Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.68.2025
Warszawa, 03 czerwca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 10 kwietnia br. Posłanki na Sejm RP Pani Olgi Ewy Semeniuk – Patkowskiej w sprawie wyzwań dla bezpieczeństwa wewnętrznego oraz stanu przygotowania służb i koordynacji działań międzyresortowych (interpelacja nr 9131)

Szanowny Panie Marszałku,

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

Ad 1) Czy planowana jest aktualizacja i wzmocnienie Krajowego Planu Reagowania Kryzysowego, w szczególności w zakresie zagrożeń hybrydowych i ataków cybernetycznych?

Zgodnie z ustawą[1] Krajowy Plan Reagowania Kryzysowego (KPZK) podlega aktualizacji nie rzadziej niż raz na dwa lata, jak również wtedy, gdy w wyniku uruchomienia procedur zostanie stwierdzona potrzeba wprowadzenia korekty, uzupełnienia danej procedury lub w przypadku zmiany aktów prawnych, mających znaczenie dla funkcjonowania KPZK. W 2024 r. Rządowe Centrum Bezpieczeństwa podjęło pracę nad aktualizacją KPZK. Jednak już obecnie obowiązujący KPZK 2021/2022, w części B identyfikuje w siatce bezpieczeństwa 19 zagrożeń w tym zakłócenia w funkcjonowaniu sieci i systemów informatycznych oraz działania hybrydowe. Zadania realizowane w tym zakresie opisano w pkt. 2 „Zadania w zakresie monitorowania zagrożeń zakłócenia w funkcjonowaniu sieci i systemów informatycznych" oraz w pkt 7 „Procedury realizacji zadań z zakresu zarządzania kryzysowego – standardowe procedury operacyjne, w tym związane z ochroną infrastruktury krytycznej".

Ad 4) Czy istnieje plan skoordynowanej edukacji obywatelskiej (np. przez MON, MSWiA i MEN) w zakresie obronności, cyberbezpieczeństwa, reagowania kryzysowego i dezinformacji?

Ministerstwo Cyfryzacji, we współpracy z NASK-PIB, realizuje wiele działań edukacyjnych z zakresu cyberbezpieczeństwa, które są kierowane do różnych grup użytkowników internetu. Działania te uwzględniają m.in. aspekty bezpiecznego korzystania z mediów społecznościowych. W ramach działań edukacyjnych, NASK-PIB prowadzi kampanie informacyjne w zakresie bezpiecznego korzystania z Internetu. NASK-PIB opracowuje i publikuje materiały edukacyjne dot. różnego rodzaju oszustw internetowych, w tym m.in. oszustw na fałszywe inwestycje (Uważaj na fałszywe inwestycje w sieci), fałszywych sklepów online (Jak kupować bezpiecznie online.).

NASK-PIB uruchomił również możliwość zgłaszania treści i profili, które noszą znamiona działań dezinformacyjnych. Inicjatywa ta nosi nazwę #WŁĄCZWERYFIKACJĘ.[2] Tego typu treści można zgłaszać na adres: informacje@nask.pl. Zgłoszone treści są weryfikowane przez doświadczonych ekspertów, którzy ocenią potencjalne przejawy działań dezinformacyjnych. Na podstawie zweryfikowanych zgłoszeń NASK-PIB informuje

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r., poz. 122)
[2] https://www.nask.pl/pl/aktualnosci/4411,WlaczWeryfikacje-NASK-przeciw-dezinformacji-w-sieci.html

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

ul. Królewska 27
00-060 Warszawa

o przypadkach dezinformacji, równocześnie przedstawiając rzetelne informacje o zagadnieniach, których dotyczyła dana nieprawdziwa wiadomość Działania te prowadzone są zarówno na Facebooka (Meta), jak i Platformie X (Twitterze). W przypadku gdy określone treści wypełniają znamiona czynu zabronionego, wówczas informowane są również organy ścigania, które podejmą działania w celu wykrycia sprawcy.

Ponadto, na portalu gov.pl rozwijana jest baza wiedzy cyberbezpieczeństwa[3], gdzie publikowane są praktyczne poradniki, artykuły, rekomendacje oraz inne materiały edukacyjne, które pozwalają społeczności internetowej zdobyć wiedzę na temat bezpiecznego korzystania z technologii cyfrowych i jak chronić się przed cyberzagrożeniami.

