Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.100.2025
Warszawa, 07 sierpnia 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 13 czerwca br. Posła na Sejm RP Pana Janusza Cieszyńskiego w sprawie zagrożeń cyberbezpieczeństwa w polskiej administracji publicznej (interpelacja nr 10151)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie konkretne działania podejmuje resort w celu poprawy stanu cyberbezpieczeństwa w polskiej administracji publicznej i czy planowane jest wprowadzenie obowiązkowych testów penetracyjnych dla instytucji publicznych?

Ministerstwo Cyfryzacji prowadzi obecnie szereg działań, których celem jest zwiększenie poziomu cyberbezpieczeństwa w administracji publicznej.

Realizowane są projekty „Cyberbezpieczny Rząd" i „Cyberbezpieczny Samorząd" w ramach, których podmioty publiczne mogą otrzymać wsparcie finansowe na cele związane z cyberbezpieczeństwem.

Prowadzone są też bezpłatne szkolenia skierowane do podmiotów krajowego systemu cyberbezpieczeństwa w tym dla administracji publicznej. W 2023 r. dodatkowo uruchomiono szkolenie e-learningowe pn. „Podstawowe zasady cyberbezpieczeństwa oraz zasady bezpieczeństwa stacji roboczych SRP", które jest dostępne na platformie pl.ID Platforma szkoleniowa. Od 2023 r. szkolenie odbyło ponad 1700 pracowników administracji publicznej.

Należy też zwrócić uwagę na przygotowane przez Ministerstwo Cyfryzacji projektu aktów prawnych w obszarze cyberbezpieczeństwa. Trwają obecnie prace nad projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), który zawiera szereg rozwiązań, mających przyczynić się do wzrostu cyberbezpieczeństwa m.in. precyzując zasady współpracy organów w przypadku wystąpienia incydentu krytycznego. Ponadto, w dniu 25 czerwca 2025 r. Sejm uchwalił, ustawę o krajowym systemie certyfikacji cyberbezpieczeństwa, która stworzy ramy certyfikacji cyberbezpieczeństwa w Polsce. Umożliwi ona podniesienie poziomu cyberbezpieczeństwa usług i produktów wykorzystywanych przez administrację

Przeprowadzono również nowelizację uchwały o zmianie uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa". Dzięki temu, administracja rządowa może korzystać z usług oferowanych w publicznych chmurach obliczeniowych w jurysdykcji krajowej ale również w jurysdykcji pozostałych państw Europejskiego Obszaru Gospodarczego, jeżeli państwa te stosują prawo Unii Europejskiej. Powszechniejsze korzystanie z usług przetwarzania w chmurze przyczyni się do podniesienia poziomu bezpieczeństwa przetwarzanych danych, trwałego obniżenia kosztów stałych przetwarzania danych, efektywności wydatkowania środków, a także skrócenia czasu realizacji nowych przedsięwzięć informatycznych.

Przygotowywana jest również aktualizacja Standardów Cyberbezpieczeństwa Chmur Obliczeniowych co pozwoli na większe wykorzystanie bezpiecznych rozwiązań

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

ul. Królewska 27
00-060 Warszawa

chmurowych w administracji. Testy penetracyjne dla podmiotów publicznych prowadzone są przez Agencję Bezpieczeństwa Wewnętrznego, w ramach oceny bezpieczeństwa, na podstawie ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[1]. Oceny bezpieczeństwa są przeprowadzane zgodnie z rocznym planem przeprowadzania ocen bezpieczeństwa, a w uzasadnionych przypadkach również z pominięciem tego planu. Testy prowadzone są w porozumieniu z podmiotem, którego systemy są badane, z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie teleinformatycznym podlegającym tej ocenie.

Jeżeli wykryta podatność może wystąpić w innych systemach teleinformatycznych, ABW informuje niezwłocznie ministra właściwego do spraw informatyzacji o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach teleinformatycznych

Szef ABW może również żądać przedstawienia informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych, w tym informacji obejmujących hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemu.

Należy również zauważyć, że zgodnie z rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2] podmioty publiczne wdrażają system zarządzania bezpieczeństwem informacji, w ramach którego jednym z obowiązków jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. Może to stanowić osobną podstawę do zamówienia przeprowadzenia testów penetracyjnych przez podmiot publiczny jeśli jest to potrzebne do przeprowadzenia oceny.

