"TO CO JEST WAŻNE TO USPRAWNIENIE PROCEDUR". NA CO ZWRÓCIĆ UWAGĘ PRZY BUDOWANIU SYSTEMU CYBERBEZPIECZEŃSTWA? [SCF2019]

"Od świata, gdzie duzi zjadają małych przechodzimy do świata, gdzie szybcy zjadają wolniejszych. Tyczy się to również cyberbezpieczeństwa". Debata „Krajowy System Cyberbezpieczeństwa - rola i znaczenie przywództwa strategicznego w efektywnej budowie i zarządzaniu bezpieczną cyberprzestrzenią" zgromadziła przedstawicieli administracji rządowej oraz kluczowych spółek technologicznych i zbrojeniowych. W ramach pierwszej debaty w ramach Strategic Cyber Forum, które obyło się 1 października, debatowano nad kluczowymi kwestiami skutecznego zarządzania cyberprzestrzenią.

Nad problematyką jak powinien wyglądać efektywny system zarządzania bezpieczną cyberprzestrzenią oraz które elementy systemu stanowią najsłabsze ogniwo a także jak powinna wyglądać współpraca biznesu i sektora prywatnego jako integralnego elementu budowy zapory dyskutowali paneliści w trakcie rozmowy moderowanej przez Ireneusza Piecucha:

- **Karol Okoński**– Sekretarz Stanu, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
- **Tomasz Zdzikot**– Sekretarz Stanu, Ministerstwo Obrony Narodowej
- **Dariusz Piotrowski**– VP, Dyrektor Generalny Dell Technologies Polska
- **Sebastian Chwałek**– Wiceprezes Zarządu PGZ
- **Michał Jaworski**– Dyrektor ds. strategii technologicznej, Członek Zarządu Microsoft Sp. z o.o.
- **Juliusz Brzostek**– Dyrektor ds. cyberbezpieczeństwa w NASK

„Cyberbezpieczeństwo to nie tylko i wyłącznie zachowywanie odpowiednich zasad związanych z bezpieczeństwem, ale również potencjalnie wehikuł dla naszego państwa z perspektywy gospodarki" - stwierdził Minister Karol Okoński, udzielając pierwszej wypowiedzi podczas debaty pośród zaproszonych gości. Wskazał również, że umocowanie strategii w Ustawie (o KSC – przyp. red.), pozwala na wyznaczenie celów dla poszczególnych elementów systemu a także pozwoli na ich lepszą realizację. Minister wskazał również na istotną rolę budowania kompetencji i edukacji, która stanowić ma element ochrony przed zagrożeniami. Podkreślił po raz kolejny to na co wcześniej wskazał w wystąpieniu inauguracyjnym Minister Cyfryzacji Marek Zagórski, że należy skupić się w szczególności na najbardziej newralgicznym elemencie systemu – człowieku.

„Jeśli chodzi o cyberbezpieczeństwo to należy podkreślić, że mniej ważna jest organizacja, mniej ważna jest struktura organizacji. To co jest ważne to usprawnienie procedur" - powiedział Minister Karol Okoński.

Wskazał także, że w Polsce „świadomie przyjęliśmy model federacyjny”. Powiedział celowo, nie będzie tworzony jeden centralny punkt zarządzania cyberbezpieczeństwa w Polsce. W jego opinii taki model daje dużą lepszą efektywność, biorąc pod uwagę kompetencję instytucji w naszym kraju. Pozwala on również na skuteczniejsze przekazywanie informacji.

„Chcemy, aby Polska należała do liderów, w obszarze cyberbezpieczeństwa. Zarówno państwo jak i siły zbrojne mają do tego niezbędną determinację” - stwierdził Tomasz Zdzikot, Sekretarz Stanu, Ministerstwo Obrony Narodowej. Ministerstwo, jak wskazał, przygotowało kompleksowy program przygotowania resortu i wojska w celu podniesienia kompetencji w zakresie cyberbezpieczeństwa. Minister określił, że zmiany skupione zostały wokół 4 filarów. Jednym z nich jest kwestia zmian strukturalnych, czyli budowanie struktur i zdolności do obrony w tym zakresie. Dotychczas rozproszenie kompetencji było zbyt duże, dlatego też skondensowaliśmy to w jednym ręku.

Kolejnym jest utworzenie Narodowego Centrum Bezpieczeństwa Cyberprzestenii jako połączenie rozproszonego potencjału. Minister podkreślił również rolę zatwierdzenia koncepcji Wojsk Obrony Cyberprzestrzeni oraz o utworzenia komponentu cyber w Wojskach Obrony Terytorialnej. Dodał, że należy również wskazać na element edukacji i nauki – kierunków, które zostały utworzone na uczelniach jak np. WAT czy akademii Marynarki Wojennej a także niedługo Akademii Wojsk Lądowych. „Zeszliśmy również do poziomu niżej – tworząc licea” wskazał Minister, a także „uruchomiony został pilotażowy program klas partnerskich w szkołach średnich”. Wszystkie te działania w jego opinii mają zwiększać potencjał przygotowania i kompetencji w zakresie cyberbezpieczeństwa. Podkreślił również rolę współpracy międzynarodowej w tym porozumień, które zostały zawarte w ramach NATO na rzecz współpracy w razie wystąpienia incydentów bezpieczeństwa oraz umowę, która została zawarta z rządem Stanów Zjednoczonych.

