Ministerstwo Cyfryzacji

Finał konsultacji społecznych Strategii Cyfryzacji Państwa – 11 grudnia 2024 r.

Panel: „Cyberbezpieczeństwo”

Panel poświęcony cyberbezpieczeństwu został otwarty przez Sekretarza Stanu w Ministerstwie Cyfryzacji Pana Pawła Olszewskiego oraz Dyrektora Departamentu Cyberbezpieczeństwa Pana Łukasza Wojewodę. Następnie Dyrektor Departamentu Cyberbezpieczeństwa przedstawił prezentację (w załączeniu) obejmującą następujące elementy:

- **Co się udało w cyber**
    - Dojrzały i ewoluujący KSC – oprócz wprowadzonych i projektowanych zmian systemowych/prawnych ciągle rozwijamy potencjał techniczny, operacyjny i osobowy polskiego cyberbezpieczeństwa.
    - Inicjatywy takie jak: PCOC, AntyDDoS, CTI, ARTEMIS, ARAKIS GOV, Komunikator i SKR-Z, S46, Fundusz Cyberbezpieczeństwa, PWCyber, Cyberbezpieczny Samorząd, Szkolenia, Zmiana WIIP, Telegraf.cert.pl i UZNKE, BezpieczeneDane.gov.pl, Ćwiczenia KSC, Rekomendacje i komunikaty Pełnomocnika, NCC PL, Współpraca międzynarodowa.
- **Cyberbezpieczeństwo w dokumentach strategicznych**
    - Strategia Cyfryzacji Polski (SCP)
    - Strategia Cyberbezpieczeństwa RP (SCRP)
    - Strategia Bezpieczeństwa Narodowego RP (SBN RP)
    - inne dokumenty strategiczne
- **Strategia Cyfryzacji Polski**
    - Cele
        - Cel 1: Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny.
        - Cel 2: Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności.

- Cel 3: Krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiada rozwinięty potencjał i cechuje się wysokim stopniem suwerenności technologicznej.
- Cel 4: Kadry podmiotów krajowego systemu cyberbezpieczeństwa oraz społeczeństwo posiadają świadomość cyberzagrożeń oraz wiedzę i kompetencje w zakresie cyberbezpieczeństwa.
- Cel 5: Polska posiada silną pozycję międzynarodową w obszarze cyberbezpieczeństwa.

o Najważniejsze przedsięwzięcia

- Powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym
- Wzmacnianie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa
- Rozwijanie Systemu S46
- Wzmacnianie potencjału instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym
- Tworzenie CSIRT-ów sektorowych
- Udzielanie podmiotom KSC wsparcia w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa, w tym JST
- Cyberbezpieczeństwo w zamówieniach publicznych
- Wyłączenie pilnych zakupów związanych z cyberbezpieczeństwem z PZP
- Rozwój krajowej kryptografii i migracja do kryptografii postkwantowej
- Skoordynowane zarządzanie podatnościami
- Chmura niejawna
- Rozwój zdolności CTI
- Zwiększenie bezpieczeństwa łańcuchów dostaw
- Mechanizm HRV
- Certyfikacja cyberbezpieczeństwa
- Wykorzystanie technologii przełomowych w cyberbezpieczeństwie, w tym AI
- Zwiększanie świadomości i wiedzy społeczeństwa

- Wzmacnianie kompetencji kadr podmiotów KSC
- Funduszu Cyberbezpieczeństwa
- Współpraca międzynarodowa na poziomie strategicznym oraz operacyjnym i technicznym
- Koordynowanie przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa

- **Strategia Cyberbezpieczeństwa RP**
  - Kontekst
  - Cele
  - Podobieństwa i różnice z SCP
  - Najważniejsze przedsięwzięcia (realizowane i rozwijane, przygotowywane, planowane)
  - Zakres przedmiotowy (cyberbezpieczeństwa a dezinformacja)

W kolejnej części panelu miały miejsce pytania i komentarze ze strony uczestników, na które odpowiadali obaj prelegenci. Poniżej przytaczane są podniesione kwestie wraz z odniesieniami do nich (które padły w trakcie spotkania, jak również inne – dodano w notatce na potrzeby informacyjne).

