Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

06/2024

SPIS TREŚCI

Centra danych w przestrzeni kosmicznej – nieprawdopodobne, a jednak 3
Sztuka maskowania, czyli jak hakerzy ukrywają malware - wybrane przykłady 5
Wykorzystanie publicznie dostępnych ChatówAI do złośliwej aktywności w cyberprzestrzeni 6
Próby rosyjskich i irańskich oddziaływań na nastroje społeczne przed francuskimi wyborami parlamentarnymi 7
Chmura niejawna na potrzeby cyberbezpieczeństwa państwa 8
Znaczenie hackathonów w rozwoju cyberzdolności 10
Rozbita grupa oszustów, handlująca nieistniejącymi autami 12
Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – ochrona klienta 13
INFORMACJA O SZKOLENIACH 16
Oznaczenia TLP 17

Centra danych w przestrzeni kosmicznej – nieprawdopodobne, a jednak

Rozwój sztucznej inteligencji gwałtownie zwiększa zapotrzebowanie na centra danych i mobilizuje do zbadania opcji przechowywania danych w przestrzeni kosmicznej, m.in. w celu zmniejszenia zapotrzebowania na energochłonne obiekty na ziemi.

Thales Alenia Space, francusko-włoskie konsorcjum oferujące rozwiązania dla przemysłu kosmicznego, ogłosiło znaczący postęp w studium wykonalności wartego ok. 2 mln. euro projektu **ASCEND (Advanced Space Cloud for European Net Zero Emission and Data Sovereignty) finansowanego przez Komisję Europejską w ramach programu 'Horyzont Europa'. Inicjatywa bada opłacalność kosmicznych centrów danych, aby wesprzeć europejski cel osiągnięcia zerowej emisji dwutlenku węgla do 2050 r.**

Współpracując z europejskimi ekspertami (Carbone 4 i VITO – w zakresie zrównoważonego rozwoju środowiska, Orange Business, CloudFerro, Hewlett Packard Enterprise – w kwestii przetwarzania w chmurze, ArianeGroup – systemy startowe oraz niemiecka agencja kosmiczna DLR, Airbus Defence & Space i Thales Alenia Space – w zakresie technologii orbitalnych), **Thales Alenia Space miało za zadanie zweryfikować korzyści środowiskowe i technologiczną wykonalność rozmieszczenia centrów na orbicie.** Na chwilę obecną przekazano, że wnioski są „bardzo zachęcające".

"*Pomysł polega na tym, aby odciąć centra danych od części zapotrzebowania na energię i wysłać je w kosmos, aby skorzystać z nieskończonej energii, jaką jest energia słoneczna*" - powiedział w rozmowie z CNBC Damien Dumestier, kierownik projektu.

Centra danych umożliwiają efektywne zarządzanie zasobami, optymalne przetwarzanie danych i dostarczanie usług, wymagają również dużych ilości energii elektrycznej. **Według Międzynarodowej Agencji Energii, całkowite zużycie energii elektrycznej przez centra danych może dojść w 2026 r. do poziomu 1000 tetrawatogodzin (odpowiadając przy tym zużyciu energii elektrycznej w Japonii).**

Problematyczną kwestię dobrze skomentowała Merima Dzanic, Szef Strategii i Operacji w Duńskim Stowarzyszeniu Przemysłu Centrów Danych:

„*Centra Danych AI potrzebują około trzy razy więcej energii niż tradycyjne centra danych i jest to problem nie tylko po stronie energetycznej, ale także po stronie zużycia.*" Wskazała konieczność zmiany sposobu w jaki budujemy i projektujemy centra danych.

Źródło: thalesaleniaspace.com – poglądowy projekt centrum danych w kosmosie

Co ciekawe, założenie jest takie, aby obiekty wystrzelone w kosmos orbitowały na wysokości około trzy razy większej niż wysokość Międzynarodowej Stacji Kosmicznej. **Projekt ASCEND ma dążyć w kierunku wdrożenia 13 bloków konstrukcyjnych centrów danych o łącznej mocy 10 megawatów w 2036 r. Każdy blok, zgodnie z zapowiedzią, ma mieć powierzchnię 6300 metrów kwadratowych i obejmować pojemność dla własnej usługi centrum danych.** Aby rezultat był dostrzegalny i miał realny wpływ na zużycie energii w sektorze, celowym byłoby wdrożenie 1300 bloków do 2050 r. z założeniem osiągnięcia 1 gigawata. **Dodatkowo ważną kwestią jest konieczność opracowania nowego typu rakiety nośnej, 10 razy mniej emisyjnej, aby znacząco zmniejszyć emisję CO2.** Centrum wymagałoby też znacznych ilości paliwa rakietowego, aby utrzymać się na orbicie. **Aktualnie badacze ASCEND prowadzą projekt w kierunku konsolidacji wszystkich zebranych danych i prac nad opracowaniem rakiety nośnej.** Należy również wspomnieć o innych projektach tego typu, np. wykorzystaniu podwodnego centrum danych przez Microsoft, które zostało umieszczone na dnie morza. Firma prowadzi również badania i współpracuje z Loft Orbital, celem zbadania wyzwań związanych z wykorzystaniem sztucznej inteligencji.

Jeśli chodzi o zalety tego typu projektu, możemy wskazać praktycznie nieograniczoną przestrzeń dostępną na orbicie, eliminującą ograniczenia lądowe, z którymi borykają się naziemne centra danych. W kosmosie bez problemu można alokować ogromne farmy serwerów bez naruszania obszarów na Ziemi. Zwolennicy projektu wskazują na korzyści płynące z ekstremalnych warunków panujących w przestrzeni kosmicznej i możliwości zwiększenia efektywności energetycznej (bez zakłóceń związanych z wzorcami pogodowymi na Ziemi). Umieszczenie centrum danych w kosmosie mogłoby również potencjalnie skrócić czas potrzebny na przesyłanie danych.

Należy również pamiętać o wyzwaniach, które należy pokonać aby urzeczywistnić opisaną powyżej wizję. Jednym z nich jest duży koszt produkcji (choćby niskoemisyjne rakiety nośne), złożoność wdrożenia, czy zapewnienie działania w trudnym środowisku. Dodatkowym aspektem jest chociażby utrzymanie łączności między centrami danych, a placówkami na Ziemi. Do tego dochodzą kwestie związane z przepisami w odniesieniu do przestrzeni kosmicznej (w tym wszystkim jest jeszcze zagadnienie związane ze spójnym podejściem do rozwoju infrastruktury kosmicznej) i kwestiami gospodarowania tą przestrzenią, która jest coraz bardziej upolityczniana i uzbrajana przez różne kraje, czy też konieczność współpracy między agencjami kosmicznymi, rządami oraz firmami prywatnymi.

Komentarz:

Jedno jest pewne, bez wątpienia będziemy świadkami kolejnego wyścigu technologicznego między gigantami branży oraz wspierającymi projekty rządami państw i organizacjami. Przy odpowiednim wsparciu i współpracy, kosmiczne centra danych mogą stać się kluczowym elementem naszej globalnej infrastruktury, torując drogę dla bezprecedensowych postępów w zakresie łączności i możliwości cyfrowych w skali globalnej. Polska powinna wspierać dalszy rozwój technologiczny polskich przedsiębiorców oraz ściągać kapitał zagraniczny w zakresie inwestycji w rozwiązania AI (inwestycje w polskie firmy i startupy), rozwijać centra danych, krajową infrastrukturę IT w tym promować rozwiązania chmurowe (konieczne do pracy z dużymi zbiorami danych) oraz partnerstwo publiczno-prywatne, które znacznie przyspiesza ewolucję technologiczną.

Źródła: cnbc.com, datacenters.com, i-hls.com, news.europawire.eu

Sztuka maskowania, czyli jak hakerzy ukrywają malware - wybrane przykłady

Powszechnie wiadomo, że hakerzy stosują przeróżne techniki w zakresie ukrywania złośliwego oprogramowania, aby uniknąć wykrycia. Stale zmieniający się krajobraz cyberbezpieczeństwa, a co za tym idzie, dostępne technologie (np. te wykorzystujące rozwiązania AI), wymagają, aby również cyberprzestępcy ewoluowali swoje strategie ataków.

Przykładowo możemy wyróżnić kilka metod wykorzystywanych, aby 'zaciemnić' złośliwy ładunek, celem uniknięcia wykrycia:

Źródło: portswigger.net

Dzielenie plików (tzw. 'file splitting') – fragmentacja bądź dzielenie plików, polega na podziale plików na wiele mniejszych części, które są umieszczane w różnych plikach lub lokalizacjach ukrytych w systemie operacyjnym. W kolejnej fazie przeprowadzany jest ponowny „montaż", gdy przykładowo skrypt ponownie łączy fragmenty w kompletny plik wykonywalny. Biorąc pod uwagę sposób działania programów filtrujących/antywirusów, które ostrzegają użytkowników, którzy próbują pobrać i zainstalować pliki wykonywalne jako potencjalnie złośliwe – ta metoda jest w stanie je ominąć. Atakujący są w stanie uniknąć wykrycia i zmniejszyć możliwość wzbudzenia podejrzeń.

Steganografia najmniej znaczących bitów ('least significant bit steganography') – inną metodą ukrywania jest steganografia LSB, która polega na ukrywaniu złośliwego kodu lub danych w pikselach obrazu. Polega ona na konwersji złośliwego kodu do formatu binarnego. Dane binarne są osadzane w najmniej znaczących bitach wartości pikseli (*„każdy piksel obrazu składa się z trzech bajtów dla każdego koloru. Jeśli wartość piksela dla koloru czerwonego wynosi 11001011, atakujący może go zmodyfikować, aby osadzić 1 bit całego złośliwego kodu. Cały proces zostanie powtórzony, aby pomieścić każdy bit złośliwego kodu"*). Obraz będzie sprawiał wrażenie normalnego pliku bez widocznych zmian. Aby wyodrębnić złośliwy kod, proces jest odwracany w celu ponownego złożenia złośliwych danych binarnych z najmniej znaczących bitów zawartych w obrazie.

Droppery – to wieloetapowy system dostarczania złośliwego oprogramowania, który oczekuje na instrukcje od atakującego w celu pobrania i wdrożenia w systemie ofiary. Droppery są często maskowane jako legalne programy, często stanowiące element pakietu innego oprogramowania (skompresowany w archiwum instalacyjnym). Może również stanowić załącznik do wiadomości e-mail w kampanii phishingowej. Bardzo często złośliwe oprogramowanie zostało zaprojektowane z wieloma warstwami unikania i zaciemniania, aby uniknąć wykrycia i usunięcia (lub zostać usunięte samoczynnie po wykonaniu zadania).

Stale aktualizowany program antywirusowy, włączone filtrowanie plików i aktywna zapora sieciowa mogą w większości przypadków zapewnić odpowiednią ochronę przed atakami, zwłaszcza w połączeniu z tzw. 'security awareness', czyli dodatkową weryfikacją przez użytkownika zanim podejmie jakąkolwiek reakcję na otrzymaną zawartość.

Źródła: medium.com, cybernews.com

Wykorzystanie publicznie dostępnych ChatówAI do złośliwej aktywności w cyberprzestrzeni

Obserwacja sfery cyfrowej potwierdza nieprzemijalną prawdę zawartą w powiedzeniu, iż każdy medal ma dwie strony. Wraz z rozwojem możliwości, wzrostem jakości wyników oraz zwiększającą się dostępnością rozwiązań cyfrowych opartych o algorytmy generatywnej sztucznej inteligencji czy LLM, rośnie nie tylko stopień automatyzacji przetwarzania danych i informacji wspierających dobrostan społeczeństw, ale wzrasta również zakres jej użycia przez przestępców, organizacje mafijne i grupy APT powiązane ze służbami specjalnymi różnych państw.

Zrzut ekranu wideo z serwisu TikTok. Ustalono, że do utworzenia wykorzystano technologię deepfake. Źródło: dfrlab.org

Liczba sposobów wykorzystania popularnych Chatów w szkodliwej działalności internetowej, jednostajnie podąża, za co raz to nowymi i bardziej zaawansowanymi możliwościami przez nie oferowanymi. **Wymienić tu można, co najmniej kilka rosnących w popularności ataków opartych o AI, jak automatyzacja pisania złośliwego kodu, czy skokowy, jakościowy wzrost socjotechniki wykorzystywanej w *phishingu*, czy „ożywienie" działalności kont-botów, poprzez umożliwienie nawiązania z nimi interakcji głosowej, tekstowej oraz wizualnej (*deepfake*).** Ponadto stosuje się również specyficzne pozycjonowanie fałszywych materiałów informacyjnych w przeglądarkach internetowych, tak aby możliwie efektywnie nadużywać algorytmy indeksowania chatów, celem zatruwania ich modeli szkodliwymi informacjami. Te ostatnie metody wykorzystywane są przy prowadzeniu kampanii informacyjnych, czy tzw. fraudów finansowych wobec osób indywidualnych, podmiotów biznesowych lub publicznych.

Na przestrzeni ostatniego miesiąca w branżowych mediach pojawiło się kilka głośnych przypadków obrazujących wykorzystanie omawianej technologii w złośliwej działalności hackerów. Portal *SecurityIntelligence.com* informuje o wynikach badań nad efektywnością *ChatGPT4* w wykorzystaniu podatności typu *one-day* (1-dzień od publikacji). Chat był w stanie wykorzystać w sposób zaawansowany 87% zgłoszonych CVE, co jest wynikiem dalece przekraczającym percepcyjne możliwości dużej części wysokiej klasy badaczy bezpieczeństwa.

Natomiast firma *Axios* w raporcie *NewsGuard* informuje, iż czołowe chatboty AI, jak *ChatGPT-4*, *Mistral*, *Gemini* i inne, powtarzają rosyjską dezinformację. W przeprowadzonym badaniu stwierdzono, że chatboty rozpowszechniały rosyjską dezinformację w 32% przypadków. Cytowały one fałszywe i propagandowe strony internetowe, jako wiarygodne źródło informacyjne oraz powoływały się na „specjalistyczne" raporty o wysokiej stronniczości i niskiej jakości badawczej.

Należy również pamiętać, że legalnie działające przedsiębiorstwa starają się utrzymywać swoje modele AI w ryzach, poprzez stosowanie swoistych bezpieczników kształtujących naukę modeli w ogólnie przyjętych normach prawnych, społecznych i moralnych, co ma wpływ na wytwarzane przez AI wyniki. Przestępcy natomiast, często starają się wykraść z podmiotów je tworzących gotowe, efektywne modele AI, i kształtować na własną modłę. Co następnie pozwala profilować je do uzyskiwania wsparcia w prowadzeniu wysoce specjalistycznych metod złośliwej aktywności w przestrzeni cyfrowej.

Źródła: securityintelligence.com, axios.com, dfrlab.org

Próby rosyjskich i irańskich oddziaływań na nastroje społeczne przed francuskimi wyborami parlamentarnymi

W ostatnich tygodniach w mediach zachodnioeuropejskich tematem przewodnim była kampania wyborcza do francuskiego parlamentu – Zgromadzenia Narodowego. Abstrahując od sympatii politycznych, i z czysto badawczej perspektywy, należy stwierdzić iż omawiany okres cechował się zaognioną, nie tylko lokalnie walką informacyjną sympatyków ugrupowań politycznych o efektach wysoce polaryzacyjnych dla francuskiej społeczności. Powyższe uzyskuje potwierdzenie w osiągniętych wysokich wynikach wyborczych ugrupowań dotychczas uważanych za skrajne i radykalne, zarówno po lewej, jak i prawej stronie francuskiej sceny politycznej - dystansując jednocześnie partie z okolic centrum politycznego kompasu, stanowiących zwykle główne siły parlamentarne.

Wybory we Francji.
Źródło: obraz wygenerowany przez copilot.microsoft.com

Oczywiście ocena wyników wyborczych pozostaje w kompetencjach politologów i innych badaczy nauk społecznych. Natomiast na podstawie doświadczeń historycznych i obserwacji światowych kampanii wyborczych ostatniej dekady można stwierdzić zaangażowanie w podsycenie najbardziej skrajnych zachowań (obu stron politycznej barykady jednocześnie) przez służby specjalne związane z rządami poszczególnych państw. Wzorcowym przykładem takiego zaangażowania są ujawnione kampanie wywierania wpływu na opinię publiczną w mediach społecznościowych przez rosyjskie służby m.in. przy wyborach w USA w roku 2016 i 2020, w brytyjskim referendum dot. *Brexitu* czy głosowaniu w sprawie autonomicznego statusu hiszpańskiej Katalonii.

Jak donosi *Insikt Group Recorded Future* obecnie dostrzegalne są operacje wpływu grup wiązanych z Rosją i Iranem, mających za zadnie kształtowanie opinii publicznej oraz zachowania wyborców. Choć dzięki podjętym przeciwdziałaniom ich wpływ pozostaje minimalny to można zauważyć „modernizacje" podejścia ujawnionego w kampaniach „*Doppelgänger*" (podszywanie się pod serwisy informacyjne) oraz „*CopyCopy*" (kampania polityczna oparta o fałszywe strony internetowe i przy wykorzystaniu treści generowanych przez AI). Ponadto, o czym informują francuskie media, krajowe służby są świadome ww. zagrożeń. Obserwowany jest stały wzrost kanałów informacyjnych i sieć kont-botów, mogących być użytych w rozbudowanej kampanii dezinformacyjnej. Póki co - w użyciu o ograniczonej intensywności. Szczytowa intensyfikacja działań prawdopodobnie nastąpi w trakcie zbliżających się igrzysk olimpijskich w Paryżu, i będzie wykorzystywać utworzoną infrastrukturę techniczną (zautomatyzowane konta botnetowe w sieciach społecznościowych, fałszywe strony internetowe, deepfake) celem propagacji szkodliwych informacji i dyskredytacji nowo wybranego francuskiego rządu w czasie, gdy wszystkie oczy świata będą zwrócone ku Paryżowi.

Źródła: recordedfuture.com, abc.net.au

Chmura niejawna na potrzeby cyberbezpieczeństwa państwa

W ostatnim czasie Australia ogłosiła, że przy współpracy z firmą AWS zbuduje niejawną chmurę do poziomu ściśle tajne na potrzeby wojskowe i bezpieczeństwa państwa. Po stronie rządowej za przedsięwzięcie odpowiada australijska agencja wywiadu sygnałowego ASD. Koszt projektu to 1,35 mld USD w ciągu 10 lat. Chmura umożliwi nie tylko bezpieczne przechowywanie najbardziej wrażliwych informacji, ale także ich udostępnianie i analizowanie, w tym przy wykorzystaniu AI i uczenia maszynowego. Rozwiązanie to ma być w pełni suwerenne, ale jednocześnie ma być interoperacyjne z amerykańską niejawną chmurą.

Logo ASD i AWS

Firma AWS odmówiła dziennikarzom odpowiedzi w jaki sposób ma być zapewnione suwerenne panowanie nad chmurą i odesłała do australijskiego rządu. Istotne w tym aspekcie jest m.in to, gdzie będzie zlokalizowana chmura i kto będzie właścicielem infrastruktury. Rząd Australii – podobnie jak wiele innych – wahał się między entuzjazmem dla chmury, a ostrożnością, ponieważ pojawiają się obawy dotyczące bezpieczeństwa. Dlatego oprócz tego agencje rządowe budują własne lokalne chmury (czasami na platformach *open source*) – aby dysponować kodem i należycie dbać o bezpieczeństwo.

Swoje chmury niejawne budują także inne państwa, np. USA i Wielka Brytania, gdzie wykonawcą również jest AWS, co właśnie umożliwia zachowanie interoperacyjność, co jest szczególnie ważne wśród sojuszników (jak Sojusz Pięciorga Oczu).

Oprócz AWS rozwiązanie z zakresu niejawnej chmury obliczeniowej oferują takie firmy jak Microsoft czy Oracle. Chmura niejawna dynamicznie jest rozwijana w USA. Departament Obrony w tym marcu br. poinformował, że podpisał już 47 (ze 100 planowanych) kontraktów na usługi chmurowe w sektorze obronnym w ramach inicjatywy Joint Warfighting Cloud Capability (JWCC). Pentagon w grudniu 2022 r. zwrócił się do Amazona, Google'a, Microsoftu i Oracle o dostarczenie usług cyfrowych dla JWCC, następcy nieudanego przedsięwzięcia pn. Joint Enterprise Defense Infrastructure (JEDI). JWCC jest wyceniane na 9 mld USD w ciągu kilku lat. Cztery firmy rywalizują o każde zamówienie, a każda z nich ma zagwarantowane tylko 100 tys. USD. Kontrakt na obsługę chmury jest uważany za podstawę koncepcji "połącz wszystko-wszędzie" o nazwie Combined Joint All-Domain Command and Control (CJADC2). Koncepcja ta zakłada płynne połączenie wojsk i ich baz danych na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej i cyber, w tym w systemach niejawnych. Ma to umożliwić

Siłom Zbrojnym USA dostarczenie właściwych danych właściwym osobom we właściwym czasie oraz bezpieczne i odporne oprogramowanie, kiedy i gdzie go potrzebują.

Również Polska planuje rozwój chmury na potrzeby administracji państwowej, w tym uwaga jest zwracana również na chmurę niejawną, w celu zwiększenia odporności systemów informacyjnych oraz rozwoju cyfrowego administracji publicznej. Dotychczas obowiązująca uchwała Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", regulująca korzystanie przez podmioty administracji rządowej z usług przetwarzania w chmurze obliczeniowej, zostanie zmieniona w taki sposób, aby jak najwięcej podmiotów mogło korzystać z usług przetwarzania w Publicznej Chmurze Obliczeniowej. Jest to niezwykle istotne z punktu widzenia bezpieczeństwa państwa, bezpieczeństwa danych i budowania państwa opartego na podejściu *Cloud First*.

Wykorzystany model przetwarzania w chmurze może znacznie pomóc urzędom zmagającym się z potrzebą szybkiego dostarczania wysoce niezawodnych, innowacyjnych usług przy wykorzystaniu posiadanych zasobów oraz współpracy z sektorem prywatnym. W Programie WIIP dokonywane będą niezbędne zmiany zwiększające poziom cyberbezpieczeństwa oraz dostosowujące do nowych rozwiązań technologicznych, w tym szerszej możliwości wykorzystania rozwiązań chmurowych. Co więcej, doświadczenie z wojny Rosji z Ukrainą, pokazuje jak ważna dla bezpieczeństwa państwa jest możliwość ewentualnej migracji danych na terytorium państw sojuszniczych w przypadku wystąpienia żywotnego zagrożenia bezpieczeństwa państwa lub wojny.

W kwestii chmury niejawnej należy podkreślić, że może pozwolić to na zwiększenie bezpieczeństwa danych, oszczędności finansowych, upowszechnienie niejawnych systemów teleinformatycznych w administracji publicznej, jak również, że będą one wprowadzane i użytkowane w sposób bardziej przyjazny dla organizatorów i użytkowników oraz należycie „widzący się".

Krytycznym aspektem jest wspomniana suwerenność, czyli panowanie kraju nad danymi i infrastrukturą. Kwestią wymagającą odpowiedzi będzie określenie, czy państwo może sobie to odpowiednio zagwarantować bazując na rozwiązaniach dostarczanych przez Big Techy kontrolowane przez inne państwa bądź podmioty z innych państw, czy też należałoby rozwijać własne technologie i infrastrukturę.

Źródła: theregister.com, c4isrnet.com,

Znaczenie hackathonów w rozwoju cyberzdolności

Jak podpowiada Wikipedia hackathon to wydarzenie skierowane do programistów, podczas którego informatycy i inne osoby związane z rozwojem oprogramowania, takie jak projektanci grafiki, twórcy interfejsów i menedżerowie projektów, stają przed zadaniem rozwiązania określonego problemu związanego z projektowaniem. Tylko część z nich jest związana z – jak sugeruje nazwa – hakowaniem, czy szerzej rozumianym cyberbezpieczeństwem. Ale to właśnie na hackathonach w dziedzinie bezpieczeństwa i obronności skupimy się w tym tekście, gdyż w ich ramach często opracowywane są innowacyjne rozwiązania, które na nowy sposób pomagają rozwiązać problemy z cyberbezpieczeństwem, łącznością, świadomością sytuacyjną, czy wykrywaniem dezinformacji i operacji informacyjnych. Aby jak najlepiej wykorzystać potencjał innowatorów i ich pomysły niezwykle ważna jest współpraca i mentoring ze strony instytucji odpowiedzialnych za bezpieczeństwo państwa. Udział przedstawicieli tych podmiotów pozwoli efektywnie wdrożyć operacyjnie wyniki projektów.

Logo EUDIS

Nowymi mechanizmami innowacji w sektorze bezpieczeństwa i obronności są Unijny System Innowacji Obronnych (*EU Defence Innovation Scheme*, EUDIS) oraz NATO-wski Akcelerator Innowacji Obronnych (*Defence Innovation Accelerator for the North Atlantic*, DIANA). Mają one na celu adaptację nowych i przełomowych technologii (*Emerging and Disruptive Technologies*, EDT) opracowanych w sektorze cywilnym do zastosowań wojskowych. Należy dodać, że obecnie postęp w technologiach cywilnych jest znacznie szybszy niż w domenie militarnej (np. w zakresie AI, IoT, 5G, autonomii pojazdów), a więc wojsko dopiero stara się na swoje potrzeby dostosować innowacyjne technologie „z cywila". Wynika to między innymi z nakładów na B+R przez prywatne firmy, dużą rolę Big Techów oraz innowacje wprowadzane przez startupy.

Oprócz takich działań jak tworzenie ośrodków akceleracyjnych i centrów testowych, współpraca z parkami naukowo-technologicznym, organizowanie wyzwań technologicznych i różnego rodzaju konkursów, kluczowym elementem EUDIS i DIANA są także hackathony.

Na przełomie maja i czerwca br. w Krakowskim Parku Technologiczny zorganizowany został hackathon „Digtial in Defence" w ramach EUDIS (Park ten wraz AGH tworzy też polski ośrodek akceleratora w ramach DIANA). W tym samym czasie hackathony z innym motywem przewodnim odbyły się w 5 innych lokalizacjach w Europie. Podejmowano tam problemy związane z dronami latającymi i pływającymi, sztuczną inteligencją, zabezpieczaniem granic, bezpieczeństwem Bałtyku oraz bezpieczeństwem w sieci. Była to druga edycja tego hackathonu, w ub.r. jego polska część odbyła się w Gdańsku i skoncentrowana była na technologiach kosmicznych do zabezpieczenia morskiej infrastruktury krytycznej.

W tym roku w polskiej edycji hackathonu wygrał projekt AquaHub dotyczący uniwersalnych stacji dokowania i ładowania dla autonomicznych pojazdów morskich (nawodnych i podwodnych). Zespół AquaHub zaprojektował swoje rozwiązanie w 48h. Pełny model 3D, obliczenia CFD oraz aktywne korzystanie z mentoringu przesądziło o zwycięstwie.

Praca wre w trakcie hackathonu.
Źródło: Krakowski Park Technologiczny

Wyróżnione także trzy inne projekty:

- Infofortress – walka z dezinformacją poprzez wykrywanie farm botów.
- Ucho Napoleona - system wspierający zarządzenie polem walki (BMS) oparty o analizę głosu przekazywanych meldunków.
- Termoblend – specjalne kamery oparte o analizę obrazu z kamer RGB i FLIR w celu szybszego wykrywania obiektów i osób.

Wydarzenie było wspierane przez PFR S.A., PGZ Stocznia Wojenna, WB GROUP, ComCERT SA, AGH, MON, DKWOC i WOT.

Źródła: Krakowski Park Technologiczny, PFR S.A., AGH.

Rozbita grupa oszustów, handlująca nieistniejącymi autami

Funkcjonariusze Zarządu w Katowicach Centralnego Biura Zwalczania Cyberprzestępczości przy wsparciu kontrterrorystów z Centralnego Pododdziału Kontrterrorystycznego Policji „BOA", zatrzymali 10 osób, które podejrzane są m.in. o udział w zorganizowanej grupie przestępczej, oszustwa i wyłudzenia mienia, a także pranie pieniędzy pochodzących z przestępstwa. Postępowanie nadzorowane jest przez Prokuraturę Okręgową w Gliwicach. Decyzją sądu 8 podejrzanych zostało tymczasowo aresztowanych.

Sprawcy na jednym ze znanych portali ogłoszeniowych w Internecie oferowali na sprzedaż samochody osobowe oraz ciężarowe.

Oszuści kontaktowali się z pokrzywdzonymi za pomocą Internetu używając technik anonimizacji. Po otrzymaniu zaliczki w wysokości 30 – 40 % wartości pojazdu sprawcy deklarowali, że zamówione przez kupujących samochody dostarczą pod wskazany adres w terminie od 30 do 60 dni, jednakże do ich dostarczenia nigdy nie dochodziło. Pieniądze wpłacone oszustom były transferowane przelewami na inne rachunki, portfele kantorów internetowych i zamieniane na kryptowaluty. Na ten moment ustalono, że sprawcy dokonali oszustw na ponad milion złotych.

Na polecenie prokuratora z Prokuratury Okręgowej w Gliwicach, funkcjonariusze Zarządu w Katowicach Centralnego Biura Zwalczania Cyberprzestępczości przy wsparciu kontrterrorystów z Centralnego Pododdziału Kontrterrorystycznego Policji „BOA", dokonali zatrzymania najpierw 7 osób, następnie kolejnych trzech osób. Wszyscy podejrzewani są o udział w opisywanym procederze. Zatrzymania miały miejsce na terenie województwa lubuskiego, małopolskiego, mazowieckiego oraz śląskiego. Poszczególne osoby podejrzane usłyszały od 10 do 47 zarzutów co w sumie dało 293 zarzutów karnych dotyczących oszustw, udziału w zorganizowanej grupie przestępczej, prania pieniędzy, a także wyłudzenia mienia. Wobec ośmiu z zatrzymanych osób na wniosek prokuratora sąd zastosował środek zapobiegawczy w postaci tymczasowego aresztowania.

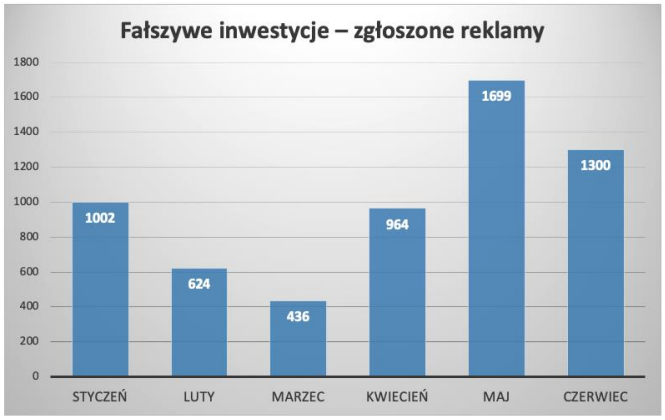
Co warte podkreślenia jednym z zatrzymanych mężczyzn jest podejrzany o pomocnictwo w pobiciu wiceszefa Komisji Nadzoru Finansowego, do którego doszło w 2014 roku. W trakcie czynności procesowych zabezpieczono gotówkę, telefony komórkowe, tablety, komputery oraz inne dowody, które są teraz poddawane dalszej, szczegółowej analizie przez śledczych.

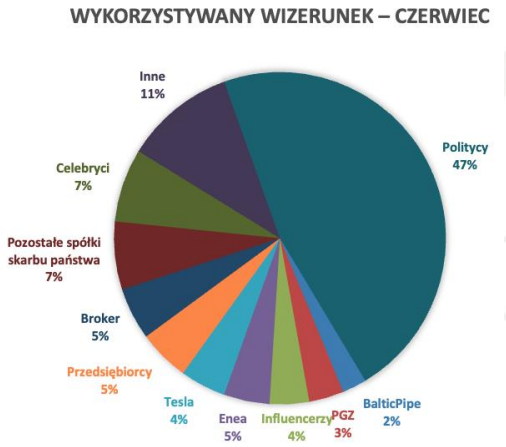
W wyniku działań policjantów CBZC z Katowic i współpracy z Prokuraturą Okręgową w Gliwicach na jednej z platform internetowych oferującej wielowalutowe usługi finansowe, zablokowano środki na kwotę 750 tys. zł. a także zajęto mienie podejrzanych na sumę niemal 650 tys. zł.

Więcej informacji: https://cbzc.policja.gov.pl/bzc/aktualnosci/360,Rozbita-grupa-oszustow-handlujaca-nieistniejacymi-autami.html

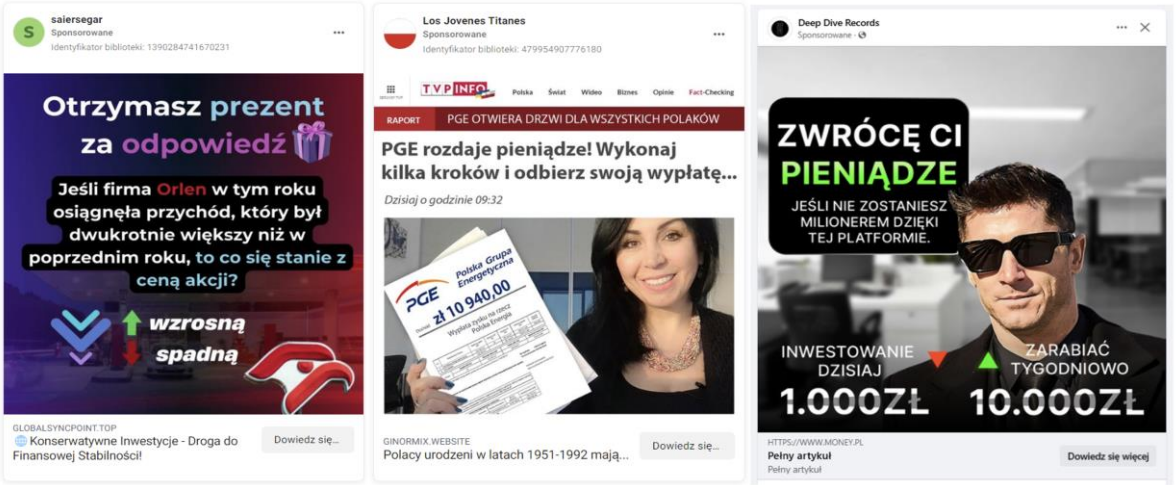
Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – ochrona klienta

