# LUDWISZEWSKI: NAJWAŻNIEJSZY PRIORYTET CYBERBEZPIECZEŃSTWA TO NOWA USTAWA

**To, co powinno być priorytetem Polski w kwestii cyberbezpieczeństwa, to stworzenie podstaw prawnych w formie ustawy. Powinna ona stanowić pierwszy, podstawowy element ram prawnych, określać zasady funkcjonowania systemu cyberbezpieczeństwa. Do dziś nie dorobiliśmy się takiego aktu prawnego. Gdyby ktoś mi zadał pytanie, kto dziś formalnie jest podmiotem wiodącym w zakresie cyberbezpieczeństwa w Polsce, to przyznam szczerze – miałbym problem z odpowiedzią - mówi Marcin Ludwiszewski, Lider obszaru Cyberbezpieczeństwa w Deloitte Polska, współtwórca CERT.GOV.PL**

To, co powinno być priorytetem Polski w kwestii cyberbezpieczeństwa, to stworzenie podstaw prawnych w formie ustawy. Nazwijmy ją roboczo ustawą o cyberbezpieczeństwie. Powinna ona stanowić pierwszy, podstawowy element ram prawnych, określać zasady funkcjonowania systemu cyberbezpieczeństwa, a przede wszystkim wskazywać podmiot wiodący w tym obszarze oraz wskazywać role i odpowiedzialność podmiotów w obszarze publicznym (cywilnym i wojskowym), a także prywatnym. Do dziś nie dorobiliśmy się takiego aktu prawnego.

> *Gdyby ktoś mi zadał pytanie, kto dziś formalnie jest podmiotem wiodącym w zakresie cyberbezpieczeństwa w Polsce, to przyznam szczerze – miałbym problem z odpowiedzią.*
>
> *Marcin Ludwiszewski*

Było wiele prób w przeszłości, które miały na celu usankcjonowanie tej dziedziny. Jeśli jednak spojrzymy całościowo na te inicjatywy, zobaczymy, że były i są one często rozproszone i realizowane na poziomie taktycznym Państwa. Gdyby ktoś mi zadał pytanie, kto dziś formalnie jest podmiotem wiodącym w zakresie cyberbezpieczeństwa w Polsce, to przyznam szczerze – miałbym problem z odpowiedzią.

Mamy bowiem wiele ośrodków – choćby  teraz działania w tej kwestii podjęło Ministerstwo Cyfryzacji. Zmierzają one do określenia kierunków działania resortu również w obszarze cyberbezpieczeństwa. Oprócz tego mamy Strategię Bezpieczeństwa Narodowego oraz Doktrynę Cyberbezpieczeństwa

przygotowane przez Biuro Bezpieczeństwa Narodowego. To są jednak doktryny, nie normy prawne. Dodatkowo jest jednostka Ministerstwa Obrony Narodowej - Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi. Warto też wspomnieć o ustawie o ochronie krytycznej infrastruktury i jej komponencie bezpieczeństwa teleinformatycznego, który stara się uwzględniać w swoich działaniach Rządowe Centrum Bezpieczeństwa.

> *Działania poszczególnych resortów są rozproszone. Potrzeba fundamentu o charakterze strategicznym, który będzie definiował ramy prawne i spójne podejście do cyberbezpieczeństwa.*
>
> *Marcin Ludwiszewski*

Wcześniej mieliśmy inicjatywy typu Polityka ochrony cyberprzestrzeni - przyjęta jako uchwała Rady Ministrów. Na dziś poza wymienionymi ośrodkami mamy wiele taktycznych i operacyjnych rozwiązań w poszczególnych sektorach. Jako przykład można podać projekt dotyczący cyberbezpieczeństwa i funkcjonujący w obrębie Związku Banków Polskich, dzięki któremu istnieje współpraca sektora bankowego np. z Policją nad poszczególnymi sprawami. Dodatkowo, na tym poziomie działa również CERT Polska i wiele sektorowych zespołów reagowania na incydenty (CERT). Te wszystkie działania oceniam bardzo pozytywnie, ale muszą one przyjąć wymiar strategiczny.

Kolejnym istotnym elementem jest również wypracowanie formuły współpracy opartej na zaufaniu, która zachęcałaby obie strony - sektor publiczny i prywatny- do współdziałania tak, aby nie było ono „jednokierunkowe" i jednocześnie dawało korzyści obu stronom (np. w zakresie wymiany informacji o zagrożeniach). Dodatkowo, kierunki działań powinny być wskazywane w wyniku zrozumienia kontekstu zagrożeń RP i powiązanych z nim ryzyk, tak aby działania inwestycyjne odpowiadały priorytetom, a środki publiczne czy też prywatne nie były marnowane.

> *Dyrektywa NIS wprowadza nowe zasady, szczególnie w kwestii krytycznej infrastruktury państwa. To daje nam okazję do rozliczenia się z tym, co już zrobiliśmy, spojrzenia na to, co mamy, i wskazania podmiotu wiodącego, który będzie koordynował te działania.*
>
> *Marcin Ludwiszewski*

Trudno też wyobrazić sobie realizację strategii bezpieczeństwa bez współpracy z dostawcami usług, oprogramowania i urządzeń wspierających obszar cyberbezpieczeństwa. Ustawa o cyberbezpieczeństwie powinna precyzować najwyższe priorytety ochrony państwa, ale również koncentrować się na bezpieczeństwie obywateli, cyfryzacji, kreowaniu i wspomaganiu cyfrowej gospodarki.

W obecnej ekipie rządowej widać wiele entuzjazmu, na przykład w działaniach Ministerstwa Cyfryzacji, RCB, BBN i MON. Jednak działania poszczególnych resortów są rozproszone. Potrzeba fundamentu o charakterze strategicznym, który będzie definiował ramy prawne i spójne podejście do cyberbezpieczeństwa.

Pytanie, przy którym ośrodku władzy powinno powstać centrum decyzyjne, jest pytaniem otwartym. Przede wszystkim spróbujmy wykorzystać szanse, które płyną z nowej dyrektywy NIS. Ta dyrektywa Unii Europejskiej wprowadza nowe zasady, szczególnie w kwestii krytycznej infrastruktury państwa. To daje nam okazję do rozliczenia się z tym, co już zrobiliśmy, spojrzenia na to, co mamy, i wskazanie podmiotu wiodącego, który będzie koordynował te działania. Dyrektywa NIS daje nam podstawy do nowego otwarcia w kwestii cyberbezpieczeństwa. Warto wykorzystać tę okazję.

**Marcin Ludwiszewski:** Lider obszaru Cyberbezpieczeństwa w Deloitte w Polsce, wspiera klientów w zakresie projektowania i wdrażania strategii cyberbezpieczeństwa, a także zarządzania ryzykiem bezpieczeństwa informacji. Zarządzał regionalnym zespołem bezpieczeństwa w Royal Bank of Scotland. Współtwórca Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, pełnił funkcję zastępcy dyrektora Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego, gdzie nadzorował bezpieczeństwo sieci niejawnych.