Również procesowany obecnie projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (UC32) zawiera obowiązki związane z oceną bezpieczeństwa przez podmioty publiczne. Po nowelizacji CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe będą mogły przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa, w tym testy penetracyjne. Ocena bezpieczeństwa systemu informacyjnego będzie mogła być przeprowadzona za zgodą podmiotu, którego system będzie testowany albo na zlecenie organu właściwego do spraw cyberbezpieczeństwa. W każdym przypadku proces ten będzie musiał zostać uzgodniony z badanym podmiotem i będzie przeprowadzany z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego. Takie rozwiązanie pozwoli zapewnić możliwość wykonywania testów penetracyjnych w podmiotach krajowego systemu cyberbezpieczeństwa. Dzięki możliwości zlecenia testu przez organ ds. cyberbezpieczeństwa będzie możliwe również przeprowadzenie ich w potencjalnie zagrożonych instytucjach wytypowanych przez organy właściwe do spraw cyberbezpieczeństwa. Rozwiązania te zapewnią większą dostępność testów penetracyjnych i pozwolą na efektywne wskazanie jednostek, które najbardziej ich potrzebują.

Ad 2) Jakie środki finansowe zostały zabezpieczone w budżecie państwa na rok 2025 na cele związane z cyberbezpieczeństwem administracji publicznej i czy kwota ta jest wystarczająca w obliczu rosnących zagrożeń?

[1] art. 32a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2024 r. poz. 812, 1222, 1562, 1684, 1871 oraz Dz. U. z 2025 r. poz. 179)
[2] Dz.U. z 2024 r. poz. 773.

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

ul. Królewska 27
00-060 Warszawa

Łącznie w budżecie państwa w zakresie cz. 27 – Informatyzacja, której dysponentem jest Minister Cyfryzacji, na 2025 r. na cele związane z cyberberbezpieczeństwem zostały zaplanowane środki w wysokości (stan na 1 stycznia 2025 r.): 433 878 000,00 zł.

Ponadto, wydatki na cyberbezpieczeństwo wyznaczają również środki zgromadzone w Funduszu Cyberbezpieczeństwa i limity wydatków w wykonywanych aktach prawnych. W 2024 r. zwiększono również środki przeznaczone na wypłatę świadczenia teleinformatycznego podnosząc limit wydatków w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa ze 100 mln złotych do 250 mln złotych. Limit ten podwyższono też dla kolejnych lat.

Ponadto, w ramach ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa[3] uchwalonej przez Sejm w dniu 25 czerwca 2025 r., przewidziano środki na realizację nowych zadań związanych z nadzorem nad certyfikacją jak i budową zdolności do certyfikacji cyberbezpieczeństwa, w tym na rozbudowę laboratoriów. Na 2025 r. przewidziano, że środki te będą wynosić:

- 9,7 mln zł dla Ministerstwa Cyfryzacji,
- 0,3 mln zł dla Polskiego Centrum Akredytacji.

W kolejnych latach kwoty te będą odpowiednio zwiększane. Ponadto, ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa ma również powiększyć limit wydatków na 2025 r. wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Ma on wzrosnąć do 80,3 mln złotych w 2025 r., umożliwiając realizację dodatkowych zadań z zakresu cyberbezpieczeństwa.

Również projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) implementujący dyrektywę NIS2 przewiduje wzrost wydatków na realizację zadań z zakresu cyberbezpieczeństwa. Zgodnie z ww. projektem środki na wykonanie tej ustawy będą w 2025 r. wynosić 310,58 mln złotych i będą rosły w kolejnych latach. Pozwoli to skutecznie sfinansować wydatki związane z przebudową krajowego systemu cyberbezpieczeństwa.

Ad 3) Czy prowadzone są regularne audyty cyberbezpieczeństwa w kluczowych instytucjach publicznych, takich jak szpitale, urzędy wojewódzkie czy samorządowe, a jeśli tak, to z jaką częstotliwością i jakie są ich wyniki?

Zgodnie z §19 ust. 2 pkt 14 Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4], podmioty publiczne są obowiązane do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Ponadto, podmioty publiczne będące jednocześnie operatorami usług kluczowych mają również obowiązek przeprowadzenia, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Przepisy prawa wymagają już regularnych audytów cyberbezpieczeństwa w podmiotach publicznych.

Jednym z przedsięwzięć, za pomocą których realizowane jest wzmacnianie ochrony kluczowych instytucji państwowych w obliczu rosnącej liczby cyberataków jest współfinansowany ze środków KPO (Inwestycja C3.1.1), konkurs grantowy pn. „Cyberbezpieczny Rząd”. Jest to przedsięwzięcie, którego celem jest wsparcie administracji rządowej w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Wsparcie skierowane jest do podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w ustawie o krajowym systemie cyberbezpieczeństwa[5], takich jak naczelne lub centralne organy administracji rządowej

[3] https://www.sejm.gov.pl/Sejm10.nsf/PrzebiegProc.xsp?nr=1238.
[4] Dz. U. z 2024 r. poz. 773.
[5] art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 i 1222)

oraz wojewodowie. Urzędy obsługujące te organy, wraz z jednostkami im podległymi. W ramach tego programu możliwe jest finansowanie kosztów związanych z przeprowadzaniem przez wykwalifikowanych audytorów, audytów systemu zarządzania bezpieczeństwem informacji, stanowiących dowód wdrożenia i stosowania ww. systemu w organizacji lub instytucji. Zgodnie z analizą treści wniosków o grant, wnioskodawcy planują w ramach środków z tego projektu wydać łącznie prawie 4,5 mln zł na realizację zadań związanych z przeprowadzeniem audytów systemu zarządzania bezpieczeństwem informacji (SZBI). Warunki naboru, w tym regulamin konkursu zostały opublikowane na stronie projektu Centrum Projektów Polska Cyfrowa..

Do konkursu przystąpiło 53 Wnioskodawców, w tym: 13 ministerstw, 21 urzędów centralnych oraz 16 urzędów wojewódzkich. Wartość zgłoszonych projektów wyniosła ponad 276,6 mln zł, co oznacza realizację alokacji środków przeznaczonych na ten projekt na poziomie ponad 79%. Ostatecznie pozytywnie ocenione zostało 51 wniosków, na łączną kwotę ponad 271,3 mln zł, zgodnie z listą rankingową opublikowaną pod linkiem https://www.gov.pl/attachment/ef4ab316-8b62-43b5-b239-6a6469d16f21.

Kolejną inicjatywą wspierającą podmioty publiczne w realizacji obowiązków audytowych jest projekt „Cyberbezpieczny Samorząd". W jego ramach przewidziana została również możliwość finansowania kosztów związanych z przeprowadzaniem audytów systemu bezpieczeństwa informacji wdrożonego w urzędzie jednostki samorządu terytorialnego, który obejmuje zgodność z kryteriami zawartymi w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[6] (KRI) lub zgodność z wymaganiami normy PN-ISO/IEC 27001. Zgodnie z zapisami umownymi Grantobiorcy są zobowiązani do załączenia raportu z tego audytu do wniosku rozliczającego projekt. Zgodnie z analizą treści wniosków o wsparcie grantowe, samorządy planują w ramach środków z tego projektu wydać łącznie prawie 55 mln zł na realizację zadań związanych z przeprowadzeniem audytów SZBI.

Projekt ten jest w trakcie realizacji. Do końca 2024 r. zostały podpisane wszystkie (2 495) umowy z JST, które złożyły wniosek o wsparcie grantowe i sukcesywnie wypłacane są im środki na realizację grantów, których łączna wartość wynosi 1 474 312 573,61 zł. Projekt jest współfinansowany ze środków UE w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Projekty grantowe mogą być realizowane do 30 czerwca 2026 r. Dokumentacja naboru oraz dodatkowe materiały informacyjne dot. tego projektu zostały opublikowane na stronie Centrum Projektów Polska Cyfrowa.

Ad 4) Jakie działania edukacyjne podejmowane są w celu podniesienia świadomości pracowników administracji publicznej w zakresie zagrożeń cybernetycznych, szczególnie tych związanych z wykorzystaniem sztucznej inteligencji przez cyberprzestępców?

W ramach projektów pn. „Cyberbezpieczny Rząd" oraz „Cyberbezpieczny Samorząd", przywołanych w odpowiedzi na poprzednie pytanie (Ad 3), zakres wsparcia obejmuje trzy kluczowe obszary cyberbezpieczeństwa, tj.: obszar organizacji, technologii i kompetencji.

W ramach wzmocnienia cyberbezpieczeństwa w obszarze kompetencji, przewidziana została możliwość finansowania m.in. kosztów:

- podstawowych szkoleń (lub dostępu do platform szkoleniowych) budujących świadomość cyberzagrożeń i sposobów ochrony dla pracowników, obejmujących m.in. symulowane cyberataki na użytkowników sieci i systemów informacyjnych w organizacji (np. phishing),
- szkoleń z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry podmiotu, istotnej z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji,

[6] Dz.U. z 2024 r. poz. 773.

- szkoleń specjalistycznych dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa,
- szkoleń powiązanych z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Zgodnie z analizą treści wniosków o grant w konkursie „Cyberbezpieczny Rząd", wnioskodawcy planują w ramach środków z tego projektu wydać łącznie prawie 18,6 mln zł na wzmocnienie cyberbezpieczeństwa w obszarze kompetencji.

Zgodnie z analizą treści wniosków o wsparcie grantowe w projekcie „Cyberbezpieczny Samorząd", samorządy planują w ramach środków z tego projektu wydać łącznie ponad 112 mln zł na wzmocnienie cyberbezpieczeństwa w obszarze kompetencji.

Ministerstwo Cyfryzacji prowadzi również szereg działań prewencyjno-edukacyjnych skierowanych do społeczeństwa, w szczególności:

- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa: od 2020 r. prowadzone są bezpłatne szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Dotychczas przeprowadzono 123 szkolenia, w których uczestniczyło ponad 66 tys. osób, a w tym:
  - szkolenia dla kadr podmiotów publicznych
  - szkolenia dla operatorów usług kluczowych
  - szkolenia dla użytkowników Systemów Rejestrów Państwowych
  - szkolenia dla podmiotów publicznych wykonujących działalność leczniczą
- Szkolenie e-learningowe: w 2023 r. uruchomione zostało szkolenie e-learningowe pn. „Podstawowe zasady cyberbezpieczeństwa oraz zasady bezpieczeństwa stacji roboczych SRP", które jest dostępne na platformie pl.ID Platforma szkoleniowa. Od 2023 r. szkolenie odbyło ponad 1700 pracowników administracji publicznej.
- Szkolenie z cyberhigieny na platformie szkolenia.gov.pl: w I kwartale 2025 r. na rządowym portalu szkolenia.gov.pl uruchomione zostanie szkolenie z zakresu cyberbezpieczeństwa. Szkolenie będzie dostępne dla każdego zainteresowanego po zalogowaniu na platformę szkolenia.gov.pl (z pomocą profilu zaufanego). Szkolenie jest e-learningowym kursem dotyczącym podstaw cyberbezpieczeństwa, stworzonym z myślą o wszystkich obywatelach pragnących zwiększyć swoją wiedzę na temat ochrony danych osobowych i prywatności w sieci.
- Projekty SecureV: od 2021 r. prowadzone są działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa m.in. dla najważniejszych osób w państwie (projekty SecureV). Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej. Jednak z uwagi na dynamiczną sytuację w cyberprzestrzeni oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców. W 2023 r. szkoleniami objęci byli: parlamentarzyści, kadra kierownicza administracji rządowej (centralnej i terenowej) i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej. Tylko w 2024 r. przeszkolono blisko 5 tys. osób.
- Projekt Cyberlekcje - od 2021 r. Ministerstwo Cyfryzacji wspólnie z NASK-PIB realizuje projekt adresowany do nauczycieli i pedagogów, chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w Internecie. W ramach projektu Cyber lekcje powstało 18 gotowych scenariuszy zajęć lekcyjnych o cyberbezpieczeństwie skierowanych do różnych grup wiekowych uczniów w szkołach podstawowych i ponadpodstawowych. W ramach projektu powstały również dodatkowe materiały, jak: infografiki, prezentacje, animacje oraz filmy z ekspertami, które wraz z scenariuszami są udostępnione dla wszystkich zainteresowanych w powszechnie dostępnej bazie wiedzy cyberbezpieczeństwa na portalu gov.pl w zakładce CyberEdukacja, a także na Zintegrowanej Platformie

Edukacyjnej, narzędziu rekomendowanym przez Ministerstwo Edukacji Narodowej. W 2024 r. zrealizowany został pilotaż w ramach którego przeprowadzono m.in. stacjonarne szkolenia dla kadry pedagogicznej.

- Konkurs CyberWizards 2024 – International Cyber Camp: Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej zorganizował nabór do CyberWizards International Camp. Nagrodą był cyberobóz w Estonii dla zwycięskiej drużyny. Wysłanie do Estonii polskiej drużyny dziewcząt stanowi jeden z wielu elementów promujących od najmłodszych lat karierę kobiet w branży cyberbezpieczeństwa.

Ministerstwo Cyfryzacji opracowało prezentację, która zawiera wskazówki jak bezpiecznie korzystać z GenAI w administracji publicznej. Wskazówki te są dostępne na portalu sztucznej inteligencji gov.pl. Choć materiał nie dotyczy bezpośrednio jakiegoś konkretnego modelu wskazujemy, aby do narzędzi GenAI nie wpisywać informacji, które np. zawierają wewnętrzne informacje urzędowe, będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia lub zawierają dane osobowe, których ujawnienie narusza przepisy o ochronie danych osobowych.

Ad 5) Czy rozważane jest utworzenie centralnej jednostki odpowiedzialnej za koordynację działań w zakresie cyberbezpieczeństwa sektora publicznego oraz czy istnieją procedury reagowania na incydenty cybernetyczne?

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 procedowanym projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) planowane jest sformalizowanie działania PCOC, które faktycznie funkcjonuje od 2022 r.

Procedury obsługi incydentów na poziomie strategicznym są określone w ustawie o krajowym systemie cyberbezpieczeństwa. Robocza koordynacja realizowana na poziomie krajowym jest realizowana w ramach spotkań PCOC. Jeśli chodzi o poszczególne incydenty obsługiwane przez CSIRTy poziomu krajowego lub sektorowe zespoły cyberbezpieczeństwa to są one rozwiązywane zgodnie z wewnętrznymi procedurami tych podmiotów.

Ponadto, Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydaje rekomendacje i komunikaty, których wdrożenie przez podmioty KSC (w tym instytucje publiczne) pozwala minimalizować ryzyka związane z identyfikowanymi podatnościami oraz kampaniami w cyberprzestrzeni.

Ad 6) Jakie są plany modernizacji systemów informatycznych w administracji publicznej, aby były one odporne na zagrożenia oparte na sztucznej inteligencji i innych nowoczesnych metodach ataku?

W tym roku przedstawimy pierwszą wersję cyber.gov.pl, który będzie nowoczesną, rządową platformą stworzoną z myślą o bezpieczeństwie cyfrowym obywateli, firm i instytucji publicznych. W jednym miejscu znajdą się wszystkie kluczowe usługi i narzędzia - od zgłaszania incydentów, przez monitorowanie zagrożeń, po dostęp do rozwiązań takich jak Artemis, S46, czy aplikacji moje.cert.pl. Platforma oferować będzie również dostęp do bazy wiedzy, szkoleń, alertów i praktycznych informacji o obowiązkach wynikających z ustawy o krajowym systemie cyberbezpieczeństwa[7] (KSC) i dyrektywy NIS2[8]. Dzięki

[7] Dz.U. z 2024 r. poz. 1077 i 1222.
[8] 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).

integracji m.in. z węzłem krajowym, logowanie i korzystanie z serwisu będzie łatwe i bezpieczne. Cyber.gov.pl to realne wsparcie w codziennym poruszaniu się w cyfrowym świecie.

Cały czas rozwijany jest System S46, który służy do wymiany informacji i zgłaszania incydentów w ramach KSC. System wspiera zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy podmiotami KSC, a także szacowanie ryzyka na poziomie krajowym. Na zakończenie 2024 r. z Systemu S46 korzystało 248 podmiotów, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, takie jak Jednostki Samorządu Terytorialnego. W obszarze utrzymania zapewniono sprawność systemu na poziomie nie mniejszym niż 99% w skali roku. System jest rozbudowywany tak aby po implementacji dyrektywy NIS2 stał się głównym kanałem komunikacji między podmiotami kluczowymi i ważnymi i organami administracji.

Ad 7) Czy planowane jest wprowadzenie obowiązkowych standardów cyberbezpieczeństwa dla wszystkich instytucji publicznych oraz systemu certyfikacji i regularnego monitorowania ich przestrzegania?

Obecne przepisy ustawy o krajowym systemie cyberbezpieczeństwa pozwalają już na wprowadzenie jednolitych rozwiązań w określonych obszarach. Zgodnie z art. 33 ust. 4 ww. ustawy pełnomocnik może wydawać rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania. Rekomendacje te pozwalają ujednolicić podejście w określonych obszarach i są wydawane na bieżąco. Listę rekomendacji można znaleźć na stronie internetowej gov.pl.

Ponadto organy właściwe do spraw cyberbezpieczeństwa mogą we współpracy z zespołami CSIRT poziomu krajowego wydawać rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów.

W zakresie systemów zarządzania bezpieczeństwem informacji funkcjonuje obecnie §19 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[9], które określa jakie elementy taki system ma zawierać, wprowadzając jednakowy standard we wszystkich podmiotach publicznych.

Ponadto, procesowana nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (projekt UC32) zawiera szereg rozwiązań, które pozwolą jeszcze bardziej zwiększyć spójność rozwiązań stosowanych w administracji publicznej. Zgodnie z dodawanym art. 67a, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa będzie mógł wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Dodawany art. 8a przewiduje, że Rada Ministrów może określić, w drodze rozporządzenia szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji stosowanego przez podmioty kluczowe i ważne z określonego sektora np. administracji publicznej. Umożliwi to uszczegółowienie i ujednolicenie wymagań z zakresu cyberbezpieczeństwa dla sektora publicznego. W dniu 25 czerwca 2025 r. Sejm uchwalił ustawę o krajowym systemie certyfikacji cyberbezpieczeństwa[10], która stworzy ramy certyfikacji cyberbezpieczeństwa w Polsce. Zgodnie z przyjętym modelem certyfikacji będzie możliwa na podstawie europejskich programów certyfikacji oraz krajowych schematów certyfikacji, które będą wydawane w drodze rozporządzeń Ministra Cyfryzacji.

Posiadanie krajowego certyfikatu będzie dowodem spełnienia wymogów z zakresu cyberbezpieczeństwa i będzie zachętą dla konsumentów do korzystania z takich

[9] Dz.U. z 2024 r. poz. 773
[10] https://www.sejm.gov.pl/Sejm10.nsf/PrzebiegProc.xsp?nr=1238.

produktów. Ponadto, tego rodzaju certyfikaty będą mogły być wykorzystane w relacjach z administracją publiczną np. w ramach postępowań o udzielenie zamówienia publicznego. Wykorzystanie na szerszą skalę certyfikowanych produktów pozwoli na zapewnienie jednolitych standardów w podmiotach publicznych.

Dzięki wprowadzeniu certyfikatów opartych o przepisy prawa będzie możliwa promocja konkretnych rozwiązań z zakresu cyberbezpieczeństwa. Certyfikaty będą dawały istotne korzyści w ramach postępowań o udzielenie zamówienia publicznego i umożliwią podmiotom publicznym łatwą oceną rozwiązań pod kątem ich cyberbezpieczeństwa

Po uzyskaniu certyfikacji dostawca danego produktu lub usługi dla której wydano certyfikat musi przez cały okres ważności certyfikatu utrzymywać zgodność z wymaganiami określonymi w programie.

Już obecnie możliwa jest w Polsce certyfikacja w ramach systemu Common Criteria, a jednostki certyfikujące i laboratoria prowadzą działania zmierzające do dostosowania do pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa – EUCC[11]. Zakończenie tego procesu umożliwi wydawanie certyfikatów uznawanych na terenie całej Unii Europejskiej.

Również w obszarze krajowych schematów certyfikacji cyberbezpieczeństwa chcemy rozwijać to co już zostało stworzone. Obecnie, NASK realizuje program certyfikacji Firma Bezpieczna Cyfrowo. Ma on na celu wsparcie polskich przedsiębiorców w budowaniu kompetencji cyfrowych oraz podniesieniu poziomu cyberbezpieczeństwa w sektorze MŚP (małych i średnich przedsiębiorstw). Inicjatywa ta odpowiada na rosnące zagrożenia cyberatakami, wzmacniając stabilność obrotu gospodarczego oraz promując nowy standard ochrony danych w firmach. Planowane jest przekształcenie tego programu w krajowy schemat certyfikacji cyberbezpieczeństwa, który będzie wyznaczał standardy w zakresie procesów zarządzania cyberbezpieczeństwem w organizacji.

W ramach krajowych schematów certyfikacji cyberbezpieczeństwa będzie rozwijany również segment certyfikacji osób. Planujemy przygotować schematy certyfikacji dotyczące kompetencji, które będą mogły być wykorzystywane zarówno przez sektor publiczny jak i prywatny. Certyfikaty pozwolą ukierunkować rozwój kompetencji w tym obszarze w stronę najistotniejszych zadań realizowanych w sektorze publicznym.

W związku z pracami na forum europejskim przygotowany zostanie również krajowy schemat certyfikacji cyberbezpieczeństwa portfela tożsamości cyfrowej. Przygotowanie takiego programu wynika z przyjętych ustaleń w ramach Unii Europejskiej.

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

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[11] Rozporządzenie wykonawcze komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881. w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC).