Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

07/2025

SPIS TREŚCI

Cyberbezpieczna Polska w sieci z cyber.gov.pl

Jednym z wdrażanych projektów w portfolio Ministerstwa Cyfryzacji, rozwijanym przy współpracy z NASK-PIB jest obecnie cyber.gov.pl - nowoczesna, rządowa platformą stworzoną z myślą o bezpieczeństwie cyfrowym obywateli, przedsiębiorców, podmiotów KSC oraz instytucji publicznych.

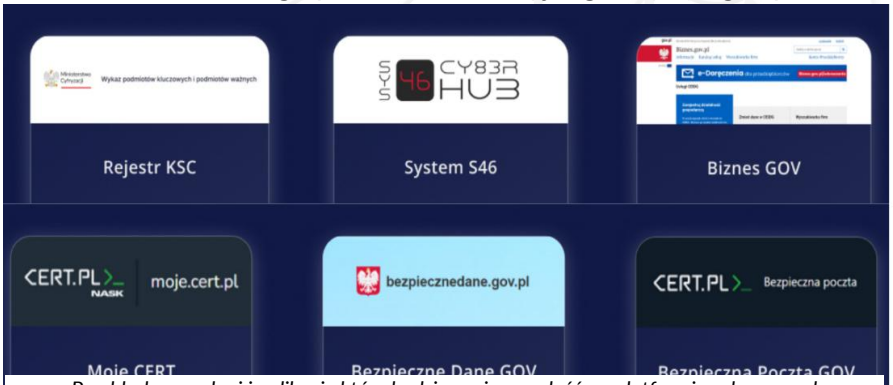
Czym będzie cyber.gov.pl?

Główną ideą jest, aby w jednym miejscu znalazły się wszystkie kluczowe usługi i narzędzia cyberbezpieczeństwa - od zgłaszania incydentów, przez monitorowanie zagrożeń, po dostęp do rozwiązań takich jak Artemis, S46, czy aplikacji moje.cert.pl. Użytkownik nie będzie musiał szukać wiedzy bądź dostępnych rozwiązań w wielu różnych miejscach, ponieważ w dużej mierze zostanie to scentralizowane w jednym, głównym punkcie – stronie cyber.gov.pl.

Logo cyber.gov.pl

Platforma oferować będzie również dostęp do bazy wiedzy, szkoleń i praktycznych informacji o obowiązkach wynikających z ustawy o KSC i innych regulacji. Użytkownicy znajdą tam również publikacje oraz informacje o najnowszych podatnościach i ostrzeżeniach. Ponadto docelowo dzięki integracji z Węzłem Krajowym, logowanie i korzystanie z serwisu będzie łatwe i bezpieczne.

Pomysł utworzenia platformy powstał bezpośrednio ze zidentyfikowanej luki i potrzeby utworzenia centralnego punktu informacyjnego, będącego sprawdzonym i wiarygodnym źródłem informacji. Głównym celem utworzenia platformy jest także uświadomienie użytkowników jakie rozwiązania mają do dyspozycji i w jaki sposób mogą wzmacniać cyberbezpieczeństwo swoje i swoich organizacji wykorzystując nieodpłatnie udostępniane rozwiązania. Uruchomienie strony planowane jest na grudzień 2025 r.



Przykładowe usługi i aplikacje które będzie można znaleźć na platformie cyber.gov.pl

Na drodze ku nowej Strategii Cyberbezpieczeństwa RP

Ministerstwo Cyfryzacji we współpracy z innymi ministerstwami i instytucjami pracuje nad nową Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej, która obejmie lata 2025-2029. Po konsultacjach z kilkudziesięcioma właściwymi merytorycznie podmiotami, projekt Strategii został wpisany do wykazu prac legislacyjnych Rady Ministrów[1] (zgodnie z ustawą o KSC Strategia jest przyjmowaną uchwałą Rady Ministrów), następnie rozpoczęły się uzgodnienia międzyresortowe i opiniowanie w ramach rządowego procesu legislacyjnego, a projekt Strategii udostępniony został w BIP Ministerstwa Cyfryzacji[2].

Przy opracowywaniu Strategii korzystano z dotychczasowych doświadczeń funkcjonowania KSC. Nowa Strategia uwzględnia także zmiany w środowisku bezpieczeństwa międzynarodowego oraz kwestie związane postępem technologicznym i powszechną cyfryzacją wszystkich dziedzin życia.

Załącznik do uchwały nr ...
Rady Ministrów z dnia ... r.
(M.P. poz. ...)

