposób, że na jednym z portali społecznościowych zamieszczali fałszywe ogłoszenia m. in. z elektronarzędziami, hulajnogami czy trampolinami. Zainteresowani zakupem klienci w konsekwencji nigdy nie otrzymali zamówionych przedmiotów a kontakt ze sprzedającymi się urywał.



Policjanci CBZC realizujący czynności. Źródło: CBZC.

Podejrzani podejmowali starania aby ukryć swoją tożsamość i uniknąć ścigania, jednak intensywne działania gdańskich śledczych z CBZC, dały efekt w postaci zatrzymania w sumie 9 osób działających w zorganizowanej grupie przestępczej. Dwóch z zatrzymanych było także poszukiwanych w celu odbycia kary pozbawienia wolności za inne przestępstwa.

Śledczy podczas przeszukań miejsc zamieszkania podejrzanych zabezpieczyli dowody cyfrowe w postaci telefonów komórkowych z kartami SIM. Funkcjonariusze znaleźli również narkotyki w postaci amfetaminy i mefedronu.

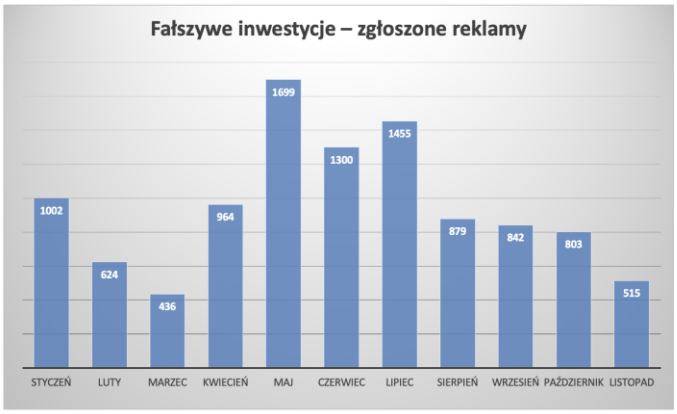
Podejrzani na chwilę obecną usłyszeli 160 zarzutów karnych, udziału w zorganizowanej grupie przestępczej, licznych oszustw internetowych i posiadania narkotyków. Wobec 6 osób zastosowano środki zapobiegawcze w postaci tymczasowego aresztowania, dwie osoby zostało objętych dozorem policji i zakazem opuszczania kraju. Śledztwo jest w toku i kolejne zarzuty będą jeszcze przedstawiane, nadzorowane jest przez Prokuraturę Rejonową w Tczewie.

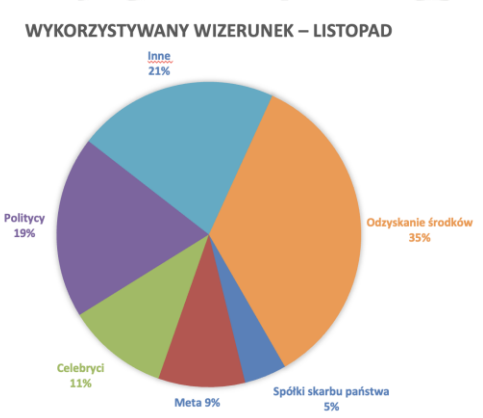
Źródła: CBZC

Podsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

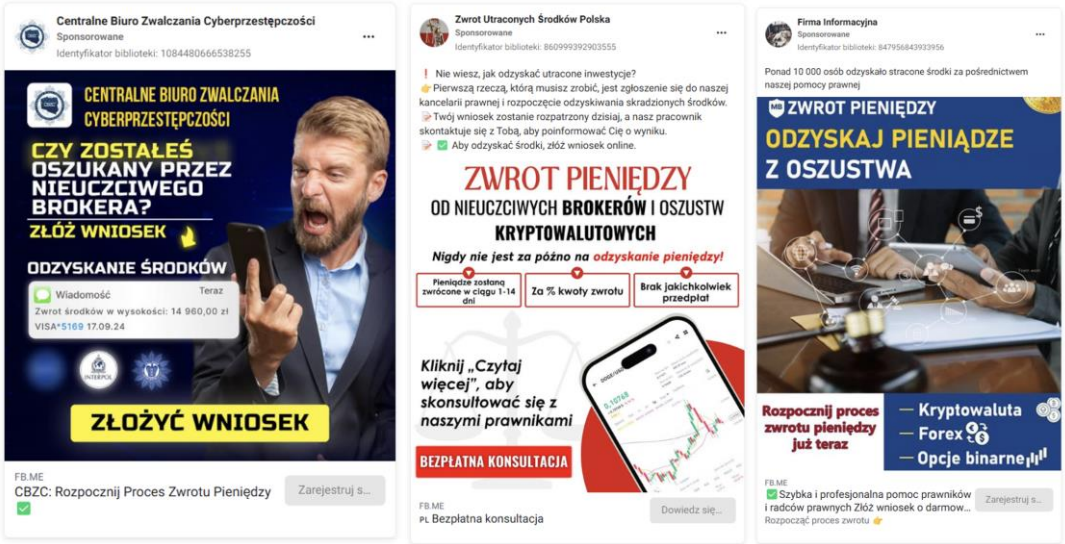
W listopadzie 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 3 502 domeny, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania CERT Polska dodał na listę ostrzeżeń 6 017 domen. A na koniec omawianego miesiąca, na liście hole znajdowało się 251 857 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.

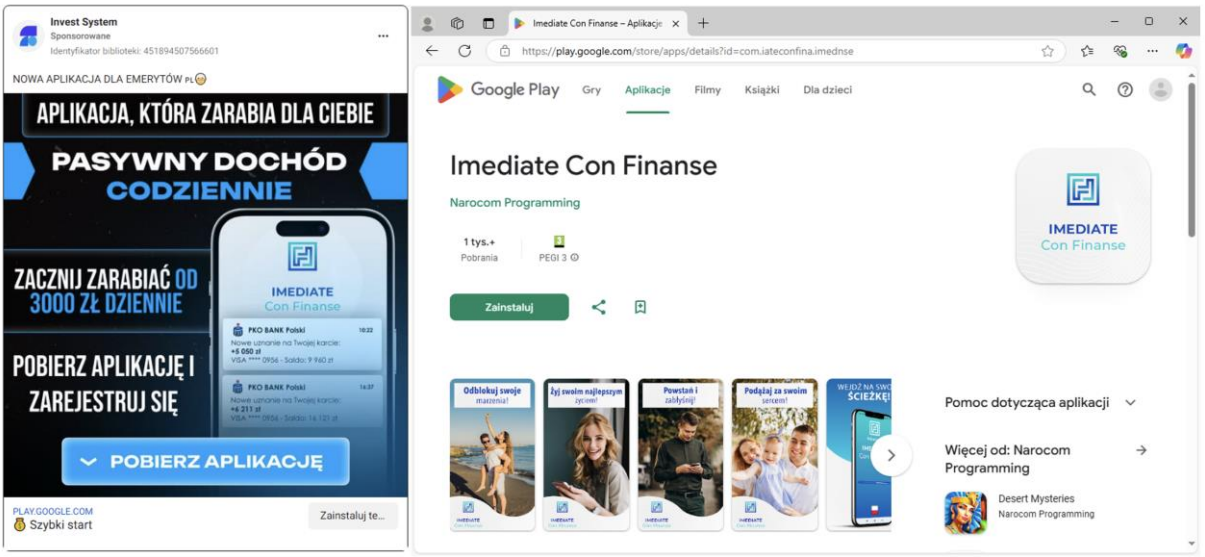




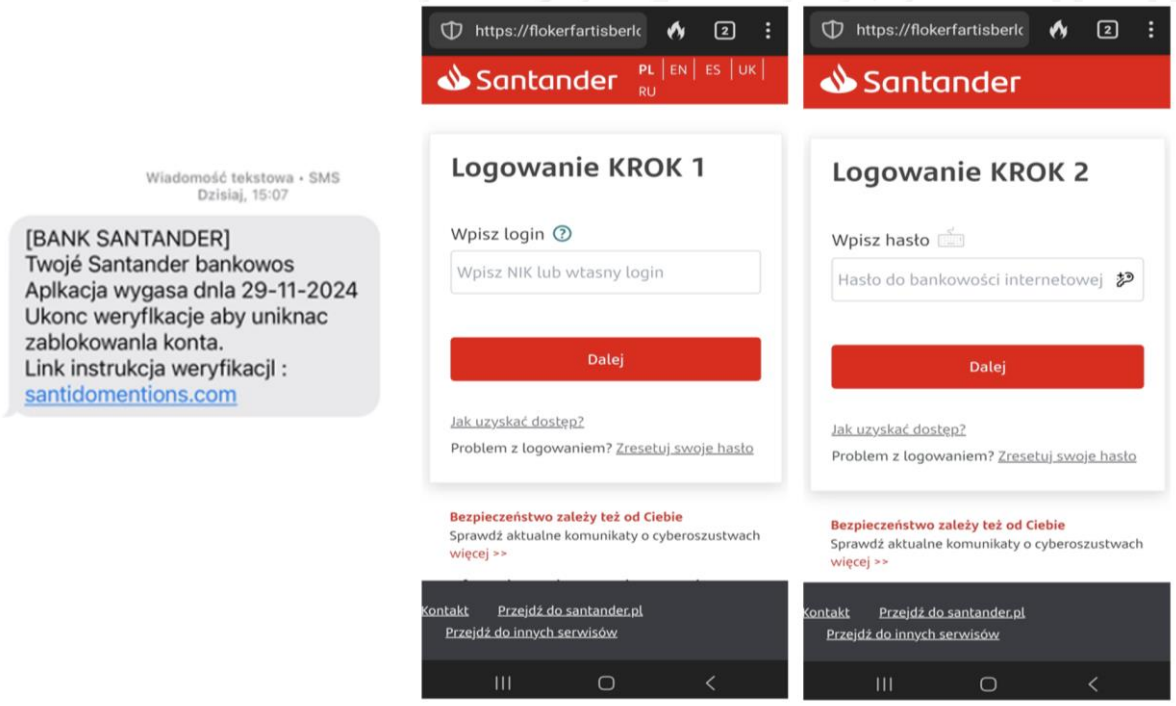
W minionym miesiącu ponownie największy procent wykrytych reklam dotyczył rzekomej możliwości „odzyskania środków". To drugi etap omawianego schematu działania przestępców, w którym przestępcy publikują informację o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości, jest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