1. Pytanie: Zbytnia nadregulacja przepisów dotyczących cyberbezpieczeństwa, w szczególności zwrócono uwagą na mechanizm umożliwiający wykluczanie dostawców wysokiego ryzyka (HRV), jak również zapytano, czy planowane jest wsparcie finansowe dla firm na wymianę sprzętu (w przypadku wykluczanie danego sprzętu w ramach mechanizmu HRV)

Wyjaśnienia:

- Przygotowywana nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (ustawa o KSC) ustanowi proces umożliwiający wykluczenie danego typu sprzętu w przypadku zidentyfikowania, że stanowi zagrożenie dla bezpieczeństwa narodowego, natomiast sama ustawa nie będzie nic wykluczyć. Nowelizacja ustawy dopiero otworzy możliwość uruchomienia odpowiedniej procedury, która będzie mogła wykluczyć dany produkt, jeśli stanowi on zagrożenie dla cyberbezpieczeństwa. Takie proces obejmować będzie zarówno szczebel

techniczno-merytoryczny (badania przez zespoły CSIRT), jak i strategiczno-polityczny (Kolegium ds. Cyberbezpieczeństwa). Będzie wiec to należycie uregulowany proces, w sposób transparentny, jak również zapewniona będzie możliwość weryfikacji przez niezawisły sąd.

- Bezpieczeństwo narodowe priorytetem.
- Mechanizm HRV (i jego ew. zastosowanie) należy traktować jako inwestycje w bezpieczeństwo i wiarygodność.
- Ministerstwo Cyfryzacji przeznacza już duże środki publiczne na cyberbezpieczeństwo dla różnych podmiotów.
- W przypadku, gdy dany sprzętu będzie wykluczony na podstawie przepisów o HRB podmioty będą mieć na jego wymianę 4-7 lat (co w wielu przypadkach przekracza cykl życia sprzętu ICT).
- Mechanizm HRV nie jest wymierzony w żadną konkretną firmę, zostanie ustanowiony proces, który będzie mógł być zastosowany, jeśli zostanie zidentyfikowane, że dany sprzętu stanowi zagrożenie.

2. Pytanie: Wpisać małe i średnie przedsiębiorstwa (MŚP) jako silną stronę w analizie SWOT w części dotyczącej cyberbezpieczństwa

Wyjaśnienia:

- Do rozważenia uwzględnienie roli MŚP w części dotyczącej suwerenności technologicznej.

3. Pytanie: Zwrócenie uwagi na nadregulację dostawców oraz krytycznie odniesiono się do mechanizmu HRV. Postulowano wprowadzić tylko niezbędne ograniczenia, w tym ograniczyć mechanizm HRV tylko do 5G, nie każdą technologię obejmować tym mechanizmem.

Wyjaśnienia: patrz pkt 1.

4. Pytanie: prośba o pomoc w oszacowaniu, które podmioty wejdą do KSC po nowelizacji ustawy o KSC (dotyczy sektora ochrony zdrowia). Pytający zwrócił uwagę, że posiadają pewne szacunki i są to bardzo duże liczby. Jednak chcieli by ustalić tę liczbę w bardziej pewny sposób.

Wyjaśnienie:

- Trwają prace nad ustawą, jeszcze nie jest znany jej ostateczny kształt.

- Należy odpowiedzieć sobie na pytanie, czy wyłącznie kogoś z systemu jest rozwiązaniem? Zamykanie oczu nie jest rozwiązaniem problemu. Takimi podmiotami, które obecnie nie mają środków na cyberbezpieczeństwo, a są ważne, trzeba pomóc w spełnieniu wymogów (stąd szereg inicjatyw MC takich jak np. Cyberbezpieczny Samorząd). To tak jakby zlikwidować mandaty, przecież nie przełoży się to na większe bezpieczeństwo na drogach
- Pewne rzeczy trzeba uregulować, aby były należycie realizowane. Doświadczenia pokazują, że bez wprost określenie pewnych ustawowych obowiązków nie będą zrealizowanie działania ważne dla cyberbezpieczeństwa kraju.

5. Pytanie: Znacznie ochrony danych osobowych w kontekście cyberbezpieczeństwa (vide: ostatni atak na MPK w Krakowie). Postulat zwiększenia odpowiedzialności administratorów danych.

