Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.13.2025
Warszawa, 17 lutego 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 17 stycznia br. Posła na Sejm RP Pani Pauliny Matysiak w sprawie cyberbezpieczeństwa i bezpieczeństwa transportu kolejowego w kontekście problemów z pociągami Impuls produkowanymi przez firmę Newag SA (interpelacja nr 7396)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie działania podjęto w zakresie cyberbezpieczeństwa, aby wyjaśnić awarie pociągów firmy Newag i zapobiec podobnym incydentom w przyszłości?

Działania podjęte przez Ministerstwo Cyfryzacji oraz z udziałem Ministerstwa Cyfryzacji:

Zespół CSIRT NASK[1], działający na podstawie ustawy o krajowym systemie cyberbezpieczeństwa[2], o sprawie potencjalnych praktyk monopolistycznych firmy NEWAG S.A., został poinformowany przez firmę Serwis Pojazdów Szynowych sp. z o.o. 5 grudnia 2022 r. z prośbą o interwencję w sprawie złożonego dwa miesiące wcześniej zawiadomieniu w UOKiK. Tego samego dnia Zespół CSIRT NASK wysłał zapytanie do UOKiK o poinformowaniu o podjętych krokach i ewentualnym wszczęciu postępowania.

Zespół CSIRT NASK ocenił raporty techniczne zespołu Dragon Sector jako wiarygodne - ich treść była rzeczowa i spójna z przyjętą metodologią zgodną z przyjętymi w branży praktykami z zakresu informatyki śledczej oraz inżynierii wstecznej oprogramowania. Sprawa w ocenie zespołu CSIRT NASK, jako zagrożenie cyberbezpieczeństwa mogła również wypełniać znamiona przestępstwa wymagając podjęcia czynności przez organy ścigania. W związku z tym, w celu przedstawienia wniosków z raportów, zespół CSIRT NASK 20 grudnia 2022 r. spotkał się z funkcjonariuszami Centralnego Biura Antykorupcyjnego, a 20 stycznia 2023 r. w siedzibie NASK zorganizowano spotkanie z funkcjonariuszami Agencji Bezpieczeństwa Wewnętrznego i członkiem zespołu Dragon Sector.

Z kolei 15 maja 2023 r., na wniosek Zespołu CSIRT NASK, zorganizowano w Kancelarii Prezesa Rady Ministrów spotkanie Kolegium ds. Cyberbezpieczeństwa z udziałem przedstawicieli najważniejszych organów odpowiedzialnych za cyberbezpieczeństwo w celu zaprezentowania raportów przez członka zespołu Dragon Sector. Spotkanie miało charakter niejawny.

Na dalszym etapie czynności w tej sprawie prowadziła Agencja Bezpieczeństwa Wewnętrznego, zgodnie z swoimi ustawowymi kompetencjami.

Obecnie postępowanie w sprawie prowadzi Prokuratura Regionalna w Krakowie.

[1] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;
[2] ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm.)

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

ul. Królewska 27
00-060 Warszawa

Działania Ministerstwa Cyfryzacji w celu koordynacji odpowiedzi na zagrożenia cyberbezpieczeństwa o charakterze uniwersalnym, które mogą stanowić także narzędzie przeciwdziałania tego rodzaju zderzeniom:

Ministerstwo Cyfryzacji w procedowanym projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która ma na celu wdrożenie w Polsce m.in. dyrektywy NIS 2, przewiduje także uwzględnienie mechanizmu umożliwiającego wykluczenie dostawców wysokiego ryzyka (HRV), co stanowić będzie implementację Toolbox 5G.

Instytucja dostawcy wysokiego ryzyka ma za zadanie 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 na bezpieczeństwo państwa oraz jego instytucji i newralgicznej infrastruktury.

Ustawa określi 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 strategiczny (Kolegium ds. Cyberbezpieczeństwa, w który zasiadają najważniejsi dla bezpieczeństwa państwa ministrowie oraz szefowie służb). Dodatkowo przewidziano możliwość weryfikacji decyzji przez właściwy sąd. W procesie tym opcjonalnie będą mogły także uczestniczyć organizacje społeczne i UOKiK.

Podjęta decyzja będzie uwzględniać zarówno przesłanki w zakresie ryzyka stworzenia zagrożeń w wymiarze ekonomicznym czy terrorystycznym, jak i techniczne, takie jak liczba i rodzaj wykrytych podatności oraz incydentów, tryb i zakres w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania, posiadanie przez dostawcę certyfikatów.

Przy nowelizacji tej ustawy planowane jest także wprowadzanie do porządku prawnego instytucji polecenia zabezpieczającego. Polecenie to będzie mogło być wydane przez ministra właściwego do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego, w celu skoordynowania efektywnej reakcji na ten incydent. Przed wydaniem polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Będzie ona przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Następnie minister właściwy do spraw informatyzacji będzie mógł wydać w drodze decyzji administracyjnej polecenie zabezpieczające odnoszące się do incydentu krytycznego. Będzie w nim zawarte wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego (z rygorem natychmiastowej wykonalności) jest konieczne dla zapewnienia bezpieczeństwa narodowego w obliczu coraz częstszych i poważniejszych cyberataków.

W obecnym stanie prawnym Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa może wydawać rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania. Przy nowelizacji ustawy planowane jest wzmocnienie mechanizmu rekomendacji.

Warto także podkreślić, że projektowane przepisy przewidują również sformalizowanie na poziomie ustawowy funkcjonowania Połączonego Centrum Operacyjnego Cyberbezpieczenstwa (PCOC). Działanie PCOC umożliwia szybką wymianę informacji, co pozwala podnieść poziom cyberbezpieczeństwa w kraju, w szczególności w zakresie reagowania na pojawiające się incydenty cyberbezpieczeństwa. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa. W związku z tym bieżąca koordynacja oraz zarządzanie incydentami

cyberbezpieczeństwa o charakterze i skali mającej potencjalny wpływ na funkcjonowanie państwa odbywa się - na poziomie operacyjnym w ramach spotkań PCOC. Natomiast w przypadku poziomu strategicznego - podczas posiedzeń Kolegium ds. Cyberbezpieczeństwa.

Ad 2) Jakie mechanizmy nadzoru i kontroli cyberbezpieczeństwa są stosowane wobec oprogramowania i urządzeń dostarczanych przez producentów taboru kolejowego? Czy wyniku awarii pociągów firmy Newag są przewidywane zmiany regulacyjne w tym zakresie?

Mechanizmy nadzoru i kontroli stosowane wobec oprogramowania i urządzeń dostarczanych przez producentów taboru kolejowego:

Zgodnie z art. 41 ust. 2 UKSC organem właściwymi do spraw cyberbezpieczeństwa dla sektora transportu (z wyłączeniem podsektora transportu wodnego) jest minister właściwy do spraw transportu, w tym w zakresie nadzoru i kontroli. Szczegółowy zakres zadań organu właściwego reguluje art. 42 UKSC[3]. Ponadto należy zaznaczyć, że przy omawianym zagadnieniu zastosowanie mają opisane powyżej Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dot. użytkowania urządzeń informatycznych lub oprogramowania.

Przewidywane zmiany regulacyjne w zakresie mechanizmów nadzoru i kontroli stosowanych wobec oprogramowania i urządzeń cyberbezpieczeństwa:

Przedstawiona w pkt. 1 interpelacji nowelizacja UKSC wprowadza szereg nowych rozwiązań prawnych wpływających na wzrost poziomu cyberbezpieczeństwa, w tym zwiększających efektywność środków przeciwdziałania incydentom bezpieczeństwa podobnym do omawianego. Do kluczowych rozwiązań zaliczyć można wcześniej wymienioną procedurę wykluczenia dostawcy wysokiego ryzyka, polecenia zabezpieczającego i rekomendacji Pełnomocnika Rządu do Sprawy Cyberbezpieczeństwa oraz dodatkowo wprowadzane zmiany w zakresie m.in. funkcjonowania podmiotów kluczowych i ważnych, zespołów CSIRT, systemu S46, nadzoru i środków egzekwowania

[3] Zadania organu właściwego do spraw cyberbezpieczeństwa zgodnie z art. 42 UKSC::
1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
2) wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
3) niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu;
4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;
5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
6) monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych;
7) wzywa na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;
8) prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych;
9) może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;
10) przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;
11) uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej.

przepisów przez organy właściwe ds. cyberbezpieczeństwa, kompetencji Ministra Cyfryzacji czy zmiany obowiązków Pełnomocnika Rządu ds. Cyberbezpieczeństwa i Kolegium ds. Cyberbezpieczeństwa.

Ad 3) Czy Ministerstwo Cyfryzacji współpracuje z innymi organami państwowymi (np. MSWiA, UOKiK, UTK) w tej sprawie?

Ministerstwo Cyfryzacji ściśle współpracuje z Ministerstwem Spraw Wewnętrznych i Administracji, Urzędem Ochrony Konkurencji i Konsumentów, Urzędem Transportu Kolejowego oraz innymi właściwymi podmiotami w zakresie swoich kompetencji celem kompleksowego rozwiązania problemów cyberbezpieczeństwa oraz przeciwdziałania przyszłym zagrożeniom o podobnej specyfice.

Należy dodać, że bieżąca koordynacja oraz zarządzanie incydentami cyberbezpieczeństwa o charakterze i skali mającej potencjalny wpływ na funkcjonowanie państwa odbywa się - na poziomie technicznym w ramach spotkań PCOC. Natomiast w przypadku poziomu strategicznego - podczas posiedzeń Kolegium ds. Cyberbezpieczeństwa.

Ad 4) Jakie wnioski wynikają z analizy tej sprawy w kontekście cyberbezpieczeństwa infrastruktury krytycznej? Jakie działania podjęto w odpowiedzi na te wnioski?

Analiza incydentu wykazała konieczność wzmocnienia efektywności podmiotów państwowych w zakresie nadzoru i kontroli systemów zabezpieczeń oraz zwiększenia świadomości na temat zagrożeń cyberbezpieczeństwa wśród operatorów infrastruktury kluczowej z perspektywy stabilnego funkcjonowania państwa oraz innych podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Wyżej wymienione wnioski są zbieżne ze zdefiniowanymi zmianami zaimplementowanymi w projekcie UKSC.

Ponadto Ministerstwo Cyfryzacji prowadzi cykliczne działania mające na celu edukację i budowanie świadomości dot. zagrożeń cyberbezpieczeństwa dla personelu podmiotów tworzących krajowy system cyberbezpieczeństwa oraz administracji publicznej.

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

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

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

ul. Królewska 27
00-060 Warszawa