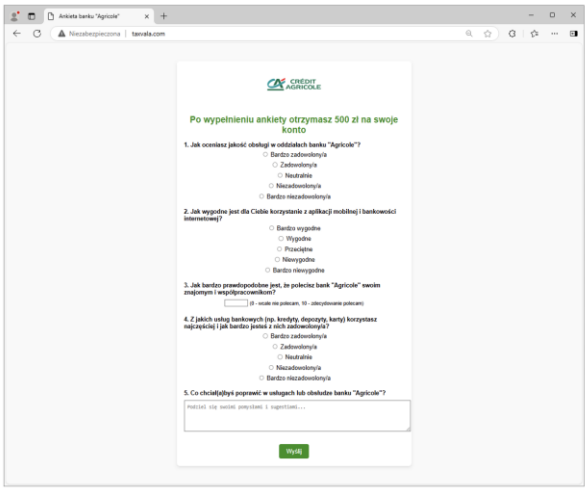


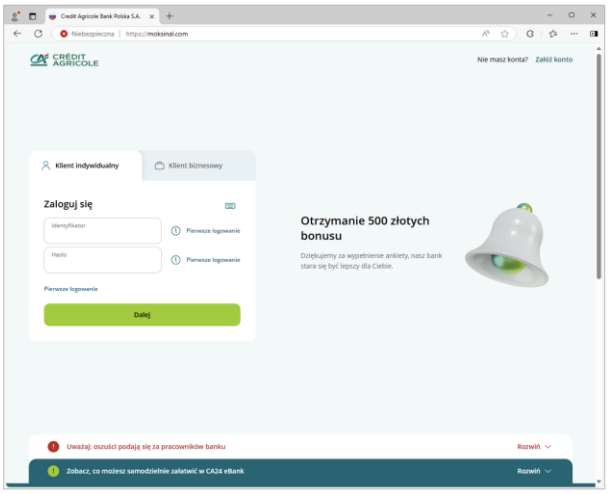
W opisywanym schemacie atakujący nadal wykorzystują nagrania deepfake (https://cebrf.knf.gov.pl/deepfake) oraz fałszywe aplikacje, które nie infekują urządzeń, ale mają na celu zwiększanie wiarygodności przedstawianych przez nich treści.



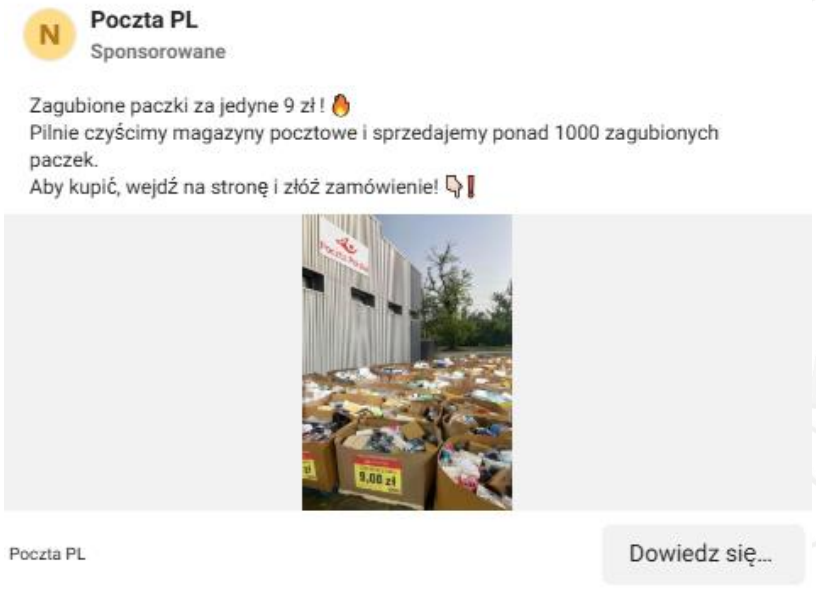
Zidentyfikowaliśmy również kampanie przestępcze podszywające się bezpośrednio pod podmioty z sektora finansowego. Przestępcy wykorzystują wizerunek banków starali się wyłudzić dane uwierzytelniające do bankowości elektronicznej. W kampaniach przestępczych informowali m.in. o rzekomej blokadzie dostępu do bankowości elektronicznej oraz możliwości zdobycia nagrody za wypełnienie ankiety.



