Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

12/2024

SPIS TREŚCI

Podsumowanie roku 2024 i prognozy na rok 2025

Styczeń już tradycyjnie jest czasem podsumowań. I tak jest i tym razem. Rok 2024 był pełen wyzwań dla branży cyberbezpieczeństwa. Przyniósł zarówno nowe zagrożenia, jak i szereg innowacyjnych rozwiązań wspierających bezpieczeństwo, głównie opartych o AI. Dlatego też, w oczekiwaniu na Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za rok 2024 możemy wstępnie ocenić krajobraz zagrożeń cyberbezpieczeństwa za minione 12 miesięcy.

Na podstawie publicznie udostępnianych danych przez komercyjne podmioty bezpieczeństwa wyraźnie widać różnicę w stosunku do ur. Zauważalny jest wzrost liczby ataków. SenitelOne w swoim raporcie podaje listę 5 kluczowych zagrożeń w cyberprzestrzeni. Zaliczył do nich:

Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za rok 2023

1. Oprogramowanie *ransomware* (35% wszystkich ataków, wzrost ataków o 84% rdr);
2. Próby wyłudzenia informacji/*phishingu* (wzrost 1,265% rdr, i stanowiły 40% wszystkich ataków); 3. Ataki na rozwiązania chmurowe (wzrost o 75% rdr, i 23% wszystkich ataków);
4. Urządzenia końcowe; 5. Ataki typu DDoS (+31% rdr). Ponadto w opinii analityków średni koszt naruszenia danych wyniósł 4,88 mld dol. (+10% rdr). Natomiast eksperci z firmy SOCRadar precyzują główne cele ataków *ransomware*. W 2024 r. na liście hakerów dominowały podmioty będące tzw. „trzecią stroną" czyli firmy wchodzące w łańcuchy dostaw innych (przykład ataku na *Cybersecurity and Infrastructure Security Agency (CISA)* z początku 2024 r., przy użyciu podatności w zabezpieczeniach *Ivanti VPN*), często globalnych organizacji. Na wymienionej liście obszarów najczęściej atakowanych znajdują się:

administracja publiczna (ww. atak na *CISA*), ochrona zdrowia (atak ransomware na *Change Healthcare* przez *BlackCat/ALPHV*), instytucje finansowe. Do wyżej wymienionych należy dodać ataki w mediach społecznościowych polegających na wyłudzeniach danych finansowych lub logowania przy wykorzystaniu wizerunku rozpoznawalnych osób (tzw. *socialmedia scam*). W minionym roku było to szczególnie zauważalne ze względu na „globalny rok wyborczy" oraz igrzyska olimpijskie w Paryżu. Ponadto wzrost liczby i zaawansowania ataków jest jednoznacznie wiązany z rozwojem znaczenie sztucznej inteligencji (AI) w cyberprzestępczości oraz wzrostowi „usług cyberprzestępczych na życzenie" (*cybercrime as a service*).

Prognozy na 2025 rok

Rok 2025 przyniesie dalszy rozwój zagrożeń związanych z AI. Sztuczna inteligencja stanie się nie tylko narzędziem wspomagającym ataki (przewiduje się, że AI będzie wykorzystywana do tworzenia bardziej zaawansowanych ataków, takich jak *deepfake'i*, pisanie złośliwego oprogramowania, oraz automatyzacja ataków *phishingowych*. Wg. *CheckPoint* w 2025 roku liczba ataków *phishingowych* z wykorzystaniem AI może wzrosnąć ale również będzie jednym z głównych trendów technologicznych wspierających systemy obronne (popularyzacja oprogramowania chmurowego zabezpieczanego przez m.in. *SPM*, *XDR* oparte o rozwiązania AI oraz transfer infrastruktur informatycznej przedsiębiorstw do chmury).

Kolejnym ważnym trendem będzie wzrost znaczenia cyberbezpieczeństwa w kontekście nowych regulacji prawnych, co jest trendem globalnym (*Deloitte*). W Polsce, ze względu na przewodnictwo w Radzie UE, można spodziewać się intensyfikacji działań na rzecz wprowadzenia regulacji mających na celu zwiększenie bezpieczeństwa cyfrowego. Nowe przepisy mogą obejmować m.in. certyfikację cyberbezpieczeństwa oraz mechanizm wykluczania dostawców wysokiego ryzyka. Powyższe rozwiązania związane są z koniecznością implementacji m.in. *dyrektyw NIS2*, *toolbox'a 5g* czy *DORA* w krajowych systemach prawnych (więcej nt. rozwoju polskiej cyberprzestrzeni zawarto w ***Strategii Cyfryzacji Polski do 2035 roku***).

Wyzwania dla branży IT

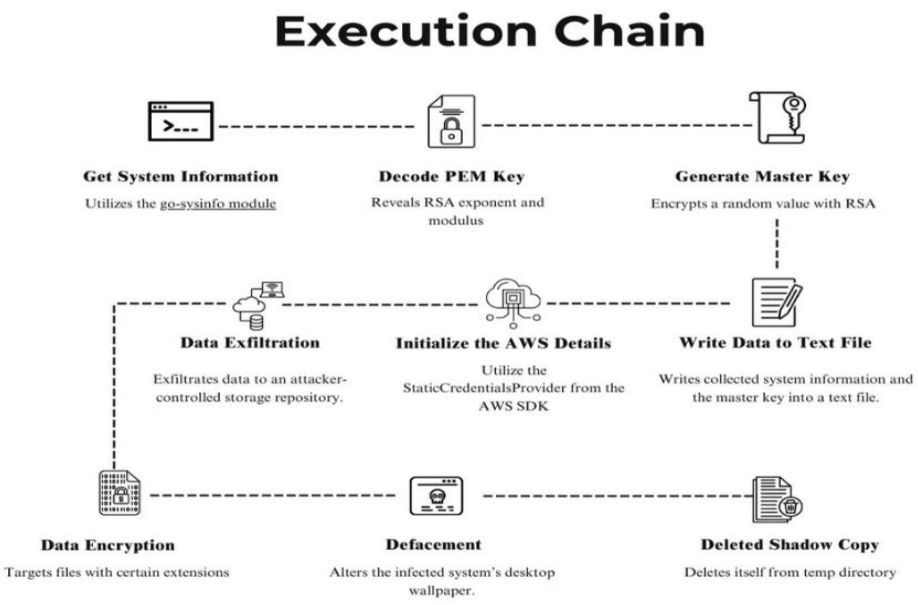
Branża IT w Polsce w 2025 roku będzie musiała zmierzyć się z kilkoma kluczowymi wyzwaniami. Po pierwsze, rosnące zagrożenia związane z wojną hybrydową i cyberatakami na infrastrukturę krytyczną będą wymagały zwiększenia inwestycji w cyberbezpieczeństwo. Po drugie, rozwój sztucznej inteligencji i jej integracja z systemami IT będą wymagały nowych kompetencji i szkoleń dla pracowników. W 2025 roku aż 86% pracodawców planuje rekrutację specjalistów IT, przyniesie to duże wyzwania na rynku pracy w IT. *Raport Płacowy Hays Polska* informuje, pomimo planów rekrutacyjnych wielu firm, aż 53% pracodawców spodziewa się trudności w znalezieniu odpowiednich kandydatów. Wzrost zapotrzebowania na specjalistów ds. cyberbezpieczeństwa oraz ekspertów AI będzie wymagał od firm większych inwestycji w rozwój kompetencji swoich pracowników. W 2025 roku przewiduje się, że liczba ofert pracy w sektorze IT wzrośnie o 15%, co dodatkowo zwiększy konkurencję na rynku pracy.