W czerwcu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 7 772 domen, które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe, etc.), **dla porównania CERT Polska dodał na listę ostrzeżeń 9 740 domen. Na koniec omawianego miesiąca, na liście znajdowało się 217 309 domen.** W związku ze znaczącą liczbą fałszywych reklam publikowanych na platformie Facebook promujących rzekomą możliwość inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków, CSIRT KNF wypracował mechanizmy wykrywające takie działanie przestępcze oraz procesy przekazywania fałszywych reklam do blokady. Poniższy wykres przedstawia wykryte i zgłoszone do blokady reklamy fałszywych inwestycji na portalu społecznościowym Facebook, w podziale na kategorie wykorzystywanego wizerunku.





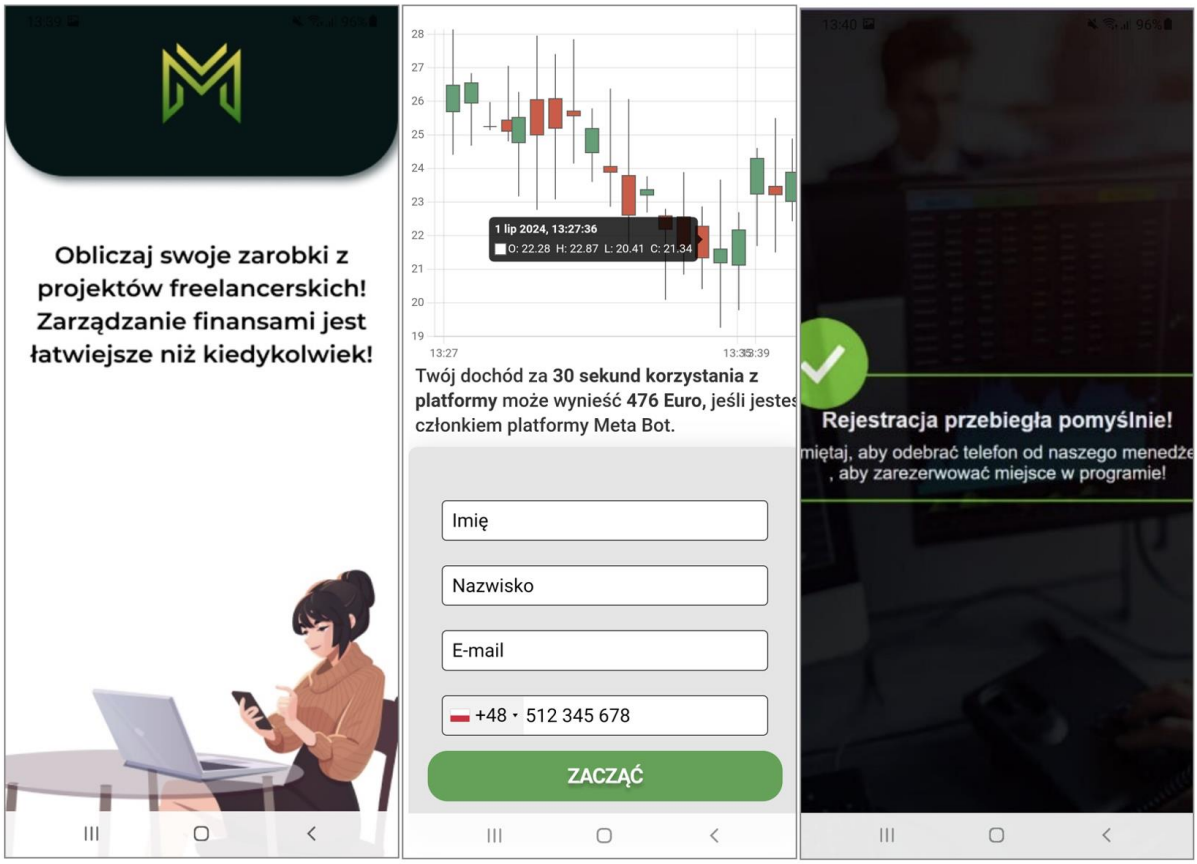
Dodatkowo, w czerwcu 2024 roku analitycy CSIRT KNF zgłosili również do blokady 366 fałszywych profili (359 w maju 2024), które publikowały fałszywe reklamy inwestycyjne.



Fałszywe reklamy inwestycyjne

W minionym miesiącu, wykryliśmy i przeanalizowaliśmy również aplikację o nazwie **Mastcalanc**. Dystrybuowano ją z wykorzystaniem reklamy na platformie Facebook.

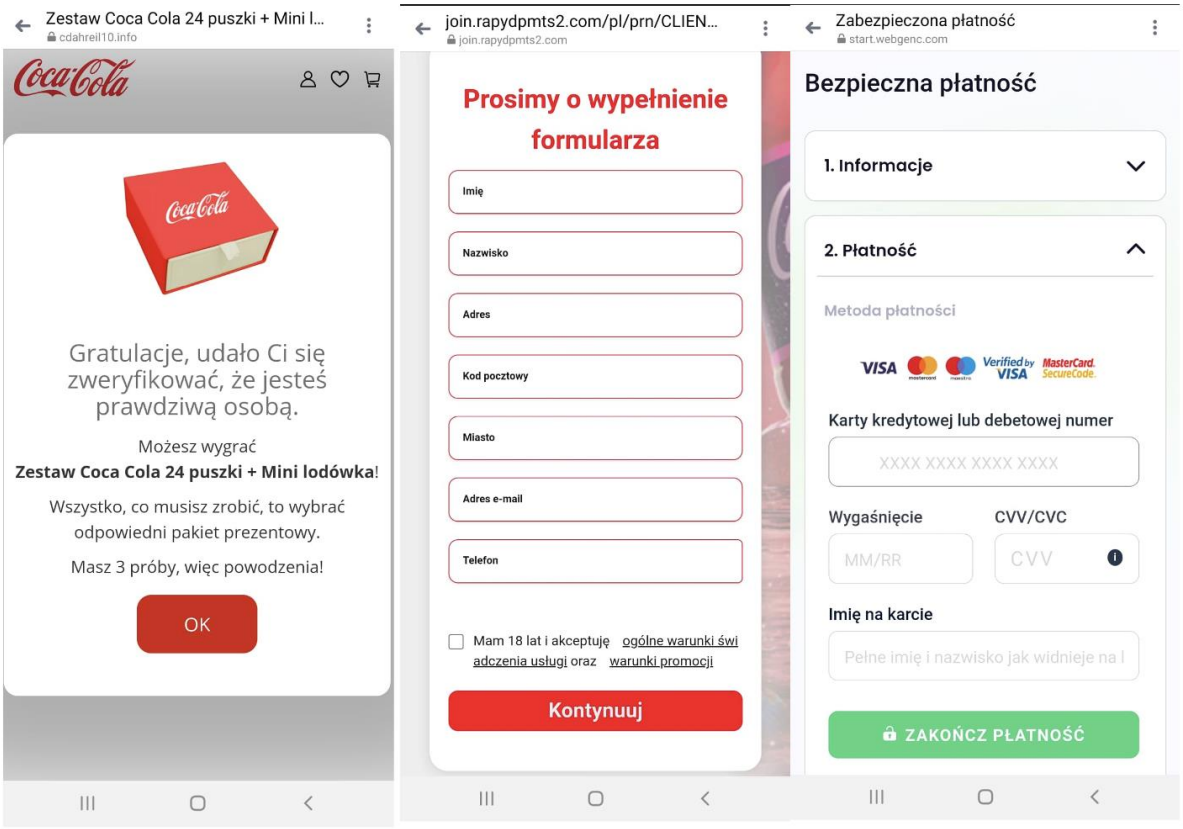
Zauważalny był schemat typowy dla oszukańczych aplikacji inwestycyjnych – błędy językowe, obietnica zysku, próba pozyskania danych (widoczne poniżej). **Aplikacja nie infekowała urządzeń, lecz zbierała dane kontaktowe. W konsekwencji jej użycia, z ofiarą kontaktowali się przestępcy.**



Oszukańcza aplikacja inwestycyjna – widok stron

Podobnie jak w poprzednich miesiącach, również w czerwcu 2024 atakujący podszywali się pod wizerunki polskich banków. Strony phishingowe dystrybuowali m.in. za pośrednictwem reklamy na platformach społecznościowych oraz poprzez wiadomości e-mail. Stosując znane mechanizmy manipulacyjne zachęcali do kliknięcia w link, rzekomą możliwością odebrania nagrody lub zastraszali groźbą zablokowania bankowości elektronicznej. Tym sposobem starali się wyłudzać dane uwierzytelniające do bankowości elektronicznej. Podobnie jak w maju 2024 roku, również w czerwcu cyberprzestępcy przygotowali kampanie phishingowe wyłudzające dane kart płatniczych, aby następnie próbować wyprowadzać środki poprzez „model subskrypcyjny". **Tym razem w publikowanych przez nich reklamach na platformie Facebook nie tylko zachęcali do rzekomego kupienia przedmiotów za 9zł, ale również podszywali się pod wizerunek Coca-Cola, oferując dużą zniżkę na pakiet puszek napoju oraz dedykowaną lodówkę. Stosunkowo innowacyjną kampanią, z jaką mieliśmy do czynienia w ostatnich tygodniach było podszycie pod Orange. Cyberprzestępcy przygotowali stronę, za pośrednictwem której można było rzekomo doładować telefon na kartę, otrzymując wybrane bonusy. W rzeczywistości była to strona phishingowa wyłudzająca dane kart płatniczych.** 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.



Podszycie pod Coca-Cola

Tak jak zaznaczamy co miesiąc, jedną z metod ochrony przed wymienionymi wyżej i innymi działaniami cyberprzestępców jest wiedza. Dlatego **zachęcamy do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook**. Dodatkowo, w ramach cyklu **#TwojeCyberbezpieczeństwo** opublikowaliśmy kolejny schemat oszustwa. Tym razem omawiamy scenariusz znany pod nazwą „**na zgubiony telefon**”. Polega on na tym, że oszuści podszywając się pod członków rodziny przesyłają wiadomości SMS, prosząc o kontakt poprzez WhatsApp. W treści wiadomości zawarty jest link prowadzący bezpośrednio do rozmowy na komunikatorze. Atakujący informują o rzekomym uszkodzeniu telefonu i proszą o przelanie kwoty na wskazany przez nich rachunek bankowy.

Opracowanie dostępne jest pod adresem: *https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/phishing-na-zgubiony-telefon*

Zachęcamy do zapoznania się z nim i pokazania go bliski oraz znajomym. Bądźmy bezpieczni!

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.