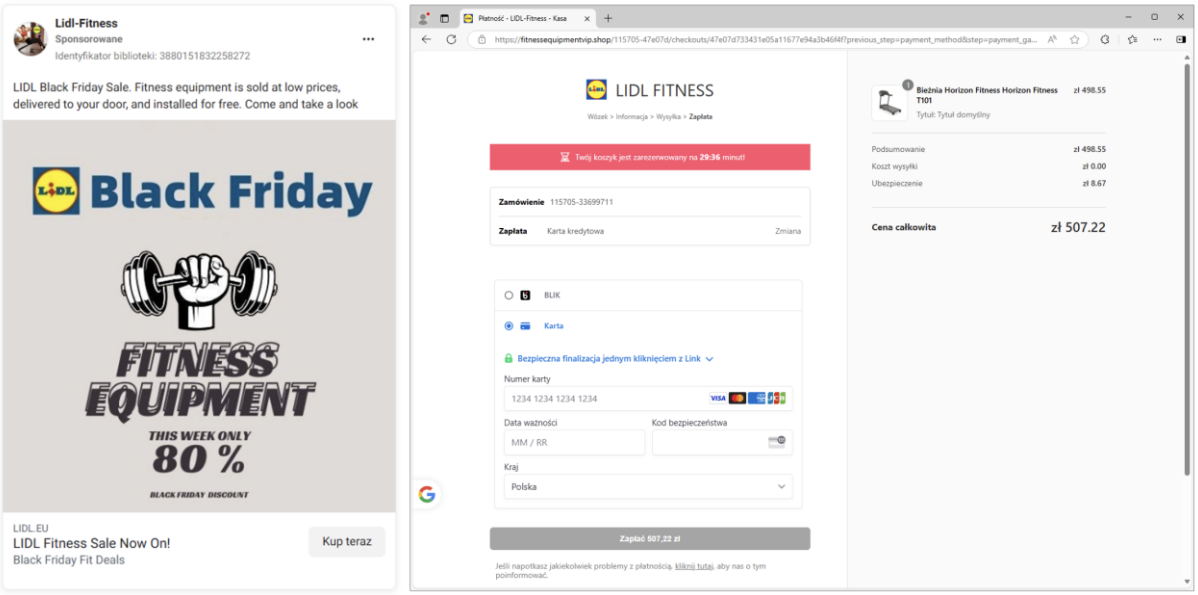




Po raz kolejny przestępcy starali się również wyprowadzać środki z rachunków, wykorzystując do tego tzw. „model subskrypcyjny". Tym razem publikowali reklamy na platformie Facebook, informowali w nich o rzekomej możliwości odkupienia nieodebranej przez kogoś paczki, za jedyne 9zł. Jeżeli ktoś dał skusić się ofertą i kliknął w link, trafił na stronę, na której proszony był o odpowiedź na kilka pytań. Następnie wyświetlał się formularz do wpisania danych osobowych oraz informacji o karcie płatniczej.



Atakujący śledzą otoczenie i wykorzystując to, co obecnie się dzieje. Dostrzegając czas intensywniejszych zakupów, stworzyli fałszywe sklepy, podszywając się pod wizerunki znanych marek. Informacje o nich dystrybuowali poprzez reklamy w mediach społecznościowych, zachęcając wyprzedażami i promocjami. W rzeczywistości starali się wyłudzić dane kart płatniczych. Należy się spodziewać, że w związku ze zbliżającymi się świętami, tego typu kampanie phishingowe będą wykorzystywane przez atakujących częściej, niż dotychczas.



Jak co miesiąc mierzyliśmy się również ze znanymi od dawna schematami, takimi jak „scam na kupującego", podszycia pod platformy streamingowe, wykorzystywanie wizerunku firm kurierskich, Poczty Polskiej i inne, o których poczytać można na stronie internetowej UKNF oraz na profilach CSIRT KNF 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: *nask.pl*

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.