Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.101.2025
Warszawa, 07 lipca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 13 czerwca br. Posłanki na Sejm RP Pani Wioletty Marii Kulpy w sprawie potencjalnego oszustwa firmy podszywającej się pod PGE (interpelacja nr 10285)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłankę pytania będące we właściwości Ministra Cyfryzacji.

Ad 1) Czy jest Panu znana sytuacja podszywania się oszustów pod państwową firmę PGE?

Minister Cyfryzacji posiada wiedzę na temat licznych przypadków podszywania się cyberprzestępców pod Polską Grupę Energetyczną. W maju br. odnotowano kampanię phishingową fałszywych wiadomości e-mail informującą o nadpłacie, którą klient może uzyskać po zalogowaniu się na fałszywą stronę i podaniu swoich danych. W grudniu 2024 r. miała miejsca kampania fałszywych reklam obiecująca wypłatę dywidendy przez PGE wszystkim obywatelom.

Ponadto CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy regularnie monitoruje kampanie phishingowe, w których oszuści podszywają się pod koncerny paliwowo-energetyczne, takie jak PGE, Orlen, PGNiG, czy Lotos, oferując rzekome inwestycje w akcje, kryptowaluty czy obligacje. Tego rodzaju kampanie prowadzą do utraty środków finansowych, ponieważ wykorzystywane platformy uniemożliwiają późniejszą wypłatę zainwestowanych pieniędzy.

Należy również zwrócić uwagę, że najczęściej występującą kategorią incydentów zarejestrowanych w 2024 r. były oszustwa komputerowe. Zarejestrowano 97 995 tego typu incydentów, co stanowi 95% wszystkich obsłużonych incydentów. W porównaniu z 2023 r. liczba oszustw komputerowych wzrosła o 29%. Skala tego typu incydentów jest znana Ministrowi Cyfryzacji, który odnosił się wielokrotnie do tej kwestii w kontekście rosnącej liczby incydentów.

Ad 2) Jaka w Pana ocenie powinna być nadana szybka ścieżka reakcji podmiotu pod który podszywa się potencjalny oszust?

Niewątpliwie czas, szybkość reakcji na każdy incydent ma ogromne znaczenie ponieważ natychmiastowe wdrożenie odpowiednich narzędzi i procedur wpływa na minimalizację skutków incydentu.

Celem działania każdego podmiotu powinno być szybkie zidentyfikowanie zagrożenia, ograniczenie jego wpływu, przywrócenie normalnego działania oraz zminimalizowanie szkód. Kluczowe etapy powinny obejmować obsługę incydentu (wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu) oraz zarządzanie incydentem, tj. wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

Ad 3) Czy w związku z zapoznaniem się ze sprawą podejmie Pan interwencję zarówno w PGE, jak i w CERT Polska?

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

CERT Polska działający w strukturze Naukowej i Akademickiej Sieć Komputerowej – Państwowego Instytutu Badawczego, będącym instytutem nadzorowanym przez Ministra Cyfryzacji, podlega ciągłemu nadzorowi ze strony Ministra Cyfryzacji. Jednocześnie w zakresie realizacji zadań w obszarze cyberbezpieczeństwa bieżąca współpraca jest koordynowana m.in. z udziałem CERT Polska w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), działającego pod auspicjami Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, którym jest Minister Cyfryzacji.
Odnosząc się do kwestii prośby CERT Polska o przesłanie podejrzanej wiadomości w formacie eml, należy wyjaśnić, że podyktowane było to koniecznością dokładnej analizy technicznej incydentu. Format ten zawiera pełną strukturę wiadomości, w tym nagłówki, oryginalną treść, załączniki, metadane oraz wszelkie użyte linki czy kod HTML. Dzięki temu możliwe jest odtworzenie całego przebiegu ataku, identyfikacja użytych serwerów, domen oraz technik socjotechnicznych, jakimi posłużyli się cyberprzestępcy. Dane te są również niezbędne, aby zablokować złośliwe kampanie i zapobiegać kolejnym atakom. Forma i treść zgłoszenia oraz brak jego uzupełnienia uniemożliwiła CERT Polska podjęcie jakichkolwiek działań w zakresie tego incydentu (np. opublikowanie ostrzeżenia w mediach społecznościowych czy dodanie złośliwej domeny do Listy ostrzeżeń przed niebezpiecznymi stronami prowadzonej przez CERT Polska). W związku z powyższym nie ma podstawy do jakiejkolwiek interwencji w sprawie przedmiotowego zgłoszenia.

Należy również wskazać, że Minister Cyfryzacji nie posiada uprawnień do interwencji w PGE, a trzeba podkreślić, że organy administracji publicznej mogą działać wyłącznie na podstawie i w granicach prawa.

Wyjaśniam jednocześnie, że ustawa o krajowym systemie cyberbezpieczeństwa[1] wskazuje szereg podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, w tym m.in. organy właściwe do spraw cyberbezpieczeństwa wyznaczone dla poszczególnych sektorów (np. energii, transportu, ochrony zdrowia), w których świadczone są usługi mające kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Zgodnie z art. 41 pkt 1 ustawy o ksc organem właściwym do spraw cyberbezpieczeństwa w sektorze energii jest minister właściwy do spraw energii - obecnie Minister Klimatu i Środowiska. Tenże Minister jest również organem nadzoru w zakresie wykonywania przez operatorów usług kluczowych z sektora energii wynikających z ustawy o ksc obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych. Zatem spółka Skarbu Państw, w przypadku gdy jest wyznaczona na operatora usługi kluczowej przez organ właściwy ds. cyberbezpieczeństwa w danym sektorze, podlega nadzorowi przez ten organ w zakresie spełniania wymogów i obowiązków określonych w ustawie o ksc. Dany organ właściwy, jako organ nadzoru, posiada również szereg ustawowych uprawnień w odniesieniu do podmiotów będących operatorami usług kluczowych w danym sektorze np. ma możliwość przeprowadzenia kontroli. Powyższe oznacza, że Minister Cyfryzacji, jako organ właściwy do spraw cyberbezpieczeństwa, w zakresie swojej właściwości może prowadzić szereg działań nadzorczych wyłącznie w odniesieniu do podmiotów z nadzorowanego sektora jakim jest infrastruktura cyfrowa bądź w wobec dostawców usług cyfrowych.

Ad 4) Czy wszystkie spółki szczególnie należące do SP, a wykonujące zadania na rzecz 1. społeczeństwa nie powinny zostać poinstruowane, jak w takich sytuacjach mają działać i podejmować czynności, aby w największym stopniu uchronić swoich klientów przed negatywnymi skutkami działań oszustów?

Minister Cyfryzacji w zakresie swojej właściwości wspiera wiele sektorów, w tym sektor energetyczny we wdrażaniu i prowadzeniu działań związanych z zapewnieniem

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077) (zwana dalej: „ustawą o ksc")

cyberbezpieczeństwa. Z punktu widzenia cyberbezpieczeństwa ważnym elementem jest budowanie świadomości i wiedzy poprzez szkoleniach z zakresu cyberbezpieczeństwa. Bez wątpienia świadomość i wykwalifikowana kadra podmiotów przekłada się na zwiększenie poziomu bezpieczeństwa obywateli.

W kontekście powyższego, z inicjatywy Ministra Cyfryzacji podejmowanych jest szereg działań edukacyjnych (w formule bezpłatnych szkolenia online[2]) kierowanych m.in. do podmiotów krajowego systemu cyberbezpieczeństwa, w tym do spółek Skarbu Państwa.

Celem szkoleń jest, nie tylko zwiększenie świadomości kadr na temat cyberzagrożeń, ale również podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzenia sobie w sytuacjach kryzysowych. Szkolenia prowadzone są przez ekspertów i praktyków na co dzień zajmujących się kwestiami cyberbezpieczeństwa – ekspertów z Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego NASK-PIB oraz przedstawicieli partnerów technologicznych Programu Współpracy w Cyberbezpieczeństwie – PWCyber. Szkolenia realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb, a ich tematyka jest bardzo zróżnicowana. Zostały podzielone na trzy kategorie:

- Szkolenia 100 - cyberhigiena dla każdego,
- Szkolenia 200 - dla kadry zarządzającej, pracowników działów IT,
- Szkolenia 300 - warsztaty dla specjalistów IT, programistów, osób zarządzających cyberbezpieczeństwem w podmiotach krajowego systemu cyberbezpieczeństwa.

Ponadto, bezpieczeństwo polskiej cyberprzestrzeni jest głównym celem działań PCOC, w którym biorą udział instytucje odpowiedzialnego za bezpieczeństwo teleinformatyczne na poziomie krajowym, co umożliwia koordynację działań i sprawne reagowania na zagrożenia. Poza tym, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa wydaje rekomendacje i komunikaty, których zastosowanie przez podmioty krajowego systemu cyberbezpieczeństwa, w tym spółki Skarbu Państwa, pozwala ustrzec się przed cyberatakami i podnieść ich odporność na cyberzagrożeń.

Spółki Skarbu Państwa otrzymują także wsparcie od właściwego zespołu CSRIT poziomu krajowego, gdy zgłoszą do niego incydent.

Ad 5) Czy do ministerstwa dotarły informacje od osób które mogły odpowiedzieć na wspomniany mail potencjalnego oszusta, jeśli tak to jaka jest to skala osób poszkodowanych?

Minister Cyfryzacji nie otrzymał informacji w powyższym zakresie.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[2] Szkolenia realizowane są jako Zebrania (*ang. Town Hall*) na platformie Microsoft Teams z udziałem ekspertów partnerów technologicznych Programu PWCyber oraz NASK-PIB.

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa