Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.94.2025
Warszawa, 07 lipca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 20 maja br. Posłów na Sejm RP Pań Agnieszki Ścigaj, Anny Dąbrowskiej – Banaszek oraz Pana Grzegorza Piechowiaka w sprawie rosnącej liczby cyberataków na polskie przedsiębiorstwa (interpelacja nr 9912)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Ad 1) Jakie konkretne działania zostały podjęte przez Ministerstwo Cyfryzacji w celu przeciwdziałania rosnącej liczbie cyberataków na polskie firmy?

Ministerstwo Cyfryzacji realizuje szereg działań, których celem jest budowanie odporności na cyberzagrożenia kraju. Działania te adresowane są do rożnych kategorii odbiorców uwzględniając ich zróżnicowane potrzeby.

W odniesieniu do przedsiębiorców, to jednym z takich działań jest udostępnienie usługi moje.cert.pl. Jest to projekt realizowany przez Państwowy Instytut Badawczy NASK (NASK-PIB), w którego strukturze działa CSIRT NASK[1] (Zespół CERT Polska). Do zadań tego Zespołu należy m.in rejestracja i obsługa incydentów bezpieczeństwa sieci, aktywne reagowanie na zagrożenia, koordynacja obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych, współpraca w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa oraz tworzenie i udostępnianie narzędzi do wykrywania podatności i cyberzagrożeń oraz ich zwalczania. Serwis moje.cert.pl umożliwia każdemu właścicielowi domeny internetowej kompleksową diagnozę pod kątem cyberbezpieczeństwa. Z usługi mogą korzystać zarówno osoby prywatne, firmy, jak i duże instytucje publiczne.

Użytkownicy platformy mogą:

- zlecić bezpłatne skanowanie swoich domen i otrzymać szczegółowy raport o lukach w zabezpieczeniach;
- otrzymywać alerty o wyciekach haseł użytkowników powiązanych z ich domenami;
- sprawdzać, czy ich strona znajduje się na Liście Ostrzeżeń przed niebezpiecznymi stronami;
- uzyskiwać powiadomienia o infekcjach złośliwym oprogramowaniem i innych zagrożeniach.

Moje.cert.pl umożliwia kompleksową diagnozę domen czy serwisów pod kątem cyberbezpieczeństwa, dzięki zintegrowaniu w jednym miejscu kilku wysokiej klasy narzędzi. Do skanowania stron w serwisie moje.cert.pl wykorzystywany jest system Artemis (opisany szerzej w odpowiedzi na pyt. 6). Wdrożenie tego rozwiązania

[1] Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa z dn. 5 lipca 2018 r. (Dz.U. z 2024 r. poz. 1077) NASK-PIB został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT poziomu krajowego. Obowiązki CSIRT NASK, o których mowa w ustawie zostały powierzone zespołowi CERT Polska funkcjonującemu w strukturze NASK-PIB. NASK-PIB jest instytutem nadzorowanym przez Ministra Cyfryzacji.

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

ul. Królewska 27
00-060 Warszawa

ma szczególne znaczenie dla małych i średnich przedsiębiorców (MŚP), które często nie dysponują wystarczającymi zasobami, aby podejmować tego rodzaju działania.

Kolejną inicjatywną mającą na celu zwiększanie cyfrowego bezpieczeństwa polskich firm jest program Firma Bezpieczna Cyfrowo. Jego celem jest rozwój kompetencji cyfrowych polskich przedsiębiorców, podniesienie poziomu ochrony cyfrowej w sektorze MŚP oraz stabilności obrotu gospodarczego w kraju, a także upowszechnianie i wdrażanie nowych standardów cyberbezpieczeństwa w firmach. Uczestnictwo w programie pozwala przedsiębiorcom zrozumieć zagrożenia i wdrożyć konkretne środki zaradcze, a po pozytywnej weryfikacji - uzyskać certyfikat potwierdzający odpowiedzialne podejście do ochrony własnej działalności, partnerów i klientów. Udział w programie Firma Bezpieczna Cyfrowo daje przedsiębiorcom jasne wskazówki jak poprawić stan cyberbezpieczeństwa w firmie, zaś uzyskany certyfikat . poświadcza, że posiadające go przedsiębiorstwo w odpowiedzialny sposób dba o bezpieczeństwo własnego biznesu, a także swoich partnerów i klientów.

Ośrodek Standaryzacji i Certyfikacji, który działa w strukturze NASK-PIB, ma także uprawnienia do przyznawania certyfikatów Common Criteria (CC) w obszarze cyberbezpieczeństwa. Standard CC jest wykorzystywany do oceny bezpieczeństwa systemów i urządzeń IT. Certyfikaty CC są uznawane w 34 krajach, w tym m.in. Stanach Zjednoczonych, Japonii, Korei Południowej i większości państw europejskich. W swoich procedurach stosuje je też NATO. CC jako międzynarodowy standard, zapewnia formalną ocenę bezpieczeństwa produktów IT, co daje użytkownikom zapewnienie ich bezpieczeństwa i pozwala producentom na udowodnienie, że ich produkty spełniają określone standardy.

Dodatkowo NASK-PIB prowadzi działania edukacyjne i doradcze, promując wśród przedsiębiorców świadomość, że cyberbezpieczeństwo stanowi integralną część strategii biznesowej i odpowiedzialności społecznej. Działania edukacyjne adresowane do przedsiębiorców NASK-PIB realizuje również we współpracy z innymi resortami. W ramach projektu Digital Biznes[2] Ministerstwo Rozwoju i Technologii, Urząd m.st. Warszawy i Urząd Pracy m.st. Warszawy we współpracy z NASK-PIB zrealizowały cykl webinarów i spotkań stacjonarnych dla przedsiębiorców poświęcony transformacji cyfrowej, w tym dot. bezpiecznego korzystania z narzędzi cyfrowych.

Następnym z kolei działaniem adresowanym do przedsiębiorców jest konkurs grantowy pn. „Cyberbezpieczne wodociągi", o którym więcej znajduje się w odpowiedzi na pyt 2.

Ad 2) Kiedy i jakie środki zostaną przeznaczone na wsparcie małych i średnich przedsiębiorstw w zakresie cyberbezpieczeństwa?

Niebawem uruchomione zostaną projekty, w ramach których określone grupy przedsiębiorstw będą mogły wystąpić o wsparcie finansowe w formie grantów. Są to:

1) Konkurs grantowy pn. „Cyberbezpieczne wodociągi" adresowany do podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę, takich jak:

- Przedsiębiorstwa wodociągowo-kanalizacyjne, które są operatorami usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[3];
- Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej[4];

[2] https://www.biznes.gov.pl/pl/portal/035260
[3] (Dz. U. z 2024 r. poz. 1077 i 1222)
[4] (Dz. U. z 2021 r. poz. 679)

- Jednostki sektora finansów publicznych w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[5].

możliwe będzie uzyskania wsparcia w formie grantów ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (Inwestycja C3.1.1).

Planowany termin uruchomienia naboru wniosków o granty to III kwartał bieżącego roku.

Wsparcie finansowe pozyskane w konkursie będzie mogło zostać wykorzystane na działania, które mają bezpośredni wpływ na wzmocnienie odporności ww. podmiotów na cyberzagrożenia. Zakres projektu obejmował będzie działania z obszarów: organizacji (procesy), technologii oraz kompetencji, tj.:

- wdrożenie środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa;
- zakup lub modernizację środków technicznych służących zapewnieniu cyberbezpieczeństwa;
- rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Przewidywana maksymalna wartość grantu dla pojedynczego wnioskodawcy może wynosić do 300 tys. EUR (ok. 1,2 mln zł) i będzie ona zależna od maksymalnego limitu dostępnej pomocy *de minimis* dla danego podmiotu.