Podsumowanie

Rok 2025 zapowiada się jako czas intensywnych zmian i wyzwań w obszarze cyberbezpieczeństwa. Firmy będą musiały dostosować swoje strategie do dynamicznie zmieniającego się krajobrazu zagrożeń, inwestując w nowe technologie i kompetencje, aby skutecznie chronić swoje zasoby i dane. Powyższe będzie pokłosiem konieczności dostosowania się nie tylko do nowych ram prawnych, ale również dynamicznie zmieniającego się krajobrazu cyberprzestrzeni.

NotLockBit – nowe zagrożenie ransomware

W ostatnim czasie pojawiło się nowe zagrożenie ransomware - złośliwe oprogramowanie NotLockBit. Jak sama nazwa wskazuje twórcy podszywają lub wzorują się na znanym zagrożeniu LockBit, jednak mechanizmy działania oraz cele tej nowej kampanii mają istotne różnice. Przede wszystkim jest to wieloplatformowość – ta odmiana ransomware jest zdolna do atakowania zarówno systemów Windows jak i macOS. NotLockBit posiada również zaawansowane możliwości w tym ukierunkowane szyfrowanie plików, mechanizmy eksfiltracji danych czy samousuwanie. Funkcje te, wraz z możliwością naśladowania istniejących ransomware sprawiają, że NotLockBit stał się znaczącym zagrożeniem w krajobrazie ransomware. NotLockBit został napisany, podobnie jak wiele innych nowoczesnych odmian ransomware w języku GO. Został tak zaprojektowany by celować w szeroką gamę systemów operacyjnych, w tym MacOS, który do tej pory był rzadziej obierany za cel przez twórców ransomware. Co istotne, NotLockBit wykorzystuje usługi chmurowe, takie jak Amazon S3, do przechowywania i kradzieży danych swoich ofiar, co świadczy o zaawansowaniu technologicznym tej kampanii. Oprogramowanie to podszywa się pod ransomware LockBit, używając podobnego interfejsu i technik szantażu, jednak jego działanie i cele są inne. NotLockBit wykorzystuje model „Ransomware-as-a-Service" (RaaS) czyli przestępcy za opłata udostępniają swoje oprogramowanie. Główne cechy NotLockBit: **Szyfrowanie plików** - Po uruchomieniu na docelowym systemie, NotLockBit generuje losowy klucz główny, który jest następnie szyfrowany za pomocą klucza publicznego RSA. Ten zaszyfrowany klucz oraz informacje o systemie są zapisywane w pliku tekstowym na pulpicie ofiary, co umożliwia atakującym identyfikację i potencjalne odszyfrowanie danych po otrzymaniu okupu. Ransomware skanuje system plików, celowo pomijając katalogi, takie jak /proc/, /sys/, /dev/, /usr/ i /run/. Ransomware koncentruje się na określonych typach plików. Obejmują one typowe formaty, takie jak dokumenty, obrazy czy inne często używane pliki (.csv, .doc, .png, .jpg, .pdf, .txt, .vmdk, .vmsd, .vbox). Do szyfrowania zawartości plików używany jest AES a do zabezpieczenia procesu szyfrowania może być używany RSA. W przeciwieństwie do innych ransomware, zaszyfrowane dane są najpierw zapisywane do pliku tymczasowego, który jest



Execution Chain ransomware NotLockBit

następnie przemianowany na oryginalny plik z rozgrzeszeniem .abcd i zapisywany w katalogu oryginalnego pliku. Na koniec ransomware usuwa oryginalny plik, zapewniając, że jego odzyskiwanie bez klucza deszyfrującego jest niemożliwe. Po zakończeniu procesu szyfrowania NotLockBit aktywnie zmienia tapetę pulpitu zainfekowanego systemu. **Eksfiltracja danych** - NotLockBit zbiera szczegółowe informacje o systemie, w tym architekturę maszyny, adresy IP oraz wersję systemu operacyjnego, co może być wykorzystane do dalszych działań przez cyberprzestępców. **Mechanizmy samousuwania** - Po zakończeniu swoich działań, ransomware usuwa się z systemu.

W celu ochrony przed NotLockBit, a także innymi zagrożeniami ransomware powinniśmy:

- Tworzyć regularne kopie zapasowe krytycznych danych, oraz przechowywać je w miejscach offline
- Korzystać ze sprawdzonego oprogramowania antywirusowego z funkcjami ochrony przed ransomware
- Korzystać uwierzytelniania wieloskładnikowego (MFA)
- Zadbać o aktualizację systemu operacyjnego oraz oprogramowania z którego korzystamy
- Przeprowadzać regularne szkolenia dla użytkowników
- Zadbać o segmentację sieci.

Tapeta systemu po ataku ransomware NotLockBit

Ransomware NotLockBit staje się coraz bardziej zaawansowanym, stale rozwijającym się zagrożeniem, ukierunkowanym na wyrządzenie jak największych szkód. Wykorzystuje precyzyjne szyfrowanie plików, udaje innego ransomware (LockBit), usuwa ślady działania by utrudnić wykrycie. Korzysta z technologii szyfrowania AES i wykorzystuje platformę AWS S3, jest wieloplatformowe stanowiąc zagrożenie w systemach MacOS i Windows. To wszystko pokazuje, że cyberprzestępcy nieustannie adaptują swoje metody by zwiększyć zasięg i skuteczność ataków. Dla specjalistów cyberbezpieczeństwa jest to sygnał , że tylko zaawansowane stale rozwijane technologie oraz nieustanne monitorowanie jest wstanie przeciwdziałać tym zagrożeniom. Musimy pamiętać o regularnych aktualizacjach, monitorowaniu swoich zasobów, a także potrzebie edukacji użytkowników.

Źródło: blog.qualys.com, sentinelone.com, securitymagazine.pl

Mechanizm HRV – istota problemu

W procedowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która wdroży w Polsce dyrektywę NIS 2, przewidziano także mechanizm umożliwiający wykluczenie dostawców wysokiego ryzyka (HRV), co stanowić będzie implementację Toolbox 5G. W tej sprawie powielanych jest wiele nieprawdziwych informacji. Dlatego też Ministerstwo Cyfryzacji przygotowało **kompleksowy materiał** rozprawiający się z mitami. Zachęcamy do zapoznania się z nim (szczególnie z infografiką szczegółowo opisującą jak wyglądać będzie podejmowanie decyzji o HRV). Tutaj omówimy kilka kluczowych aspektów.

Instytucja dostawcy wysokiego ryzyka ma eliminować z użycia niebezpieczny sprzęt i usługi z kluczowych dla funkcjonowania państwa systemów. Obecnie nie istnieją środki prawne umożliwiające nakazanie wycofywania tego rodzaju rozwiązań. Mechanizm HRV będzie mieć istotny wpływ nie tylko na bezpieczeństwo państwa, jego instytucji i infrastruktury, ale też na bezpieczeństwo ekonomiczne i społeczne naszego kraju. Sprzęt, który dostarcza niebezpieczne rozwiązania, może zostać wykorzystany do ataku na Polskę, np. poprzez zablokowanie internetu, usług cyfrowych, dostaw prądu czy innych kluczowych usług. Państwo musi mieć narzędzia, aby chronić obywateli przed takimi zagrożeniami. Jest to więc kwestia fundamentalna dla bezpieczeństwa narodowego.

Przy czym trzeba podkreślić, że sama ustawa nie będzie określać, że dany producent uznany zostanie za dostawcę wysokiego ryzyka. Mechanizm HRV nie jest wymierzony w żadną konkretną firmę. Ustawa dopiero ustanowi proces umożliwiający wykluczenie danego typu sprzętu w przypadku zidentyfikowania, że stanowi zagrożenie dla bezpieczeństwa narodowego. Aby procedura taka została uruchomiona muszą wystąpić realne i potwierdzone przesłanki. Taki proces obejmować będzie zarówno szczebel techniczno-merytoryczny (badania przez zespoły CSIRT), jak i strategiczno-polityczny (Kolegium ds. Cyberbezpieczeństwa, w który zasiadają najważniejsi dla bezpieczeństwa państwa ministrowie oraz szefowie służb). Dodatkowo przewidziano możliwość weryfikacji decyzji przez sąd. W procesie tym opcjonalnie będą mogły także uczestniczyć organizacje społeczne i UOKiK. Wszystko odbywać się transparentnie i zgodnie z procedurami. Nie ma tu żadnego automatyzmu ani arbitralności.

Podjęta decyzja będzie uwzględniać zarówno przesłanki prawno-polityczne (ryzyko stworzenia zagrożeń w wymiarze ekonomicznym, wywiadowczym czy terrorystycznym), jak i techniczne, takie jak liczba i rodzaj wykrytych podatności i incydentów, tryb i zakres w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania, posiadanie przez dostawcę certyfikatów. Przy czym ustawa przewiduje długie okresy przejściowe: 4 lata dla podmiotów kluczowych i 7 lat dla pozostałych, co na ogół pokrywa się z cyklem życia sprzętu ICT.

Podsumowanie 2024 roku w Centralnym Biurze Zwalczania Cyberprzestępczości

Miniony 2024 rok z perspektywy Centralnego Biura Zwalczania Cyberprzestępczości, był wymagającym rokiem. Prowadzone realizacje wymagały dużego zaangażowania wielu policjantów z całego kraju i współpracy z zagranicznymi służbami. Ubiegły rok to także stały rozwój Biura, przekształcanie komórek terenowych z wydziałów na zarządy i przyjęcia do służby nowych funkcjonariuszy, a także przygotowania polskiej Policji, w tym policjantów CBZC, do rozpoczętej 1 stycznia 2025 roku prezydencji Polski w Radzie Unii Europejskiej.

WYNIKI PROCESOWE BIURA

Zwalczanie cyberprzestępczości ściśle wiąże się z wykrywaniem, ujawnianiem sprawców takich przestępstw, ich zatrzymywaniem oraz przedstawianiem zarzutów karnych. To główne zadania, jakie realizują policjanci CBZC każdego dnia.

W 2024 roku funkcjonariusze CBZC przedstawili zarzuty karne ponad 1000 podejrzanym, zatrzymali niemal 850 osób, spośród których 312 decyzją sądów zostało tymczasowo aresztowanych. Ważnym elementem walki z cyberprzestępcami jest zabezpieczane im mienie.

I tak w minionym roku śledczy zabezpieczyli od podejrzanych ponad 72 mln zł. Policjanci Biura odzyskali niemal 50 mln zł.

REALIZOWANE SPRAWY

Rok 2024 to wiele działań podjętych na terenie całego kraju ale także na arenie międzynarodowej, co było możliwe dzięki współpracy z organami ścigania innych państw. Każda sprawa to wynik skrupulatnych i czasochłonnych analiz oraz ustaleń. Specyfika przestępstw popełnianych w sieci powoduje, że mają one wielowątkowy charakter i walka z nimi to czasami wiele miesięcy wytężonej pracy policjantów. Z prowadzonych spraw, przypominamy te najistotniejsze z punktu widzenia CBZC.