"Miałem okazje zapoznać się z różnymi przypadkami i modelami jak zbudować system cyberbezpieczeństwa. W Polsce cyberbezpieczeństwo powinno być głównym źródłem budującym polskie PKB. Mamy ku temu predyspozycje"

Wiceprezes Polskiej Grupy Zbrojeniowej, Sebastian Chwałek, wskazał na konieczność przygotowania grupy do odpowiadania na zagrożenia, które płyną z cyberprzestrzeni oraz jednocześnie wymóg wpasowania się w strategię wyznaczoną przez Ministerstwo. Ważnym aspektem, na który zwrócił Wiceprezes jest dostępność potencjału ludzkiego na rynku polskim dla spółek takich jak PGZ. Jak wskazał "mimo dostępności młodych i zdolnych osób na rynku przemysł państwowy może mieć problem z ich pozyskaniem z uwagi na zdolności finansowe”. Jednocześnie podkreślił, że „należy pamiętać, że potencjał buduje się latami". PGZ, jak wskazał Wiceprezes, aby przygotować się na zagrożenia pochodzące z branży cyber, wskazała swoją spółkę QBITT do stworzenia całego środowiska cyberbezpieczeństwa oraz wdrażania nowoczesnych technologii informatycznych oraz innowacji. Podkreślił również rolę nawiązywania współpracy, jak np. z Exatelem, aby podnosić zdolności w tym zakresie.

Punkt widzenia największych spółek technologicznych przedstawili Dariusz Piotrowski reprezentujący DELL oraz Michał Jaworski z Microsoft. Jak podkreślił Michał Jaworski: "celem dzisiejszej naszej obecności tutaj jest konieczność globalnego budowania strategicznej odporności naszego państwa. Wyzwanie nie jest po stronie technicznej ani prawnej – wyzwanie jest po stronie organizacyjnej". Wskazał również, że Microsoft widzi 3 poziomy współpracy, które stara się realizować w każdym państwie w tym Polsce. Pierwszy poziom to strategiczne umowy z rządami, drugi to poziom lokalny - samorządowy, a trzeci to poszczególni klienci. Zdaniem Dyrektora Zarządzającego DELL, Dariusza Piotrowskiego obecnie prowadzone przez polski rząd zmierzają w dobrym kierunku - "działania rządu i ministerstw w ostatnich latach idą w dobrym kierunku - przyciągają potentatów branży cyber do Polski. Pozwala to na transfer technologii, ale również pozyskanie wykwalifikowanej kadry” – stwierdził. Piotrowski podkreślił również kluczową kwestię, która powinna stać u podstaw zmian z

zakresu budowania cyberbezpieczeństwa dla administracji publicznej – finansowanie. Jak wskazał konieczne są również zmiany w zakresie zakupów dokonywanych w sferze publicznej "ustawa w takim kształcie jakim jest teraz, nie promuje kupowania najbardziej bezpiecznych rozwiązań. To są efekty zaszłości z przed lat". Drobne zmiany w prawie, pozwoliłyby w jego opinii na znaczną poprawę bezpieczeństwa.

"Cyberbezpieczeństwo jest jednym z filarów działań NASK. Zależy nam na tym, aby w trakcie pracy realizować cele również Ministerstwa Cyfryzacji" stwierdził Juliusz Brzostek reprezentujący NASK. Ustawa o KSC wskazała NASK jako jeden z kluczowym elementów systemu – stwierdził. Podkreślił również, że Ustawa pozwoliła osadzić działania NASK oraz nawiązanie współpracy z innymi organizacjami, które tworzą cały ekosystem cyberbezpieczeństwa w Polsce. Podkreślił również, że każdego roku rośnie liczba zgłaszanych incydentów, które wpływają do NASK, jednak zauważa duży przełom, jeśli chodzi o wzrost świadomości - choćby poprzez prowadzone debaty czy rozmowy. Instytut, jak podkreślił, wchodzi również w działania, które mają na celu budowanie świadomości w tym zakresie – czy to poprzez prowadzenie portalu informacyjnego, branie udziału w ćwiczeniach krajowych i międzynarodowych, a także co istotne działania edukacyjne pośród uczniów i nauczycieli. Wskazał również na uruchamiane z inicjatywy NASK nowe kierunki studiów uruchamiane obecnie na uczelniach wyższych. NASK, jak wskazał, prowadzi bardzo istotną pracę na rzecz budowania technologii cyberbezpieczeństwa a sam instytut prowadzi bardzo wiele projektów w tym zakresie. Dyrektor wskazał te elementy jako wkład NASK w budowanie płaszczyzny edukacji i wymiany informacji.

"Od świata, gdzie duzi zjadają małych przechodzimy do świata, gdzie szybcy zjadają wolniejszych. Tyczy się to również cyberbezpieczeństwa" - zreasumował Ireneusz Piecuch kończąc pierwszą debatę w ramach Strategic Cyber Forum.

PARTNERZY GŁÓWNI

PGZ · DELL · EY · Microsoft

PATRONAT HONOROWY

Ministerstwo Cyfryzacji · BBN · UKE · RCB

PARTNERZY

EXATEL · NASK · ORACLE · GRUPA WB · PKPCARGO · PIIT

Defence 24 · Energetyka 24 · CyberDefence 24 · Space 24 · InfoSecurity 24