2) Konkurs grantowy dla polskich przedsiębiorców prowadzących działalność w obszarze cyberbezpieczeństwa, który. zostanie przeprowadzony w ramach realizacji projektu „National Coordination Centre – Poland", dofinansowanego ze środków programu Cyfrowa Europa. Planowane jest udzielanie wsparcia w obszarach: rozwoju istniejącego produktu lub usługi, stworzenia nowego rozwiązania, zwiększenia rozpoznawalności na rynku oraz certyfikacji produktu, a całkowita wartość planowanego dofinansowania to 1 800 000 EUR. Wsparcie to pomoże przedsiębiorcom oferującym produkty i usługi w obszarze cyberbezpieczeństwa na rozwijanie swoich rozwiązań i zwiększanie ich widoczności, co stanowi element wzmacniania krajowego potencjału w obszarze cyberbezpieczeństwa.

Ad 3) Czy Ministerstwo planuje wprowadzenie obowiązkowych standardów bezpieczeństwa dla firm działających w sektorach krytycznych?

Obecnie procesowany jest projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), który określi nowe obowiązki z zakresu cyberbezpieczeństwa dla szeregu podmiotów określanych jako podmioty kluczowe i ważne. Podmioty kluczowe i ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług kluczowych przez te podmioty. Odpowiada to zakresowi wymogów, co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy NIS2[6].

Tak jak do tej pory operatorzy usług kluczowych, tak i podmioty kluczowe i ważne będą obowiązane przeprowadzać audyty bezpieczeństwa swoich systemów informacyjnych, co trzy lata.

Podmioty kluczowe i ważne będą obowiązane korzystać z systemu S46 służącego wymianie informacji o incydentach, cyberzagrożeniach i podatnościach.

[5] (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756, i 1907 oraz z 2025 r. poz. 39)
[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

Rozwiązania te pozwolą zwiększyć cyberbezpieczeństwo w podmiotach krytycznych dla gospodarki. Projekt ten znajduje się na etapie Stałego Komitetu Rady Ministrów.

Publikowane są też rekomendacje standaryzujące rozwiązania zabezpieczające w sieciach i systemach informatycznych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. Dokumenty te są dostępne na portalu gov.pl w bazie wiedzy o cyberbezpieczeństwie[7], o której więcej w odpowiedzi na pyt. 4.

Ad 4) Jakie działania edukacyjne są planowane w celu zwiększenia świadomości przedsiębiorców na temat zagrożeń cybernetycznych?

Oprócz opisanego w odpowiedzi na pyt. 1 programu Firma Bezpieczna Cyfrowo, Ministerstwo Cyfryzacji, we współpracy z NASK-PIB, realizuje różnorodne projekty edukacyjne z zakresu cyberbezpieczeństwa, skierowane do szerokiego grona odbiorców – zarówno instytucji publicznych, jak i obywateli oraz przedsiębiorców. Warto podkreślić, że zasady cyberhigieny dotyczą każdego użytkownika internetu – niezależnie od wieku, miejsca pracy czy poziomu zaawansowania technologicznego. Dlatego nasze kampanie, szkolenia i materiały edukacyjne są przygotowywane tak, aby wspierać zarówno indywidualnych użytkowników, jak i przedstawicieli sektora biznesowego – w tym MŚP.

W ramach takich działań, NASK-PIB prowadzi kampanie informacyjne w zakresie bezpiecznego korzystania z Internetu, opracowuje i publikuje materiały edukacyjne[8] dot. różnego rodzaju oszustw internetowych[9].

Opisany w odpowiedzi na pyt. 1 serwis moje.cert.pl jest rozwijany o nowe funkcjonalności. Od maja br. dostępna jest nowa zakładka, gdzie umieszczane są ostrzeżenia dotyczące polskiej cyberprzestrzeni i alerty o podatnościach. Kolejną planowaną funkcjonalnością portalu moje.cert.pl jest włączenie systemu powiadomień dla użytkowników, którzy zgłoszą się do systemu i wyrażą zgodę na ich otrzymywanie. Dzięki temu będą mogli oni otrzymywać alerty o zagrożeniach, w tym ostrzeżenia o podatnościach oraz informacje o nowych, potencjalnych zagrożeniach.

Ministerstwo Cyfryzacji prowadzi również powszechnie dostępna bazę wiedzy o cyberbezpieczeństwie na portalu gov.pl, o której wspomniano w odpowiedzi na pyt. 3. Oprócz opisanych powyżej rekomendacji standaryzujących, w bazie tej publikowane są opracowania z obszaru cyberbezpieczeństwa dla różnych grup odbiorców, w tym dla każdego[10] użytkownika Internetu, a także podmiotów krajowego systemu cyberbezpieczeństwa (dla profesjonalistów)[11].

Ad 5) Czy Ministerstwo współpracuje z sektorem prywatnym w zakresie wymiany informacji o zagrożeniach i najlepszych praktykach w dziedzinie cyberbezpieczeństwa?

Tak, Ministerstwo Cyfryzacji od lat aktywnie rozwija partnerstwo z podmiotami prywatnymi w obszarze cyberbezpieczeństwa, zgodnie z zapisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[12]. Współpraca ta obejmuje zarówno wymianę informacji o zagrożeniach, jak i wspólne działania na rzecz budowy odporności infrastruktury krytycznej i cyfrowej. Współpraca ta jest prowadzona w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber)[13] zainicjowanym w 2019 r. Program ten służy integracji wiedzy eksperckiej i doświadczenia firm technologicznych z działaniami

[7] https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyberbezpieczenstwa2
[8] https://cert.pl/
[9] https://cert.pl/ouch/
[10] https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
[11] https://www.gov.pl/web/baza-wiedzy/dla-profesjonalistow
[12] Art. 45 ust. 1 pkt 2 Ustawa z dnia z dnia 5 lipca 2018 r., Dz.U. z 2024 r. poz. 1077
[13] https://www.gov.pl/web/baza-wiedzy/o-programie

administracji publicznej. W ramach PWCyber prowadzone są wspólne działania w kilku strategicznych obszarach, jak: podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatyczny oraz identyfikacja podatności i zagrożeń, wymiana informacji, wypracowywanie metod zgłaszania i obsługi incydentów, organizacja i udział w ćwiczeniach symulacyjnych, przekazywanie zaleceń i dobrych praktyk dotyczących zabezpieczeń i konfiguracji systemów.

Dzięki wspólnym działaniom i wymianie wiedzy, partnerzy Programu przyczyniają się do rozwoju kompetencji w zakresie cyberbezpieczeństwa oraz wdrażania nowoczesnych rozwiązań w sektorze publicznym, co jest kluczowe w obliczu dynamicznie zmieniających się wyzwań technologicznych. Jedną ze sztandarowych inicjatyw PWCyber są bezpłatne, specjalistyczne szkolenia online, organizowane cyklicznie przez Ministerstwo Cyfryzacji we współpracy z partnerami Programu, które adresowane są do kadr podmiotów krajowego systemu cyberbezpieczeństwa. Podzielone są na trzy kategorie: szkolenia dotyczące podstaw cyberhigieny (poziom 100), szkolenia dla kadry zarządzającej i pracowników działów IT (poziom 200) oraz szkolenia dla specjalistów IT (poziom 300). Od 2020 r. dzięki zaangażowaniu partnerów przeprowadzono 102 szkolenia, w których łącznie udział wzięło prawie 57 tys. osób, w tym specjaliści IT z administracji rządowej, samorządowej, szpitali i placówek ochrony zdrowia. Przekazana wiedza przyczynia się do podnoszenia kompetencji z zakresu cyberbezpieczeństwa i budowania silnego systemu cyberbezpieczeństwa w Polsce, zdolnego do skutecznego przeciwdziałania zagrożeniom. Prowadziliśmy także cykle szkoleniowe adresowane do konkretnych grup podmiotów funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa.

Ponadto w Ministerstwie Cyfryzacji zostało powołane Krajowe Centrum Kompetencji Cyberbezpieczeństwa będące ogniwem europejskiej sieci krajowych ośrodków koordynacji utworzonych w 2021 r. i współdziałających z Europejskim Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC). NCC-PL pełni rolę punktu kontaktowego i ośrodka informacji dla polskich podmiotów działających w obszarze cyberbezpieczeństwa.