Realizowane są również projekty wpierające nauczanie o bezpieczeństwie online: „CYBER lekcje"[4] oraz „Bezpieczni w Sieci"[5] skierowane do uczniów szkół podstawowych i ponadpodstawowych. Celem tych projektów jest edukacja o cyberbezpieczeństwie dopasowana do aktualnych trendów funkcjonowania dzieci i młodzieży w internecie oraz cyberzagrożeń, z którymi stykają się najmłodsi użytkownicy sieci m.in. w mediach społecznościowych. Jednocześnie, Ministerstwo Cyfryzacji prowadzi intensywne działania informacyjne dotyczące zgłaszania incydentów cyberbezpieczeństwa i prób oszustw. Wszystkie próby oszustw internetowych należy zgłaszać do Zespołu CERT Polska. Zgłoszeń można dokonać poprzez formularz na stronie https://incydent.cert.pl lub wysyłając e-mail na adres cert@cert.pl. Fałszywe wiadomości SMS można zgłosić używając w swoim telefonie funkcji "przekaż" albo "udostępnij" i przesłać treść otrzymanej wiadomości na numer 8080.

Ad 5) Czy rząd przewiduje wsparcie samorządów w zakresie tworzenia lokalnych systemów bezpieczeństwa – takich jak monitoring, patrole obywatelskie, centra zarządzania kryzysowego?

Ministerstwo Cyfryzacji wspiera samorządy w zakresie tworzenia lokalnych systemów bezpieczeństwa poprzez udostępnienie dla ich potrzeb systemów łączności:

- **Systemu SKR-Z** (System Komunikacji Rządowej – Zastrzeżonej) to system niejawnej łączności mobilnej, umożliwiający przetwarzanie informacji niejawnych o klauzuli ZASTRZEŻONE/NATO RESTRICTED/EU RESTRICTED. W ramach świadczonej usługi telekomunikacyjnej, użytkownik ma zapewniony dostęp do:
  - usługi jawnej (bezpiecznej) łączności głosowej;
  - poczty elektronicznej umożliwiającej przekazywanie informacji niejawnych do klauzuli „zastrzeżone", Restraint UE/UE Restricted, NATO Restricted;
  - komunikatora głosowego umożliwiającego przekazywanie informacji niejawnych do klauzuli „zastrzeżone", Restraint UE/UE Restricted, NATO Restricted;
  - wytwarzania dokumentów niejawnych do klauzuli „zastrzeżone", Restraint UE/UE Restricted, NATO Restricted.

  System powstał na zlecenie Ministra Cyfryzacji w 2021 r., został zrealizowany przez NASK-PIB w ramach zadania publicznego p.n. „Budowa systemu łączności mobilnej umożliwiającej przetwarzanie informacji niejawnych do klauzuli „zastrzeżone" w oparciu o system „CATEL".

  W systemie SKR-Z wykorzystywane są certyfikowane telefony służbowe, dedykowane do komunikacji w trybie niejawnym oraz „laptopy Z" - działające jedynie w obszarze niejawnym o klauzuli ZASTRZEŻONE. System SKR-Z

[3] https://www.gov.pl/web/baza-wiedzy/aktualnosci
[4] https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji
[5] https://bezpieczniwsieci.edu.pl/

współpracuje z systemami: Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego i Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. Aktualnie zapewnia komunikację pomiędzy użytkownikami zarówno za pomocą komunikatora, jak też poczty elektronicznej.
NASK-PIB udostępnia podmiotom urządzenia systemu w ramach indywidualnych porozumień, umów użyczenia, podmioty ponoszą jedynie koszt abonamentu.

- **Komunikatora Threema OnPrem**, jest to aplikacja mobilna na licencji szwajcarskiej, utrzymywana na serwerach polskiego dostawcy Operatora Chmury Krajowej (OChK) i zarządzana przez Zespół Komunikatora w Ministerstwie Cyfryzacji.
  Aplikacja mobilna komunikatora dostępna jest dla systemów Android i iOS oraz przez przeglądarkę www. Dane osobowe przetwarzane są w Polsce. Komunikator Threema onPrem powstał na zlecenie Ministra Cyfryzacji w 2022 r. z potrzeby zapewnienia bezpiecznej, jawnej komunikacji służbowej pracownikom administracji publicznej i terenowej, infrastruktury krytycznej oraz podmiotów należących do krajowego systemu cyberbezpieczeństwa. Jako rozwiązanie zastępuje powszechnie dostępne i używane komunikatory.

  Komunikator jest stale monitorowany w trybie 24/7 przez zespół SOC i helpdesk w OChK. Komunikacja w aplikacji szyfrowana jest „end-to-end" z wykorzystaniem kluczy szyfrujących rozmówców. Jest rozwiązaniem, utrzymywanym na lokalnej infrastrukturze w Polsce u polskiego Dostawcy OChK, posiadającego wdrożony System Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania i certyfikaty na zgodność z ISO 27001, ISO 22301, ISO 27017 (BI w chmurze) i ISO 27018 (bezpieczne dane w chmurze).

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