



## Konsultacje społeczne dot. strategii cyfryzacji państwa

### „Cyberbezpieczeństwo – administracji, biznesu i obywateli”

#### Panel prowadzili:

- Monika Pieniek – zastępca dyrektora Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
- Marcin Wysocki – zastępca dyrektora Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

#### Pytania do uczestników konsultacji

1. Papierowe cyber, czy niezbędne formalności w zakresie dokumentacji – co należy zmienić?
2. Co powinno być priorytetem wynikającym ze Strategii Cyberbezpieczeństwa i Strategii Cyfryzacji?
3. Jak wspierać podmioty krajowego systemu cyberbezpieczeństwa?
4. AI, kryptografia kwantowa w cyberbezpieczeństwie – szansa czy zagrożenie?

#### Wypowiedzi uczestników konsultacji

##### Alina Zając, Cyber Woman

Zwróciła uwagę na problem papierowego cyberbezpieczeństwa. Z jej praktyki wynika, że musi zebrać dużo podpisów, aby spisać dokumentację, czy sprawozdanie z audytu, co demotywuje. W kontekście AI wskazała na brak standaryzacji dokumentów źródłowych – potrzebny byłby odcisk, pieczęć, znak wodny potwierdzający, że informacja jest z danego źródła.

##### Paweł Wołoch

Zapytał dlaczego MC wdraża postępowanie w sprawie dostawcy wysokiego ryzyka, które wynika z aktów prawa miękkiego UE, czyli aktów niemających charakteru powszechnie obowiązującego. Przepisy te stanowią ograniczenie swobody prowadzenia działalności gospodarczej. Zapytał również jak Państwo może wesprzeć przedsiębiorców – wskazał tutaj na kwestię wprowadzenia klauzul waloryzacyjnych. Konieczne byłyby w tym zakresie negocjacje z UOKiK.

##### Teresa Wierbowska

Zauważyła, że cyberprzestępczość chodzi parami. Istnieją serwisy pirackie zawierające złośliwe oprogramowanie. Zaapelowała o sprawne wdrożenie mechanizmów live blocking. Komisja europejska odpytuje państwa nt. mechanizmów związanych z live blocking – przedstawienie wniosków przypada na polską prezydencję.

##### Andrzej Umiński, dyrektor Biura Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości

Zauważył, że mają wiele systemów o charakterze krytycznym. Mają ambicje do utworzenia



CSIRT. Jednakże nie wiedzą jak traktować taki CSIRT w administracji w projektowanej nowelizacji KSC. Inwestycje w kadrę - świadczenie teleinformatyczne.

Ryszard Stefańczyk, Polski PCS sp. z o.o.

Poprosił o wsparcie MC w utworzeniu SOC-a w PCS dla stoczni/portów.

Robert Solnica, Huawei

Wskazał, że powinny być utworzone architektury referencyjne dla samorządów. Jego zdaniem poważnym problemem jest to, że w zamówieniach publicznych są pokazywane dane o zamówieniach – co później ułatwia ataki. Ważna jest kryptografia cyfrowa.

Grzegorz Latosiński, Palo Alto

Kupowanie rozwiązań cyberbezpieczeństwa jest trudne. Zanim zbudujemy rozwiązanie to już mamy potencjalnego atakującego. Może warto pomyśleć o standardach kupowania dla infrastruktury krytycznej. Standardy cyberbezpieczeństwa - mamy problem z dostępem do fachowców. Może pozwólmy samorządom korzystać ze standardów wskazujących, co i jak kupować. Jego zdaniem cyberbezpieczeństwo to chmura. Większość rozwiązań cyberbezpieczeństwa korzysta z chmury. Konieczne jest propagowanie dobrych praktyk – jego zdaniem obecnie nie ma możliwości wymiany doświadczenia, które mają poszczególne zespoły cert. Warto ująć wymianę informacji w ustawie.

Kinga Pawłowska-Nojszewska, KIKE

Wskazała, że izba ta zrzesza 30% dostawców internetu w Polsce. Zdaniem KIKE najlepszą drogą jest certyfikacja i dywersyfikacja dostawców. Wyłączenie dostawców w szczególności chińskich temu nie służy. Usunięcie chińskiego sprzętu nie zwiększy cyberbezpieczeństwa. Nowy dostawca może także zostać uznany za dostawcę wysokiego ryzyka. Wskazała, że w mniejszych miejscowościach jest dostępna infrastruktura z wykorzystaniem urządzeń chińskich. KIKE wyraża poparcie dla uwag RPO zgłoszonych do projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Anna Kwaśniewska-Lach, Dynacon

Ważne jest cyberbezpieczeństwo przemysłowe. Istnieje potrzeba doprecyzowania wytycznych dla sektorów i dla poszczególnych działów w firmach.

Piotr Kowalski, PIIT

Zauważył problem papierowego cyberbezpieczeństwa. Regulacje wprost wymieniają wymogi dokumentacji a organy kontrolne wymagają udokumentowania działań, co tworzy problem nadmiernej dokumentacji. W nowej strategii należy ująć sytuację geopolityczną; ważny jest też łańcuch dostaw na poziomie europejskim i krajowym. Należy wprowadzić fundusz odporności cyfrowej przy czym odporność cyfrowa powinna być rozumiana jako dostępność usług.

Michał Hryciuk, ISACA

Zapelował o przyspieszenie prac legislacyjnych projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Projektowane przepisy powinny być maksymalnie zgodne z NIS2. Ponadto należy budować świadomość cyfrową w zarządach firm.

Robert Grochulski, Oracle Polska

Zapelował o zmianę Prawa Zamówień Publicznych i dostosowanie go pod kątem infrastruktury chmurowej.



## Karol Celiński, pentester

Wskazał, że inżynierowie mogliby robić testy penetracyjne dla administracji pro publico bono. Pan spotkał się z odmową pentestów w firmie, która integrowała się z mObywatelom i nie można było pentestować logiki mObywatela.

## Patryk Brożek, Fudosecurity

Zapelował o większe wsparcie szczególnie dla startupów – firmy te nie dostają szans we współpracy z administracją. W USA są programy dla małych firm, a najlepsze startupy dostają kontrakty rządowe. Ponadto apelował o wsparcie polskości, polskich firm.

## Adrian Brodzik

Priorytetem strategii cyberbezpieczeństwa powinna być edukacja. Państwo powinno wspierać portale szerzące wiedzę dot. cyberbezpieczeństwa. Zarekomendował organizację olimpiady cyberbezpieczeństwa. Wniósł o wsparcie edukacji cyberbezpieczeństwa w szkołach.

## Rafał Żukowski, Deloitte

Wniósł o uproszczenie procedur przetargowych. Jest wiele archaicznych zapisów wobec dostawców usług i wymogów. Konieczne jest wsparcie w wymianie wiedzy między resortami bowiem nie wszystkie resorty chcą dzielić się informacją. Zauważył, że trudna będzie współpraca międzynarodowa, jeżeli polskie regulacje cyberbezpieczeństwa będą odmienne od zagranicznych, bowiem regulacji NIS2 będą także wymagać kontrahenci zagraniczni.

## Mateusz Flak

Zapelował, aby nie schodzić z drogi kar w NIS2. Jego zdaniem szefowie SOC mają dobre pomysły, ale dla członków zarządów cyberbezpieczeństwo jest kosztem dlatego konieczne jest zaimplementowanie kar i obostrzeń dla zarządów.

## Wawrzyniec Jakubowski

Wskazał, że brakuje w ustawie KSC rozwiązań analogicznych jak w amerykańskim prawie - Executive order 1395/2020, który dotyczy zabezpieczenia infrastruktury kluczowej od sygnału satelitarnego.

## Adrianna Kilińska

Wskazała, że często zapominamy o bezpieczeństwie danych po ataku. Zwróciła uwagę, że w ZUS wdrożono cyfrowy bunkier.

## Marcin Stoński, Narodowe Archiwum Cyfrowe

Zapelował o urealnienie płac pracowników budżetówki zajmujących się cyberbezpieczeństwem.

## Jarosław Boryń

Brakuje standardów, nie można oczekiwać od informatyka w małej gminie, że będzie wiedział jaki sprzęt kupić. Należy też zadbać o ciągłość projektu finansowanego z cyberbezpiecznego samorządu - jeśli po 2 latach ma być projekt kontynuowany z własnych środków to władze rezygnują z niego.

## Cyprian Gutkowski

W nowelizacji KSC powinna być szerzej zaadresowana kwestia bezpieczeństwa łańcuchów dostaw. Podkreślił, że Fundacja Bezpieczna Cyberprzestrzeń nie wyraża obaw dot. Regulacji postępowania w sprawie uznania za dostawcę wysokiego ryzyka i polecenia zabezpieczającego.



Paweł Kiepuszewski

Wskazał że, nic nie będzie działało jeśli nie będzie prądu. Zwrócił uwagę, że panele fotowoltaiczne nie są aktualizowane i są źródłem cyberzagrożeń. Zaapelował o wsparcie techniczne w usuwaniu podatności.

Stefan Kamiński, KIGEIT

Zaapelował o wprowadzenie certyfikacji sprzętu.

Rafał Górski, Instytut Spraw Obywatelskich

Zauważył, że jeśli mamy mieć strategię inteligentnej cyfryzacji to powinna znaleźć się w niej informacja czego nie będziemy cyfryzować z uwagi na cyberbezpieczeństwo czy infrastrukturę krytyczną.