Wyjaśnienia:

- Osobne reżimy prawne ochrony danych osobowych i cyberbezpieczeństwa, ale pracujemy nad tym, aby były coraz bardziej spójne.
- Przykładowo w nowelizacji ustawy KSC przewiduje się, że incydent cyberbezpieczeństwa i dotyczący danych osobowych będzie się zgłaszać jednocześnie w systemie S46, który będzie „jednym okienkiem". Chcemy, żeby ta funkcjonalność zaczęła działać w S46 w I poł. 2025.

6. Pytanie: Znaczenie zarządzania kryzysowego, w tym zapewnienie odpowiedniej komunikacji i systemu powiadamiania, unifikacja podmiotów systemu zarządzania kryzysowego i KSC

Wyjaśnienia:

- Osobne reżimy prawne zarządzania kryzysowego i cyberbezpieczeństwa, ale pracujemy nad tym, aby były coraz bardziej spójne. Na poziomie ustawowo-systemowym systemy zarządzania kryzysowego oraz KSC zostaną zbliżone w związku z unijnymi dyrektywami (CER dla zarządzania kryzysowego oraz NIS 2 dla cyberbezpieczeństwa).
- Funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) – format cotygodniowych spotkań z udziałem najważniejszych instytucji dla bezpieczeństwa państwa (w tym zarządzania kryzysowego). Planujemy dalej

rozwijać PCOC i powołać centralną instytucję odpowiedzialną za cyberbezpieczeństwo na poziomie krajowym – pomoże to jeszcze lepiej koordynować działania.

- Posiadamy i rozwijamy narzędzia komunikacji (Komunikator, SKR-Z, ponadto zgodnie z ustawą o ochronie ludności (będącą na finalnym etapie legislacyjnym) MSWiA ma uruchomić System Bezpiecznej Łączności Państwowej (SBŁP)).
- Obsługa incydentów cyberbezpieczeństwa jest realizowana przez zespoły CSIRT, które współpracują ze sobą, jak również z MC, organami ścigania i innymi służbami.
- Aby zapewnić szybkie zalecenie w przypadku cyberataków i wykrycia nowych podatności Ministerstwo Cyfryzacji przygotowuje rekomendacje i komunikaty Pełnomocnika Rządu ds. Cyberbezpieczeństwa.
- W kwestii komunikacji strategicznej należy podkreślić, że w PCOC bierze udział też KPRM, gdzie zlokalizowane jest Centrum Informacyjne Rządu (CIR).

7. Pytanie: Bezpieczeństwo sprzętowe (hardwere'owe). Postulat uzależnienia administracji rządowej i infrastruktur krytycznej od korzystania z własnego czasu (synchronizacja czasu przy wykorzystaniu własnych serwerów czasu)

Wyjaśnienie:

- Jest to bardzie specyficzne zagadnienie, nie wszystko należy aż tak uszczegółowić, tym bardziej na poziomie strategicznym
- Ta kwestia będzie pośrednio ujęta w przepisach dot. łańcucha dostaw (certyfikacja w cyberbezpieczeństwie)
- Jest to też rola podmiotów, które wprowadzają pewne rozwiązania w ramach swojej organizacji, aby zapewnić ich cyberbezpieczeństwo (także w wymiarze sprzętowym)

8. Pytanie: Kiedy będą znane szczegóły i harmonogram dla inicjatywy Lokalnych Centrów Cyberbezpieczeństwa

Wyjaśnienia:

- Prawdopodobnie projekt będzie uruchamiany na początku przyszłego roku

9. Pytanie: Czy z punktu widzenia Strategii kwestia open source jest postrzegana jako istotna. Czy postrzega się to bardziej jako szansę czy zagrożenie?

Wyjaśnienie:

- W części Strategii dotyczącej cyberbezpieczeństwa nie ma ukierunkowania na open source. W Strategii jest osobny rozdział o open source.
- Należy zauważyć, że open source jest i będzie obecny. Wykorzystania tego typu oprogramowania w kontekście cyberbezpieczeństwa sprowadza się do analizy ryzyka, która pokaże co w danym przypadku w danych uwarunkowania wniesie w danej organizacji.

10. Pytanie: Dane osobowe i cyberbezpieczeństwo

Wyjaśnienie: patrz pkt 5.