Centrum realizuje to zadanie poprzez:

- bieżące udostępnianie informacji w zakresie działań i inicjatyw europejskich organizacji i europejskiej społeczności cyberbezpieczeństwa, w tym o prowadzonych projektach, dobrych praktykach i opracowanych zasobach. Informacje są na bieżąco udostępniane na stronie internetowej NCC-PL (https://www.gov.pl/web/cyber-nccpl) i poprzez bieżącą wymianę informacji ze społecznością cyberbezpieczeństwa;
- wspieranie podmiotów zainteresowanych aplikowaniem o granty ze środków europejskich na projekty w obszarze cyberbezpieczeństwa, (w szczególności z Programu Cyfrowa Europa – Cyberbezpieczeństwo), poprzez rozpowszechnianie informacji o ogłaszanych konkursach, udzielanie odpowiedzi na pytania dotyczące naborów oraz udzielanie pomocy przy poszukiwaniu partnerów i dołączaniu przez polskie podmioty do konsorcjów projektowych;
- wspieranie współpracy i wymiany informacji, zarówno krajowej jak i transgranicznej, poprzez organizację paneli eksperckich, sesji pitchingowych, wydarzeń matchmakingowych;
- gromadzenie informacji o potrzebach polskiego sektora cyberbezpieczeństwa, m. in. poprzez realizację badania polskich małych i średnich przedsiębiorców działających w obszarze cyberbezpieczeństwa, którego celem jest identyfikacja barier hamujących rozwój tych podmiotów na rynku, stojących przed nimi wyzwań, a także form wsparcia, którego potrzebują (badanie obecnie jest w toku).

W maju br. wiceminister cyfryzacji Rafał Rosiński zapowiedział powołanie *Grupy Roboczej ds. Wsparcia Polskiego Biznesu ICT w Ekspansji Zagranicznej*. Celem nowej inicjatywy będzie opracowanie strategii wspierania polskich firm technologicznych na rynkach zagranicznych.

Grupa skupi się na:

- identyfikacji barier i szans ekspansji,
- tworzeniu narzędzi wsparcia dla firm z sektora ICT,
- budowie systemowego podejścia do umiędzynarodowienia polskich technologii.

W skład grupy wejdą przedstawiciele ministerstw, instytucji publicznych, firm technologicznych oraz innych partnerów wspierających cyfrowy rozwój Polski.

Powołanie grupy roboczej to odpowiedź na dynamiczny rozwój sektora ICT i rosnącą potrzebę wsparcia jego międzynarodowej obecności. Wypracowana strategia ma zwiększyć konkurencyjność oraz widoczność polskich firm technologicznych na rynkach światowych.

Ad 6) Jakie mechanizmy monitorowania i raportowania incydentów cybernetycznych są obecnie stosowane i czy planowane są ich ulepszenia?

Tak jak zostało opisane w odpowiedzi na pyt. 1, za monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, reagowanie na zgłoszone incydenty, a także rozwijanie narzędzi i metod do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa, odpowiada działający w strukturach NASK-PIB CSIRT NASK (Zespół CERT Polska). Podsumowanie kluczowych wydarzeń w polskiej cyberprzestrzeni prezentowane są w formie corocznego raportu: Krajobraz bezpieczeństwa polskiego internetu[14].

W celu należytej koordynacji bieżącego zarządzania cyberbezpieczeństwem Ministerstwo Cyfryzacji organizuje spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). Funkcjonowanie PCOC umożliwia szybką wymianę informacji oraz reagowania na pojawiające się incydenty. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa. W procedowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa planowane jest sformalizowanie działania PCOC.

Ponadto, jak zostało już wspomniane w odpowiedzi na pyt. 3, Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydaje rekomendacje i komunikaty, których wdrożenie przez podmioty krajowego systemu cyberbezpieczeństwa pozwala minimalizować ryzyka związane z identyfikowanymi podatnościami oraz kampaniami w cyberprzestrzeni.