FRAUDPLACE

Postępowanie to dotyczyło zorganizowanej grupy przestępczej, która sprzedawała witryny fałszywych sklepów lub domen internetowych m.in Allegro, Allegro lokalnie, Olx. Na stronach znajdowały się fałszywe bramki płatności BLIK, gdzie wpisane kody wykorzystywane były do zakupu kryptowalut. Grupa liczyła kilkudziesięciu członków, a infrastrukturę informatyczną stworzyły i założyły osoby nieletnie. W wyniku podjętych działań zatrzymano 29 członków grupy przestępczej, 17 podejrzanych tymczasowo aresztowano, 2 nieletnich trafiło do schroniska dla nieletnich. Podejrzanym przedstawiono 232 zarzuty karne dotyczące udziału w zorganizowanej grupie przestępczej, prania pieniędzy i licznych oszustw internetowych. Dokonano tymczasowego zajęcia mienia na kwotę ponad 200 tys. zł.

HANDEL NARKOTYKAMI W DARKNECIE

Mimo, że walka z przestępczością narkotykową w Internecie nie jest głównym zadaniem policjantów CBZC, to policjanci również takie spawy realizowali w minionym roku.
W ramach tylko jednej z nich, pozwolono zabezpieczyć ponad 1,8 tony narkotyków. Realizacja dotyczyła grupy przestępczej zajmującej się przemytem, produkcją i dystrybucją dużych ilości narkotyków w darknecie.

Sprawcy oferowali do sprzedaży przeciwbólowe leki narkotyczne, psychotropowe oraz bardzo duże ilości narkotyków, tzw. kryształy w postaci 3-CMC i 4-CMC (pochodne mefedronu).

Funkcjonariusze CBZC ustalili tożsamość osób zamieszanych w produkcję i handel narkotykami na terenie całej Polski. Pod koniec czerwca ubiegłego roku na terenie województwa wielkopolskiego i kujawsko-pomorskiego, blisko 100 policjantów przeprowadziło realizację w wytypowanych wcześniej 8 lokalizacjach.

W jednym z domów jednorodzinnych pod Koninem, podczas procesu wytwarzania narkotyków, zatrzymano m.in. dwóch mężczyzn w wieku 52 i 29 lat, jeden z nich okazał się magistrem chemii. Ujawniono również miejsca, w których ukrywano dokumenty służące do legalizowania majątku pochodzącego z przestępczej działalności, gotowe narkotyki, prekursory oraz linie produkcyjne służące do ich wytwarzania.

W toku czynności policjanci zabezpieczyli 1770 kilogramów środków odurzających, psychoaktywnych i ich prekursorów, dwie linie produkcyjne, pieniądze w kwocie blisko 400.000 zł, szereg nośników elektronicznych i ustalono sposób prania pieniędzy

pochodzących z przestępstwa. Jest to dotychczas największa ilość narkotyków zabezpieczonych przez komórki zwalczające cyberprzestępczość w Europie.
Link: Prawie 1,8 tony narkotyków zdjętych z rynku przez CBZC.

OSZUSTWO TYPU BEC (BUSINESS EMAIL COMPROMISE)
Przestępstwo to polega na dostarczeniu w formie poczty elektronicznej sfałszowanej dokumentacji, w której podmieniony jest rachunek bankowy firm, z którymi oszukane spółki prowadzą interesy. W ramach prowadzonego postępowania rozbito zorganizowaną, międzynarodową grupę przestępczą oszukującą spółki na całym świecie (Europa, Ameryka Płn. i Azja) i ustalono członków grupy przestępczej. W ramach tej samej sprawy zgromadzono dowody procederu lokowania korzyści poprzez zakup nieruchomości na dane osób trzecich.

Efekty procesowe to 45 podejrzanych, 8,8 mln zł odzyskanego mienia, 6,9 mln zł zabezpieczenia majątkowego i 12 tymczasowo aresztowanych. Zatrzymano nie tylko tzw. „słupów", ale również członka grupy wykonującego zadania „bankiera" oraz osoby zajmujące się zlecaniem oszustw.
Link: Oszukiwali metodą BEC – cyberpolicjanci z Warszawy rozbili międzynarodową grupę przestępczą

OSZUSTWA METODĄ „NA PRACOWNIKA BANKU"
Policjanci CBZC bardzo aktywnie działają na tym polu, aby ograniczać ten rodzaj przestępczości. Poza działaniami profilaktycznymi, funkcjonariusze m. in. przeprowadzili dużą operację wymierzoną w członków zorganizowanej grupy przestępczej, w wyniku której zatrzymali 13 osób i zabezpieczyli wiele dowodów wskazujących na przestępczą działalność tej jednej z grup. 8 zatrzymanych osób zgodnie z wnioskami prokuratora zostało tymczasowo aresztowanych. Policjanci zabezpieczyli również sztabki złota, biżuterię, pieniądze w różnej walucie w łącznej kwocie ponad 44 tys. zł. i 94 banknoty o nominale 100$, które jak wynika z analizy, mogą być fałszywe.
Link: Podawali się za pracowników banków i oszukiwali właścicieli kont - grupę rozbili policjanci CBZC

W wyniku kolejnej operacji wymierzonej w oszustów stosujących metodę „na pracownika banku" ustalono 21 podejrzanych, spośród których 9 zostało tymczasowo aresztowanych, a 11 zostało objętych dozorem Policji. Funkcjonariusze zabezpieczyli od podejrzanych ponad 400 tys. złotych.
Link: Oszukiwali podszywając się pod pracownika banku – zostali zatrzymani przez policjantów CBZC

OPERACJE „DAKOTA" i „ENOLA GAY" WYMIERZONE W SPRAWCÓW PRZESTĘPSTW O CHARAKTERZE SEKSUALNYM
Walka z seksualnym wykorzystaniem osób małoletnich i przeciwdziałanie udostępnianiu materiałów przedstawiających takie wykorzystanie w Internecie, jest jednym z zadań policjantów Centralnego Biura Zwalczania Cyberprzestępczości. Funkcjonariusze w trakcie prowadzenia czynności współpracują z Departamentem ds. Cyberprzestępczości i Informatyzacji Prokuratury Krajowej, a także prokuraturami w całym kraju. Współpraca

odbywa się również na poziomie międzynarodowym, m.in. z EUROPOL-em, FBI, NCA i amerykańską organizacją walczącą z tego rodzaju nadużyciami NCMEC (National Center for Missing and Exploited Children).

Podczas 2 operacji przeprowadzonych w 2024 roku o nazwie „DAKOTA" i „ENOLA GAY" skierowanych w sprawców przestępstw o charakterze seksualnym, brało udział ponad 700 policjantów. W efekcie tych operacji funkcjonariusze przeprowadzili 215 przeszukań, przedstawili zarzuty 137 podejrzanym i zabezpieczyli niemal 1,2 mln. Plików i 56 osób zostało tymczasowo aresztowanych.

Skrajne przypadki jakie opisaliśmy to: ustalenie mężczyzny, który produkował materiały o pedofilskim charakterze z udziałem swojej kilkuletniej córki, oraz innego mężczyzny, który w dwóch przypadkach wytwarzał takie materiały z udziałem kilkuletnich dzieci pozostających z nim w bliskich relacjach.

Ustalenie mężczyzny, który przeprowadzał remonty mieszkań u znanych mu rodzin, dzięki czemu miał możliwość ukrywania kamery w łazience i nagrywania osób małoletnich. Inny przypadek to kolejny mężczyzna wyszukujący na portalach społecznościowych zdjęcia małoletnich dziewcząt, który podawał się za kobietę i nawiązywał z małoletnimi kontakt on-line, szantażując je i nakłaniał do wysyłania kolejnych obscenicznych materiałów.

Przypadek mężczyzny, który skradł i wykorzystywał wizerunek jednej z agencji reklamowych, co umożliwiło późniejsze wyłudzanie od kobiet zdjęć o charakterze seksualnym ich małoletnich dzieci. Przypadek kobiety, podżeganej przez 6 mężczyzn, do wykorzystywania seksualnie swojego małoletniego syna, a następie udostępniania i sprzedaży materiałów z tych czynów, osobom poznanym na portalu randkowym. Czy też sprawa mężczyzny rozpowszechniającego pliki wideo zawierające treści z seksualnym wykorzystaniem małoletnich osób.
Link: Operacja DAKOTA – uderzenie w przestępczość o charakterze pedofilskim
Link: Krzywdzili dzieci – zostali zatrzymani przez policjantów CBZC!

ATAKI DDOS
Sprawa dotyczyła serii ataków DDoS przeprowadzonych na serwery firmy zajmującej się usługami hostingowymi. Sprawcy w celu osiągnięcia korzyści majątkowej i wyrządzenia szkody firmie, poprzez lawinowo wysyłane miliony zapytań i żądań, zakłócili prace systemu informatycznego, powodując przeciążenie serwerów i zablokowanie dostępu do usług internetowych oferowanych przez firmę. Policjanci zatrzymali 4 osoby, przeszukali 12 lokali, w których zabezpieczyli sprzęt i infrastrukturę służącą do popełnienia przestępstwa oraz skierowali akt oskarżenia do Sądu wobec 4 osób.
Link: Sprawcy ataków DDoS zatrzymani

RATOWANIE ŻYCIA I ZDROWIA W TRYBIE „EMERGENCY"
Policjanci Centralnego Biura Zwalczania Cyberprzestępczości poza wykonywaniem zadań związanych ze zwalczaniem cyberprzestępczości, realizują również czynności w przypadku otrzymania informacji od podmiotów współpracujących z Biurem, z której wynika, że czyjeś życie jest zagrożone.

Właściwa i szybka reakcja na takie zgłoszenie, daje szansę na udzielenie pomocy osobie, która znajduje się w kryzysie emocjonalnym. Policjanci nie lekceważą żadnego zgłoszenia, a każdy sygnał jest szczegółowo sprawdzany.

W minionym roku funkcjonariusze podjęli niemal 3 tys. czynności ustaleniowych, z czego ponad 1700 dotyczyło osób małoletnich. W niemal 850 przypadkach działania zakończyły się umieszczeniem młodej osoby w szpitalu, a w prawie 890 przypadkach przekazaniem osobie najbliższej pod opiekę. Policjanci współpracowali z komórkami organizacyjnymi KGP, KWP, CBŚP, BSWP, Europolem i Interpolem, innymi służbami, zespołami zajmującymi się incydentami komputerowymi (ABW), CERT NASK, CSIRT MON, CEZ, CSIRT KNF, FINCERT oraz operatorami telekomunikacyjnymi, organizacjami zajmującymi się pomocą ludziom w kryzysie: Fundacja Dajemy Dzieciom Siłę, Biuro Rzecznika Praw Dziecka, Niebieska Linia, Gdyński Ośrodek Stażowo-Terapeutyczny, Towarzystwo Przyjaciół Dzieci oraz moderatorami grup na social mediach.

LOGISTYKA

Wydział Wsparcia Logistycznego CBZC we współpracy z Biurem Logistyki Policji, Biurem Łączności i Informatyki i Biurem Finansów Komendy Głównej Policji, oraz wydziałami logistycznymi wszystkich komend wojewódzkich Policji, realizował w 2024 roku postępowania zakupowe, w wyniku których CBZC zostało doposażone w następujący asortyment:

- materiały i sprzęt łączności i informatyki, urządzenia szyfrujące, radiotelefony, zestawy komputerowe stacjonarne oraz mobilne, telefony stacjonarne oraz mobilne, zestawy wideokonferencyjne,
- oprogramowanie z dziedziny informatyki śledczej i techniki operacyjnej,
- sprzęt infrastruktury specjalnej wraz ze wsparciem technicznym producenta na 36 miesięcy,
- flota pojazdów z segmentu C, D, kombi-van, furgon, SUV,
- materiały oraz sprzęt uzbrojenia i techniki specjalnej, kamizelki kuloodporne,
- materiały i sprzęt gospodarczy, kwaterunkowy, administracyjno-biurowy, szafy metalowe,
- zakończono budowy nowych siedzib zarządów terenowych CBZC we Wrocławiu i Łodzi, trwają prace inwestycyjne związane z budową pozostałych siedzib.

DZIAŁANIA PROFILAKTYCZNE

W dobie cyfrowej rewolucji, w której technologia odgrywa kluczową rolę w niemal każdym aspekcie naszego życia, niezwykle ważna jest profilaktyka. Rok 2024 w tym obszarze również był niezwykle aktywny. Przeprowadziliśmy niemal 300 różnego rodzaju spotkań z wieloma grupami społecznymi, głównie młodzieżą i seniorami, w których udział wzięło kilkanaście tysięcy osób. Podczas spotkań omawialiśmy aktualne zagrożenia związane z cyberprzestępczością, metody stosowane przez oszustów, a także przedstawialiśmy warunku i procedurę doboru do CBZC. Podpisaliśmy także 10 porozumień o współpracy ze szkołami i uczelniami wyższymi o profilach technicznych lub informatycznych.

STAN ETATOWY I REKRUTACJA DO CENTRALNEGO BIURA ZWALCZANIA CYBERPRZESTĘPCZOŚCI

Stan etatowy w momencie powołania CBZC (tj. 12 stycznia 2022 roku) wynosił 334 etaty – w tym 300 etatów policyjnych i 34 cywilne. Zwiększanie etatów Biura zostało zaplanowane

na następne trzy lata. I tak kolejno, w każdym roku liczba zwiększała się odpowiednio o 400 i 500 etatów. W tym roku ta liczba osiągnie zakładaną wartość 1800 etatów.

Dobór funkcjonariuszy do Biura rozpoczął się już z chwilą jego powołania. Na początku był to dobór wewnętrzny, polegający na kierowaniu do CBZC funkcjonariuszy z innych komórek i jednostek Policji. W listopadzie 2022 roku rozpoczął się proces rekrutacji dla osób niebędących policjantami. Na koniec 2022 roku służbę w CBZC pełniło 398 policjantów (łącznie z delegowanymi).

W latach 2023 i 2024 w CBZC prowadzono wewnętrzny i zewnętrzny dobór do służby. Od początku trwania rekrutacji w CBZC podania o przyjęcie do służby złożyło 1197 kandydatów. W latach 2023 – 2024 przyjęto do służby 84 osoby. Na dzień 31 grudnia 2024 roku 120 osób zostało w tzw. opracowaniu – na różnych etapach rekrutacji. Porównując dwa ostatnie lata zauważamy wzrost zainteresowania służbą w CBZC – liczba złożonych podań wzrosła ponad dwukrotnie. Na dzień 1 stycznia 2025 roku służbę w CBZC pełni 848 funkcjonariuszy (w tym 50 delegowanych).

PODSUMOWANIE

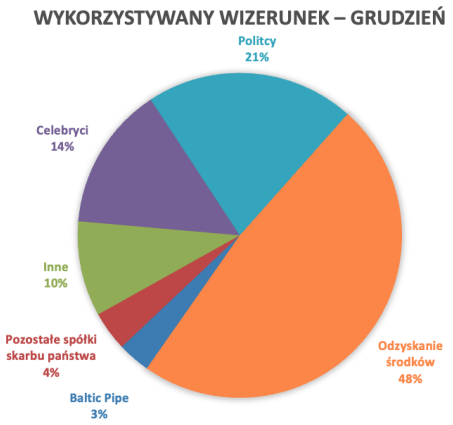
Obecny rok to dalszy rozwój Biura w zakresie infrastruktury technicznej i logistycznej. Planowane są kolejne przyjęcia funkcjonariuszy w ramach stale prowadzonego doboru do służby CBZC. Funkcjonariusze CBZC stale monitorują mechanizmy oraz nowe trendy i scenariusze tworzone przez oszustów, a także na bieżąco reagują na pojawiające się zagrożenia w sieci.

Jesteśmy gotowi na nowe wyzwania, jakie niesie nam 2025 rok!

Podsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

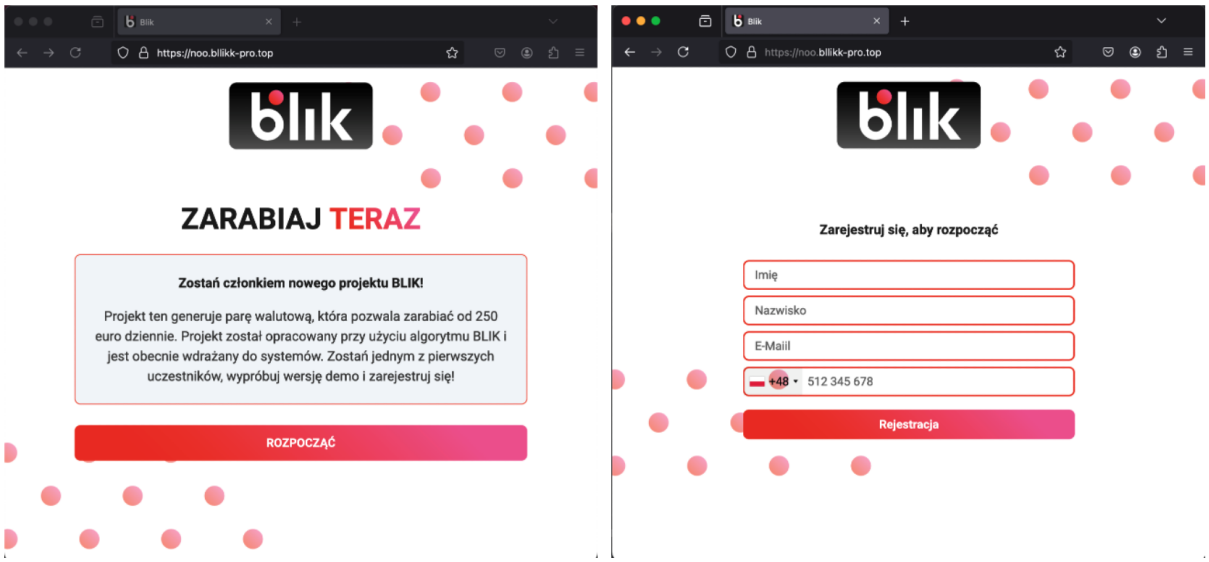
W grudniu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 2 149 domeny, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania CERT Polska dodał na listę ostrzeżeń 4 737 domeny. A na koniec omawianego miesiąca, na liście hole znajdowało się 256 337 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.

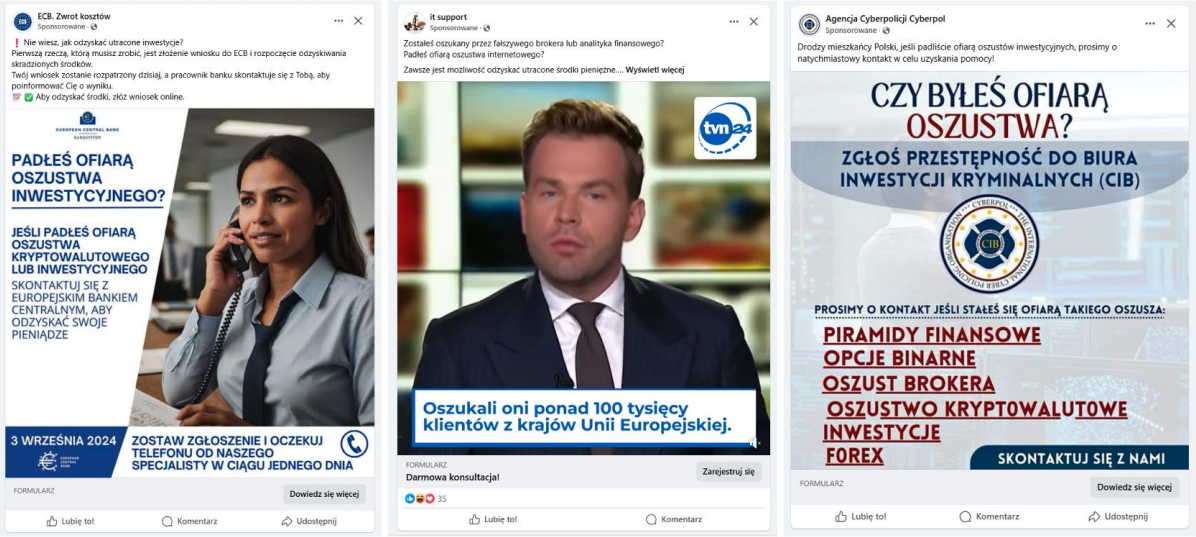


Przestępcy reklamując rzekome inwestycje wykorzystują często wizerunki znanych osób, wizerunki rozpoznawalnych firm oraz motywy rządowe. Nadal chętnie wykorzystują również technologię deepfake do tworzenia materiałów oszukańczych. Przedstawiona treść zachęca do rzekomych inwestycji.

Po kliknięciu w link z reklamy, ofiara trafiała na stronę, na której przestępcy starali się wyłudzić dane kontaktowe.

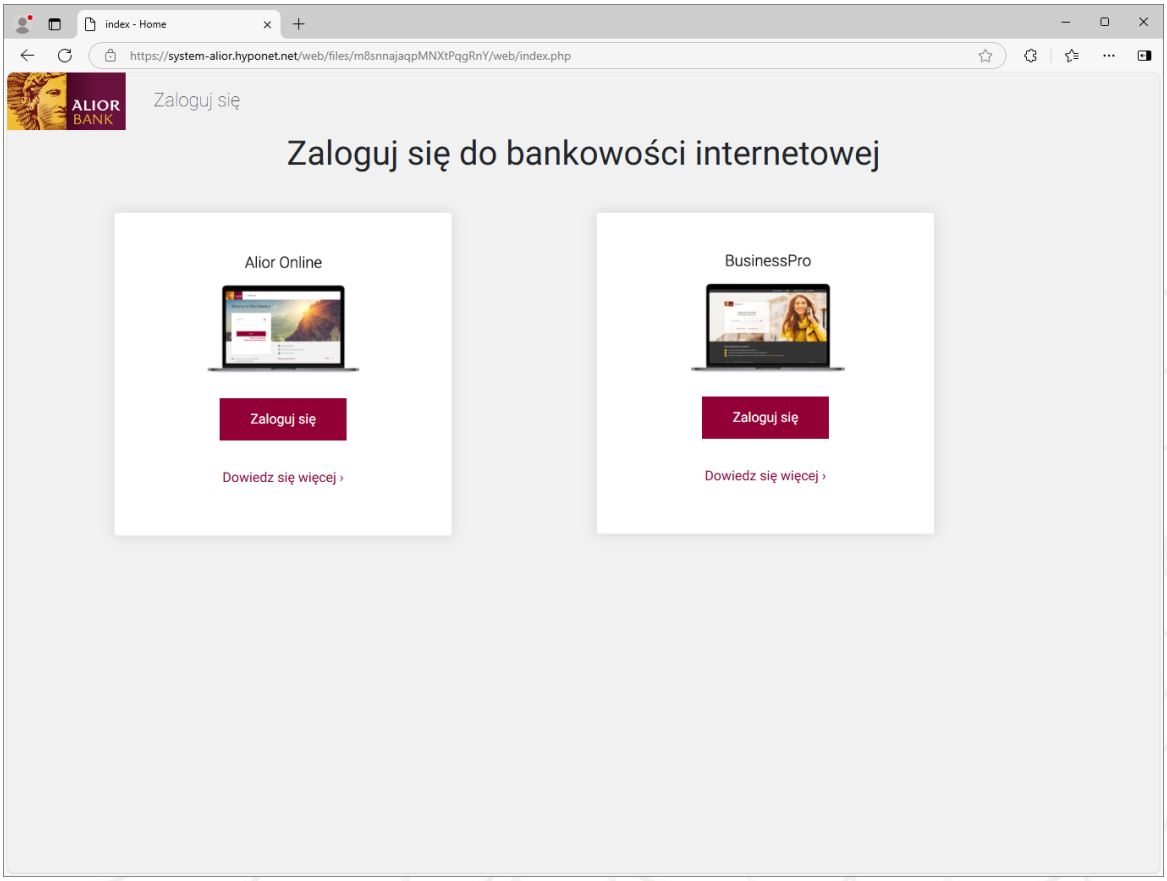


W minionym miesiącu ponownie największy procent wykrytych reklam dotyczył rzekomej możliwości „odzyskania środków". To drugi etap omawianego schematu działania przestępców, w którym przestępcy publikują informację o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości, jest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

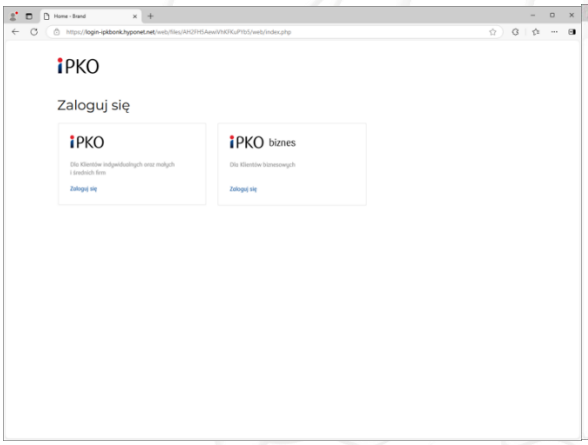


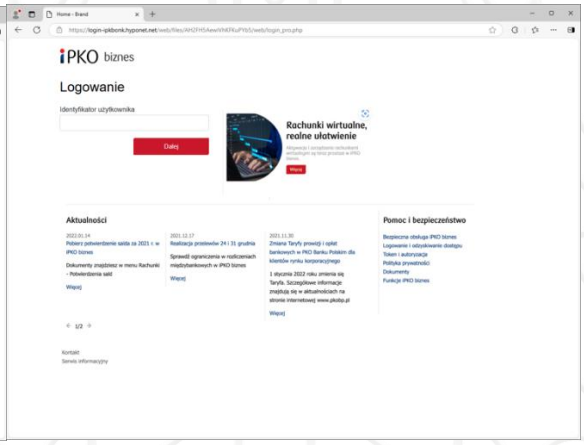
Przestępcy wykorzystują również wizerunek znanych instytucji, aby zwiększać wiarygodność kampanii phishingowych, dlatego też regularnie podszywają się pod polskie Banki. Wyłudzają w ten sposób m.in informacje o kartach płatniczych, dane uwierzytelniające do bankowości elektronicznej, czy kody BLIK. W grudniu 2024 roku nadal wykorzystywali ten sposób. Zidentyfikowane kampanie phishingowe wykorzystywały wizerunki m.in:

Alior Banku:



PKO Banku Polskiego (klienci indywidualni oraz biznesowi):





Banku Peako S.A:

--- Treść przekazanej wiadomości ---

Temat: Hasło wygasło msg id:0014
Data:2 Jan 2025 12:00:21 -0800
Nadawca: Pekao <manager.pko@malagayachts.com>
Adresat:manager.pko@malagayachts.com

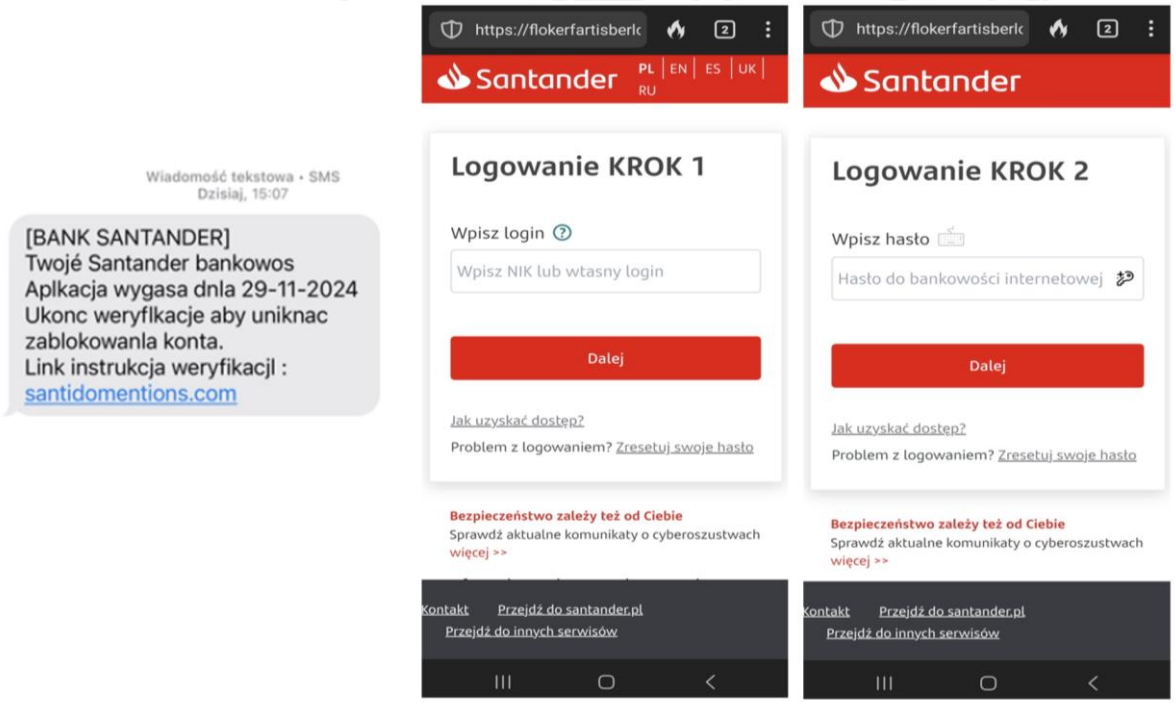
Drogi Kliencie!

Twoje hasło do konta Pekao wygaśnie za 24 godziny. Aby uniknąć zawieszenia, prosimy o aktualizację hasła poniżej lub jak najszybszy kontakt z bankiem.

Zmień hasło

Dziękujemy,
Bank Pekao

Santander Bank Polska:



Jak co miesiąc mierzyliśmy się również ze znanymi od dawna schematami, takimi jak „scam na kupującego”, podszycia pod platformy streamingowe, firm kurierskich, czy fałszywe sklepy. Poczytać o nich 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.