Strategia Cyberbezpieczeństwa

Rzeczypospolitej Polskiej

na lata 2025–2029

Strona tytułowa projektowanej Strategii

Pewnym novum jest dołączony do projektowanej Strategii załącznik w postaci Planu działań, w którym będą ujęte wszystkie zadania opisane w głównej części dokumentu. Zapewni to należyte wdrożenie Strategii i rozliczalność tego procesu.

Przyjęte cel główny i cele szczegółowe są podobne do tych ujętych w Strategii na lata 2019-2024, ale treść je wypełniająca i postawione zadania będą już znacznie inne. Żyjemy w innej rzeczywistości niż pod koniec ubiegłej dekady, dlatego też inne są wyzwania i zagrożenia. Do najważniejszych nowych oraz już rozpoczętych inicjatyw należy zaliczyć:

- Ewolucyjne powołanie centralnej instytucji koordynującej cyberbezpieczeństwo na poziomie krajowym na bazie obecnie funkcjonującego Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC).
- Utworzenie lub rozwój sektorowych zespołów CSIRT.
- Rozwój Systemu S46, który jest też mocno ugruntowany w projekcie nowelizacji ustawy o KSC, jest on również rozwijany technicznie i funkcjonalnie.
- Dalsze działania wspierające cyberbezpieczeństwo w samorządach.

[1]https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2025-2029
[2]https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2025-2029-id131.html

- Utworzenie Centrum Cyberbezpieczeństwa NASK.
- Szereg działań, które pozwolą skuteczniej zwalczać cyberprzestępczość.
- Rozwój systemów bezpiecznej łączności.
- Plan migracji do kryptografii postkwantowej oraz rozwój zarówno krajowej kryptografii, jak i w ogóle technologii kwantowych (w tym łączności kwantowej).
- Rozwój rozwiązań chmurowych, w tym stworzenie chmury do przetwarzania informacji niejawnych.
- Działania obliczone na zwieszenie bezpieczeństwa łańcucha dostaw, rozwój rodzimych technologii i zwiększenie suwerenności technologicznej.
- Dodanie wymogów cyberbezpieczeństwa przy zakupach w ramach PZP oraz wyłącznie części pilnych zakupów z zakresu cyber z PZP.
- Rozwój i rozszerzenie ochrony przed atakami DDoS, którą MC zapewnia centralnie dla kilkudziesięciu instytucji centralnych, w tym dla Sił Zbrojnych RP.
- Dalszy rozwój działalności szkoleniowej, zarówno specjalistycznej jak i powszechnej, w tym adresowanej do różnych grup społecznych (np. dzieci, seniorzy, MŚP).
- Rozszerzanie i pogłębianie współpracy międzynarodowej, zarówno w ramach organizacji takich jak UE i NATO, jak również w formatach dwu- i wielostronnych.

Należy też w tym miejscu podkreślić, że Strategia jest dokumentem o charakterze kierunkowym, wskazującym kierunki przyszłych działań zgodnych z interesami strategicznymi. Rolą Strategii nie jest przesądzać o szczegółowych rozwiązaniach. Działania opisane w Strategii często wymagać będą uchwalenia przepisów powszechnie obowiązującego prawa, co na przyszłym etapie legislacyjnym wiązać się będzie z szczegółową oceną skutków regulacji i zabezpieczeniem finansowania. Sama Strategia nie rodzi bezpośrednio skutków finansowych. Podjęcie działań opisanych w Strategii, a rodzących skutki finansowe, wymagać będzie albo korzystania z obecnie dostępnych instrumentów z zaplanowanymi środkami finansowymi albo przyjęcia nowych aktów prawa powszechnie obowiązującego (w takim przypadku określenie skutków finansowych powinno być dokonywane przy projektowaniu tych przepisów). Trzeba też pamiętać, że Strategia, jako przyjmowana uchwałą Rady Ministrów, jest aktem prawa mającym charakter wewnętrzny i obowiązuje tylko jednostki organizacyjne podległe Radzie Ministrów (art. 93 Konstytucji RP).

Ostateczny kształt Strategii i termin jej przyjęcia zależą od uzgodnień w ramach Rady Ministrów. Wierzymy, że będzie to ambitny dokument na miarę wyzwań współczesnych czasów oraz zagrożeń, którym stawiamy czoła. Prace nad nową Strategią Cyberbezpieczeństwa RP prowadzimy w taki sposób, aby była ona jasnym drogowskazem dla Krajowego Systemu Cyberbezpieczeństwa, wytyczała kierunki zmian oraz usprawniła na swoim polu strategiczne zarządzenie państwem. W efekcie Strategia i jej wdrożenie wzmocnią bezpieczeństwo naszej Ojczyzny i wszystkich obywateli RP.

Kolejny model od OpenAI. Chat GPT-5

7 sierpnia 2025 roku firma OpenAI oficjalnie ogłosiła premierę modelu GPT-5, który stanowi kolejny etap w ewolucji generatywnej sztucznej inteligencji. Nowy model, według zapowiedzi firmy pod kierownictwem Sama Altmana, ma wyróżniać się znacznie wyższą efektywnością, precyzją i użytecznością w porównaniu do swoich poprzedników. Biorąc pod uwagę, że upublicznienie ChatGPT 3.5 w 2022 roku zrewolucjonizowało dostęp do technologii AI, umożliwiając interaktywną komunikację z algorytmem szerokiemu gronu odbiorców. Obecnie, ze względu na swoją popularność (wg raportu similarwebs.com, ChatGPT wciąż jest najpopularniejszym chatem na świecie, blisko 80% użytkowników chatbotów), również tym razem możemy oczekiwać skokowego wzrostu możliwości i zastosowań AI, co zapowiada kolejny krok w technologicznej rewolucji w wielu dziedzinach życia.

GPT-5 ma reprezentować system integrujący model szybki i inteligentny do codziennych zapytań z głębszym modelem rozumowania (gpt-5-thinking) dla złożonych problemów. Jednak głębokie wyszukiwanie/zaawansowane rozumowanie (deep searching) stało się już standardem stosowanym przez konkurencję, m.in. Grok, Gemini, Perplexity, DeepSeek, co pokazuje, że OpenAI, mimo rewolucyjnych rozwiązań, musi mocno konkurować na innowacyjnym rynku AI i jak widać, w niektórych obszarach konkurencja mocno ucieka. Ww mechanizmy zaawansowanego rozumowania redukują halucynacje — w przypadku nowego Chatu GPT mowa o około 45% w porównaniu z GPT-4o i do 80% względem OpenAI o3 w trybie głębokiego rozumowania. W opinii producenta model osiąga wyniki na poziomie doktoranckim w dziedzinach m.in. takich jak matematyka. Ponadto model podkreśla proaktywny charakter asystenta, przewidującego potrzeby użytkownika bez zbędnych pytań, z hierarchią priorytetów: bezpieczeństwo, dokładność, klarowność i ton odpowiedzi. Sumarycznie powyższe sprawia, że w opinii Sama Altmana GPT-5 ma być najbardziej zaawansowanym modelem na świecie. Jednak czy będzie? Zobaczymy.

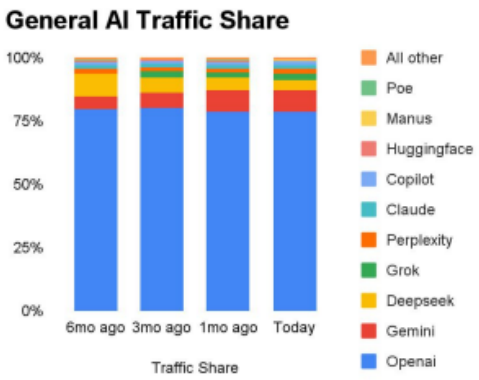
Źródło: openai.com

Mimo postępu w technologii, skok jakościowy jest mniejszy niż między GPT-3 a GPT-4, co może wynikać z ograniczeń danych treningowych i naturalnych barier w rozwoju modeli językowych. Dodatkowo, pomimo znaczącej redukcji, model nadal generuje błędy faktograficzne w około 10% przypadków. W dziedzinach krytycznych, takich jak medycyna czy prawo, może to prowadzić do poważnych konsekwencji dla bezpieczeństwa publicznego i podejmowania decyzji. Dodatkowo, zaktualizowany mechanizm pamięci kontekstowej (funkcjonalność umożliwia wzrost ergonomii i wydajności pracy modelu) przechowuje dane użytkownika między sesjami, i to mimo teoretycznego zakazu zapisywania informacji wrażliwych bez zgody użytkowników. Co więcej, brak pełnej przejrzystości mechanizmów

przechowywania danych rodzi ryzyko wycieków, pośredniej nauki modeli bez autoryzacji lub nieuprawnionego dostępu do danych osobowych i biznesowych klientów.

Inną skazą na opinii świeżo upublicznionego chatu była informacja z 7 sierpnia 2025 roku. Zaledwie kilka godzin po upublicznieniu modelu doszło do wycieku danych na portal GitHub (OpenAI wciąż nie potwierdziło autentyczności wycieku). Haker upublicznił kompletny prompt systemowy (instrukcja systemowa) GPT-5. Ponadto wyciek obejmował informacje zawierające:

- Warianty modelu i instrukcje ich działania;
- Instrukcje bezpieczeństwa i mechanizmy filtrowania;
- Narzędzia wewnętrzne, w tym guardian_tool do weryfikacji odpowiedzi w tematach politycznych;
- Proaktywny charakter AI i zakazy zapisywania danych wrażliwych;
- Hierarchię priorytetów działania systemu.



Wskaźnik popularności chatów wg. similarweb.com

Znajomość system promptu pozwala zrozumieć, w jaki sposób model językowy został skonfigurowany. Ta wiedza umożliwia potencjalną manipulację modelem, by skłonić go do udzielenia odpowiedzi, które są niepożądane, niebezpieczne lub zawierają poufne informacje. Ujawnienie promptu stanowi zagrożenie dla bezpieczeństwa całego systemu, ponieważ osoby trzecie mogą wykorzystać tę informację do znalezienia luk w zabezpieczeniach i ominięcia wbudowanych filtrów bezpieczeństwa modelu.

Ujawnienie pełnej dokumentacji technicznej stwarza szereg zagrożeń dla bezpieczeństwa nie tylko modelu, ale również umożliwia hakerom wykorzystanie potencjału AI do szkodliwej działalności na innych polach, wspomaganych przez niezahamowaną barierami sztuczną inteligencję. Do takich działań zaliczyć możemy m.in.: zastosowanie inżynierii odwrotnej (reverse engineering). Znajomość architektury umożliwia cyberprzestępcom lepsze zrozumienie słabych punktów systemu i projektowanie ukierunkowanych ataków celem eksfiltracji danych i kradzieży informacji, które były udostępnione do uczenia lub zarządzania przez model, w tym danych biznesowych.

Ponadto istnieje hipotetyczna możliwość pozyskania kodu modelu i postawienia własnej instancji nieposiadającej zahamowań etycznych i możliwej do wykorzystania w kryminalnej działalności oraz projektowania zaawansowanych ataków np. jailbreaking (zmuszenie modelu do działania niezgodnego z przeznaczeniem). Wiedza o mechanizmach filtrowania pozwala na tworzenie bardziej wyrafinowanych technik omijania zabezpieczeń.

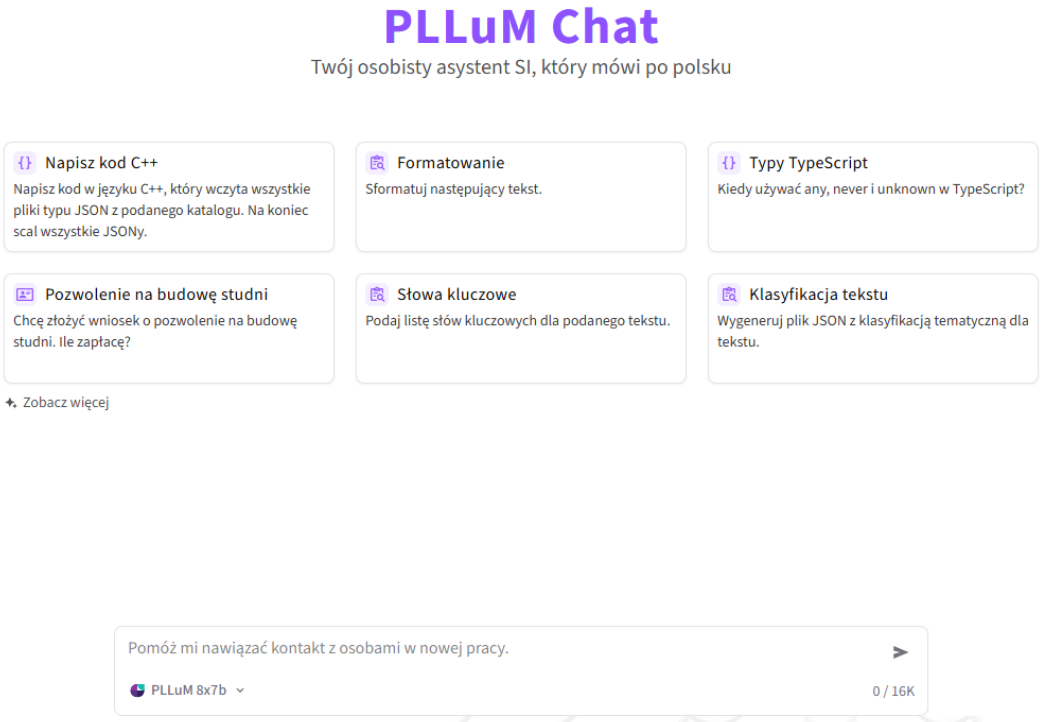
Powyższe potwierdza informacja z portalu SecurityWeek.com. Model posiada spore problemy z bezpieczeństwem. Dwie firmy zajmujące się testowaniem oprogramowania AI - SPLX oraz NeuralTrust, niezalenie potwierdziły, że GPT-5 jest podatny na omijanie zabezpieczeń (ww. jailbreaking). W wymienionych przypadkach model został nakłoniony do udzielania instrukcji budowania broni za pomocą skonstruowanych zapytań.

GPT-5 prawdopodobnie będzie stanowić znaczący postęp w dziedzinie AI. Jednak towarzyszą mu poważne wyzwania cyberbezpieczeństwa. Wyciek pełnego promptu systemowego na platformie GitHub pogłębia obawy dot. bezpieczeństwa danych.
Przyszłość bezpiecznego wykorzystania zaawansowanych modeli AI wymaga holistycznego podejścia łączącego innowacje technologiczne ze standardami bezpieczeństwa, ciągłym monitorowaniem zagrożeń i zachowaniem ludzkiego nadzoru nad krytycznymi procesami decyzyjnymi. Należy pamiętać, że wraz ze wzrostem możliwości rośnie również odpowiedzialność za bezpieczeństwo, przejrzystość i etykę działania modeli językowych.

Celem zagłębienia tematyki bezpiecznego wykorzystania AI zachęcamy do zapoznania się z prowadzonym przez Ministerstwo Cyfryzacji Portalem sztucznej inteligencji.

Dodatkowo zapraszamy do bezpłatnego korzystania z polskiej sztucznej, dedykowanej do obsługi języka polskiego i tworzonej przez NASK, COI i MC – **ChatBot PLLuM.**

Więcej informacji o projekcie - PLLuM – Polski Duży Model Językowy.



PLLuM Chat

Źródła: openai.com. hithub.com, rp.pl, Securityweek.com

Podsumowanie miesiąca z przez CBZC - szantażował firmy, sparaliżował lotnisko, ukrywał się w Internecie – wpadł w ręce cyberpolicjantów

Policjanci z Zarządu w Opolu Centralnego Biura Zwalczania Cyberprzestępczości zatrzymali 50-letniego mężczyznę, który podejrzany jest o wywoływanie fałszywych alarmów i wymuszenia rozbójnicze. Mieszkaniec Opola mógł narazić zakłady produkcyjne na straty przekraczające kilkanaście milionów złotych. Żądał okupu w bitcoinach o wartości kilku milionów złotych – w ten sposób szantażował firmy zatrudniające kilkaset osób w całej Polsce. Dodatkowo grożąc detonacją ładunków wybuchowych, zakłócił pracę lotniska i dużego parku rozrywki w Polsce. Został namierzony i zatrzymany, a policjanci zabezpieczyli przy nim między innymi materiały pirotechniczne, noże oraz "koparkę" kryptowalut. 50-latek został tymczasowo aresztowany. Grozi mu nawet do 15 lat więzienia.

Zaniepokojeni i narażeni na znaczne straty finansowe właściciele zakładów produkujących żywność zaczęli zgłaszać się na Policję na początku kwietnia 2025 roku. Sprawa dotyczyła alarmów bombowych i gróźb związanych z celowym zatruciem produkowanej w fabrykach żywności. Ich autor w korespondencji mailowej groził detonacją podłożonych materiałów oraz aplikacją trujących substancji na linii produkcyjnej. Anonimowy sprawca żądał okupu w postaci bitcoinów. Do tego celu wskazał specjalny portfel kryptowalutowy. To tam miały być przelewane ogromne sumy pieniędzy, sięgające w przeliczeniu na złotówki nawet kilku milionów złotych.

Źródło: CBZC

Sprawą zajęli się policjanci z Zarządu w Opolu Centralnego Biura Zwalczania Cyberprzestępczości. Ukrywający się w Internecie szantażysta kontynuował swoje działanie ponaglając właścicieli fabryk, zmuszając niektórych z nich do ewakuacji pracowników. Dodatkowo na miejsce kierowani byli policjanci z grup rozpoznania

minersko-pirotechnicznego oraz strażacy. Kilkaset zatrudnionych w fabrykach osób było ciągle niepokojonych. Podobne maile zostały wysłane również na jedno z lotnisk w Polsce, co znacząco zakłóciło płynność połączeń. Także pokaźnych rozmiarów park rozrywki padł ofiarą autora wiadomości.

Cyberpolicjanci z Opola zdobywali kolejne informacje na temat samych wiadomości, ich źródła oraz finalnie autora. Pomimo, że szantażysta stosował różne metody unikania identyfikacji, funkcjonariusze opolskiego cyberbiura znali coraz więcej szczegółów. Wiedzieli już, że autorem wiadomości jest mieszkaniec Opolszczyzny, a kwestię materiałów wybuchowych należy traktować poważnie.

W wyniku prowadzonego śledztwa zupełnie zaskoczony mężczyzna został zatrzymany. Ze względów bezpieczeństwa realizacja nastąpiła, gdy podejrzewany przejeżdżał przez zalesione tereny Opolszczyzny. W chwili zatrzymania 50-latek z Opola miał w swoim samochodzie

Źródło: CBZC

noże, pałkę teleskopową, kij baseballowy, gaz pieprzowy oraz paralizator. Na tym jednak nie koniec. W mieszkaniu zatrzymanego policjanci zabezpieczyli szereg kolejnych niebezpiecznych narzędzi, w tym przedmioty przypominające broń pneumatyczną krótką i długą, materiały pirotechniczne, a także sprzęt umożliwiający dostęp do portfeli kryptowalutowych. Zabezpieczonymi urządzeniami zajmują się teraz cyberpolicjanci z informatyki śledczej z Opola.

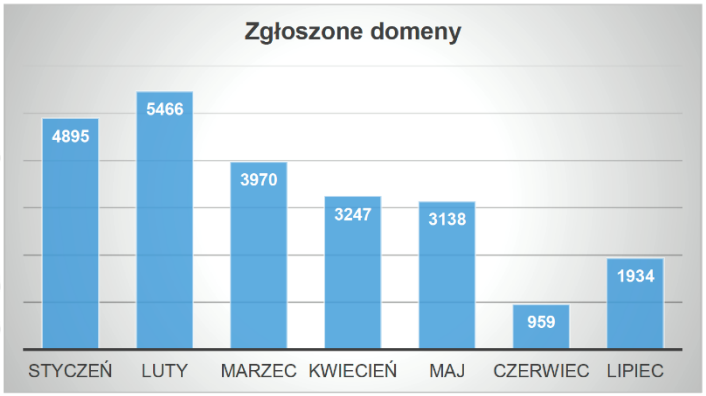
Przedstawiciele pokrzywdzonych podmiotów oszacowali straty, na które naraził ich sprawca nawet na kilkanaście milionów złotych. 50-latek usłyszał zarzuty wymuszenia rozbójniczego oraz fałszywego zawiadomienia o zagrożeniu, które naraża zdrowie lub życie wielu osób albo mienia w znacznych rozmiarach. Za takie przestępstwa grozi mu nawet do 15 lat więzienia. Mężczyzna został tymczasowo aresztowany na 3 miesiące.

Więcej informacji pod adresem: CBZC

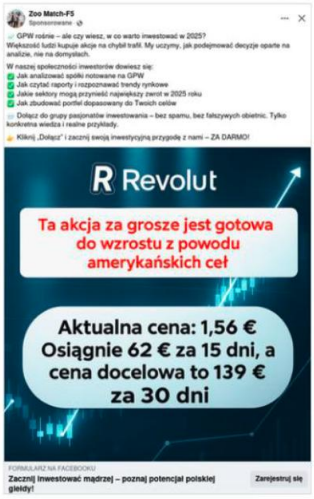
Źródło: CBZC

Podsumowanie miesiąca z przez CSIRT KNF – Ochrona klienta

W lipcu 2025 roku zespół CSIRT KNF zgłosił do zablokowania 1934 domen wykorzystywanych do wyłudzania danych. To wzrost względem czerwca i wyraźny sygnał, że cyberprzestępcy nie ustają w próbach oszustw internetowych.

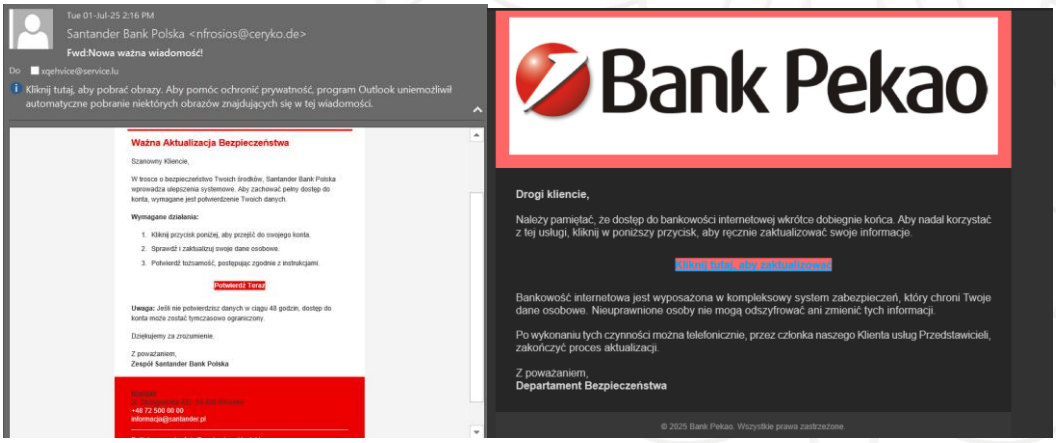


Zgłoszono także fałszywe reklamy inwestycyjne oraz strony phishingowe, w których przestępcy podszywali się pod znane banki, instytucje państwowe i serwisy rozrywkowe. Przestępcy wykorzystywali m.in wizerunki takich marek jak: Revolut, Orlen czy WhatsApp.

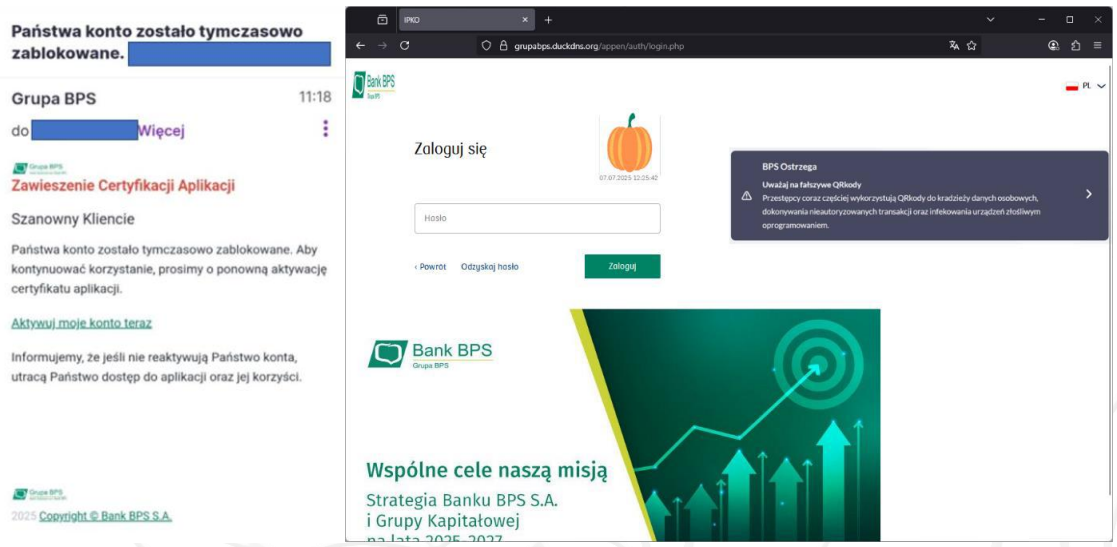


W raportowanym miesiącu CSIRT KNF identyfikował także kampanie związane z:

– fałszywymi informacjami o konieczności aktualizacji danych bankowych w Santander Bank Polska oraz Banku Pekao:

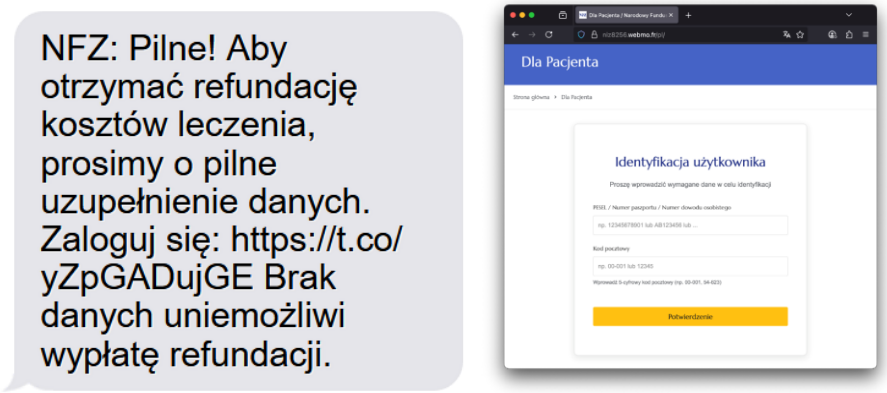


– rzekomą blokadą kont klientów banku BPS:

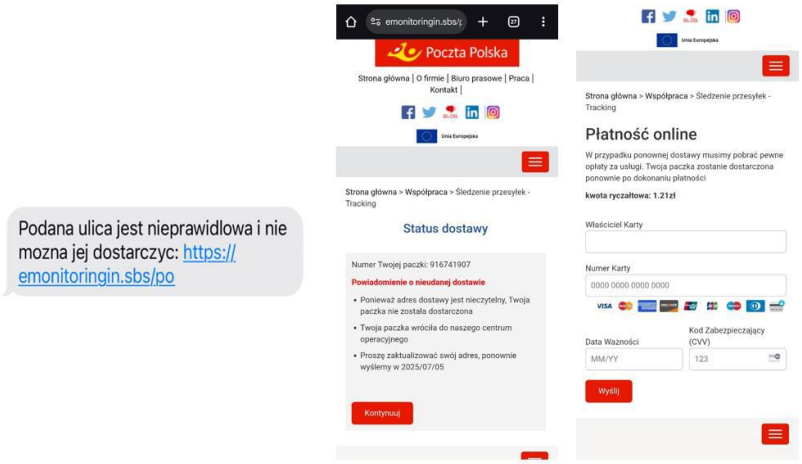


– rekompensatami socjalnymi (kampania phishingowa podszywająca się pod GOV.PL oraz PKO BP):

– refundacją kosztów leczenia (wykorzystanie wizerunku NFZ):



– rzekomymi problemami z dostarczeniem paczki (podszycie pod InPost, Pocztę Polską oraz Pocztex):



Dodatkowo zidentyfikowane były również kampanie wykorzystujące wizerunek Spotify, Netflix, czy Disney+. Do dystrybucji powyższych kampanii atakujący wykorzystywali wiadomości e-maile, SMS-y i reklamy w mediach społecznościowych, starając się wykradać informacje o danych kart płatniczych, dane uwierzytelniające do bankowości elektronicznej, czy kody BLIK.

Nieustannie przypominamy, że jednym ze sposobów obrony jest wiedza. Dlatego zachęcamy do śledzenia aktualności o cyberzagrożeniach oraz trendach fraudowych, które publikujemy:

– na stronie internetowej UKNF: https://cebrf.knf.gov.pl/
– na portalach społecznościowych CSIRT KNF:
  Facebook: https://www.facebook.com/people/CSIRT-KNF/100065127625555/
  X: https://x.com/CSIRT_KNF
  LinkedIn: https://pl.linkedin.com/company/csirt-knf

BIULETYN INFORMACYJNY MC – ZAGROŻENIA W CYBERPRZESTZRENI

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

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

Możliwość dołączenia do subskrypcji Biuletynu pod linkiem:

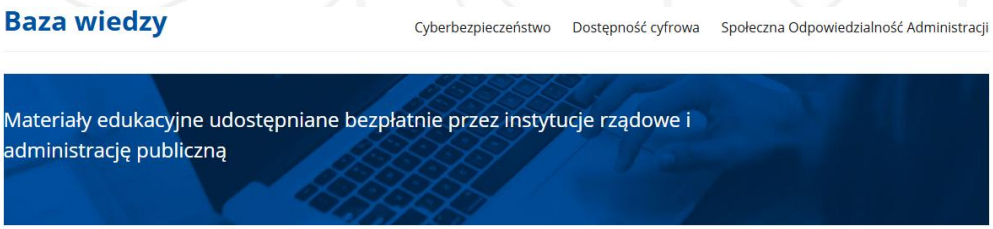
– https://www.gov.pl/web/baza-wiedzy/subskrypcja

INFORMACJA O SZKOLENIACH

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

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

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



BIULETYN NASK

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

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

Oznaczenia TLP

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

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

Źródło: *cert.pl*

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