Ważne są także działania takie jak:

- ARAKIS GOV - system wczesnego ostrzegania o zagrożeniach w sieci Internet, który powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej. System jest prowadzony przez Agencję Bezpieczeństwa Wewnętrznego. W 2024 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 1 947 791 593 przepływy, co przełożyło się na 5 446 734 wygenerowane przez system alarmy, w tym 3 322 068 o priorytecie pilnym, tzn. wymagających natychmiastowej reakcji administratorów.
- ARTEMIS - narzędzie służące do wykrywania najczęściej występujących podatności i błędów konfiguracyjnych obecnych w ramach usług sieciowych.

[14] https://cert.pl/publikacje/

Za rozwój tego narzędzia odpowiada zespół CERT Polska. Regularne skanowanie systemów pozwala monitorować i poprawiać poziom ich bezpieczeństwa. Weryfikacji podlegają przede wszystkim podmioty z obszaru działania CSIRT NASK[15]. Podmioty nieobjęte skanowaniem mogą samodzielnie zlecić sprawdzanie swoich domen w serwisie moje.cert.pl. opisanym w odpowiedzi na pyt. 1. W 2024 r. system znalazł ponad 331 tys. podatności i błędnych konfiguracji, w tym niemal 20 tys. wiążących się z wysokim ryzykiem.

Ad 7) Czy Ministerstwo przewiduje wsparcie finansowe dla firm, które padły ofiarą cyberataków, w celu szybkiego przywrócenia ich działalności?

Ministerstwo Cyfryzacji nie przewiduje wprowadzenia takiego mechanizmu, co nie oznacza, że nie prowadzi działań mających na celu wspieranie podmiotów również po skutecznym ataku hakerskim.

Jednym z takich działań jest przedsięwzięcie polegającego na utworzeniu zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych oraz prowadzeniu działań podnoszących świadomość o cyberbezpieczeństwie. Jest to przedsięwzięcie o wartości 37,5 mln zł, które zostanie zrealizowane do 30 czerwca 2026 r. w ramach inwestycji C3.1.1 Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).

Celem przedsięwzięcia jest modernizacja i profesjonalizacja zespołów policji, które będą wspierać zaatakowane podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych. Grupy te będą działać w oparciu o wypracowane i transparentne metodyki oraz współpracować z przedstawicielami CSIRT NASK i organów ścigania.

Zakres tego przedsięwzięcia obejmie m.in.:

- realizacji specjalistycznych szkoleń dla organów ścigania;
- utworzenie i wdrożenie centralnego narzędzia wsparcia działań prowadzonych na miejscu zdarzenia, a także współdzielenia rezultatów uzyskanych w toku analizy;
- wypracowanie zasad współpracy pomiędzy organami ścigania a CSIRT NASK.

Więcej informacji temat tego przedsięwzięcia jest dostępnych pod adresem: https://www.gov.pl/web/cyfryzacja/375-mln-zl-na-wsparcie-polskiej-policji-w-zakresie-cyberbezpieczenstwa oraz https://www.gov.pl/web/cppc/inwestycja-c-311-cyberbezpieczenstwo---cyberpl-piaty-nabor.

Kolejnym działaniem, którego celem jest m.in. wspieranie podmiotów po skutecznym ataku hakerskim, jest współfinansowany ze środków UE w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), projekt pn. „Centrum Cyberbezpieczeństwa NASK" (CCN). Celem tego projektu jest utworzenie 7 nowych specjalistycznych centrów, ośrodków i laboratoriów istotnych z punktu widzenia wzmocnienia krajowego systemu cyberbezpieczeństwa, tj.:

- Krajowe Centrum Odzyskiwania Danych;
- Krajowe Centrum Operacyjne Cyberbezpieczeństwa;
- Modelowy Ośrodek treningowo-szkoleniowy w obszarze Cyberbezpieczeństwa;
- Laboratorium Bezpieczeństwa AI;
- Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania;
- Krajowe Centrum Wsparcia Security dla JST;

[15] Zgodnie z art. 26 ust. 6 ustawy o krajowym systemie cyberbezpieczeństwa z dn. 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077)

- Ośrodek Modelowania Certyfikacji Cyberbezpieczeństwa.

Celem utworzenia Krajowego Centrum Odzyskiwania Danych jest w szczególności wsparcie podmiotów, które w wyniku ataku mają zaszyfrowane dane. W ramach tego centrum zakłada się powstanie mobilnych zespołów reagowania i budowę infrastruktury odzyskiwania danych.

Celem utworzenie Krajowego Centrum Wsparcia Security dla JST jest z kolei zapewnienie wsparcia zaatakowanym jednostkom samorządu terytorialnego, w tym identyfikacja zagrożeń w infrastrukturze tych podmiotów.

Całkowita wartość projektu CCN wynosi 310 mln zł. Więcej informacji na jego temat jest dostępnych na stronach https://nask.pl/projekty/centrum-cyberbezpieczenstwa-nask oraz https://www.gov.pl/web/cppc/centrum-cyberbezpieczenstwa-nask-akronim-ccn.

Ad 8) Jakie działania są podejmowane w celu zwiększenia liczby specjalistów w dziedzinie cyberbezpieczeństwa w Polsce?

Zwiększenie liczby specjalistów ICT jest jednym z priorytetów Ministerstwa Cyfryzacji. Jest to zgodne z założeniami unijnej strategii "Cyfrowa Dekada 2030". Ministerstwo koordynuje wdrażanie tego programu, który wyznacza cele cyfrowe dla UE do 2030 r. Kluczowe wskaźniki do osiągnięcia to: 6-procentowy udział specjalistów ICT wśród ogółu pracujących oraz zwiększenie udziału kobiet w tym gronie do 29%.

Jedną z inicjatyw, która ma zwiększyć liczbę specjalistek w branży teleinformatycznej jest konkurs „Zostań cyfrową ekspertką", w ramach którego organizacje pozarządowe składały propozycje szkoleń dla kobiet z zakresu kompetencji cyfrowych Przemysłu 4.0. (AI, big data, systemy cyberbezpieczeństwa, przetwarzanie danych w chmurze itp.). Ministerstwo Cyfryzacji w 2024 r. przeznaczyło dla zwycięzców konkursu we wszystkich mikroregionach 6 milionów złotych.

Należy też wspomnieć o działaniach takich jak Cyberbezpieczny Samorząd[16] oraz Cyberbezpieczny Rząd[17] adresowanych do podmiotów administracji publicznej, w ramach których część środków zostanie przeznaczona na:

- podniesienie kompetencji pracowników i specjalistów odpowiedzialnych za cyberbezpieczeństwo w danej instytucji.

Ad 9) Czy Ministerstwo planuje kampanie informacyjne skierowane do obywateli w celu zwiększenia ich świadomości na temat zagrożeń w cyberprzestrzeni?

W 2024 r. Ministerstwo Cyfryzacji przystąpiło do procedury pozyskiwania środków unijnych na prowadzenie kampanii w obszarze cyberbezpieczeństwa. W maju 2024 r. zawarto z Centrum Projektów Polska Cyfrowa porozumienie na dofinansowanie drugiej edycji projektu pn. „Kampanie edukacyjno-informacyjne na rzecz upowszechniania korzyści z wykorzystywania technologii cyfrowych" (dalej projekt KEI2).
Projekt przewiduje realizację przez NASK-PIB kampanii nt. głównych cyberzagrożeń dotykających osoby dorosłe oraz tematu uzależnienia dzieci i młodzieży od internetu.

Kampania będzie realizowana w sposób ciągły do końca 2027 r., a zaplanowany budżet na kampanię wynosi około 23 mln zł. Opis projektu znajduje się na pod linkiem: https://www.gov.pl/web/cyfryzacja/kampanie-edukacyjno-informacyjne-na-rzecz-upowszechniania-korzysci-z-wykorzystywania-technologii-cyfrowych

[16] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad
[17] https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad

Pierwsza odsłona tej kampanii została uruchomiona w maju 2025 r. przez NASK-PIB i jest aktualnie emitowana w internecie:

- link do komunikatu nt. startu kampanii: https://nask.pl/aktualnosci/bezpieczny-dzien-nowa-kampania-nask-i-ministerstwa-cyfryzacji;
- link do strony kampanii : https://nask.pl/bezpiecznydzien;
- link do spotu reklamowego emitowanego w kampanii: https://www.youtube.com/watch?v=-osiI3IWhg0.

W projekcie od sierpnia 2024 r. także prowadzone są bieżące działania komunikacyjne obejmujące publikację komunikatów prasowych oraz ich promocji w postaci postów na mediach społecznościowych. Za realizację tych zadań odpowiada NASK-PIB, oto 2 przykładowe komunikaty z tej kampanii dystrybuowane na kanałach NASK i do mediów:

- „Chcesz szybko zarobić w internecie? Uważaj, żeby dużo nie stracić" https://nask.pl/aktualnosci/chcesz-szybko-zarobic-w-internecie-uwazaj-zeby-duzo-nie-stracic;
- „Granie z głową – jak chronić dzieci w cyfrowym świecie?" https://nask.pl/aktualnosci/granie-z-glowa-jak-chronic-dzieci-w-cyfrowym-swiecie.

Ponadto, w marcu 2025 r. uruchomiona została druga edycja kampanii edukacyjnej pn. „W cyfrowym świecie". W jej ramach są emitowane audycje na antenach 17 rozgłośniach radiowych Polskiego Radia. Kampania będzie emitowana do końca czerwca 2025 r.

W kampanii emitowano 15-minutowe audycje radiowe, z których część dotyczyła także bezpieczeństwa w sieci. Poniżej lista tematów:

- „Dzieci w wirtualnej rzeczywistości" dotyczący użytkowania Internetu i korzystania z technologii przez dzieci.
- Rodzice w cyfrowym świecie", dotyczący korzyści edukacyjnych i zagrożeń korzystania z Internetu przez dzieci, ochrony dzieci przed niebezpieczeństwem w sieci.
- „Bezpieczeństwo w sieci" dotyczący świadomego i bezpiecznego korzystania z nowych technologii oraz podniesienia świadomości zagrożeń i problemów występujących w świecie cyfrowym.
- „Senior w wirtualnej rzeczywistości" dotyczący użytkowania Internetu przez seniorów, bezpieczeństwa w sieci, dezinformacji.

Link do komunikatu nt. uruchomienia tej kampanii z jej opisem: https://www.gov.pl/web/cyfryzacja/kampania-spoleczna-w-cyfrowym-swiecie-ponownie-w-polskim-radiu--edukacja-cyfrowa-w-calej-polsce

Równocześnie, aktualnie ministerstwo cyfryzacji przygotowuje bardzo dużą i istotną kampanię świadomościową i edukacyjną nt. rozwoju kompetencji cyfrowych. Będzie ona skierowana do wszystkich obywateli, a także zawierała wyodrębnioną komunikację do przedsiębiorców. Kampania jest planowana na pierwszą połowę 2026 r. i będzie ona finansowana z Krajowego Planu Odbudowy.

W kampanii będziemy zachęcać Polaków do rozwoju kompetencji cyfrowych, także w zakresie bezpiecznego korzystania z internetu (cyberbezpieczeństwa oraz cyberhigieny). Będziemy zachęcać do dbania o kompetencje cyfrowe w życiu prywatnym i zawodowym oraz doradzać jakie kompetencje rozwijać. Będziemy w kampanii także zachęcać do rozpoczęcia edukacji i kariery zawodowej (np. przebranżowienia się) w kierunkach związanych z ICT (w tym cyberbezpieczeństwie).

Aktualnie trwają przygotowania do ogłoszenia przetargu na agencję reklamową, która będzie realizowała kampanię – trwają konsultacje rynkowe, w ramach których Ministerstwo Cyfryzacji zbiera opinie do projektu dokumentacji przetargowej. Link do informacji o konsultacjach: https://www.gov.pl/web/cyfryzacja/konsultacje-rynkowe-przed-przetargiem-na-kampanie-zachecajaca-do-rozwoju-kompetencji-cyfrowych

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