Stanowisko Rady do Spraw Cyfryzacji dotyczące konieczności systemowego wsparcia cyberbezpieczeństwa sektora naukowo-badawczego w Polsce.

Wraz z rekordowym wzrostem cyberataków na świecie (75% wzrost w III kwartale 2024 vs. 2023 zgodnie z raportem firmy Checkpoint), lawinowo rośnie liczba cyberataków na instytucje akademickie. 50% organizacji, które padły ofiarą naruszeń danych osobowych, badawczych i finansowych, a także ingerencji w działanie sieci i systemów teleinformatycznych to organizacje sektora badań i edukacji (*2024 Data Breach Investigations Report*). **Sektor badań i edukacji jest w tym momencie jednym z najczęściej narażonych na cyberataki**, a dopiero za nim znajdują się sektory: rządowy/wojskowy i sektor opieki zdrowotnej.

1. Z uwagi na stale rosnące znaczenie nowych i przełomowych technologii podwójnego zastosowania i palącą potrzebę zwiększenia innowacyjności państwa, cyberbezpieczeństwo i cyberodporność sektora naukowo-badawczego stają się kluczowym wymiarem bezpieczeństwa gospodarczego i narodowego. Jak wskazują wnioski raportu Boston Consulting Group, z roku na rok rośnie potrzeba coraz intensywniejszej współpracy uczelni i sektora akademickiego z ministerstwami obrony narodowej, polegającej m.in. na angażowaniu ich w rozwój zdolności obronnych i odporności państwa. Ponadto, w budowanie niezbędnych zdolności konieczne jest także zaangażowanie akceleratorów na rzecz innowacji, które często również funkcjonują w ramach uczelni wyższych, bądź w ośrodkach naukowo-badawczych. Z uwagi na rozpoczynający się tzw. “wyścig zbrojeń między Unią Europejską a Federacją Rosyjską”, dodatkowo rośnie konieczność zwiększenia cyberbezpieczeństwa i odporności na ataki, w tym cyberszpiegostwo wymierzone w wysokie technologie.
2. W związku z implementacją dyrektywy NIS2, a także oczekiwanymi obowiązkami, które będą nałożone na sektor badań i edukacji przez nowelizację Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz zaliczenie podmiotów z tego sektora do kategorii podmiotów ważnych, zaś części z nich do kategorii podmiotów kluczowych, konieczne będzie osiągnięcie przez te podmioty w krótkim czasie wysokich standardów w zakresie cyberbezpieczeństwa. Dodatkowo problem cyberzagrożeń sektora naukowo-badawczego podkreślają zalecenia Rady UE z 23 maja 2024 r. *Enhancing Research Security*, które wskazują je jako jedne z kluczowych zagrożeń dla bezpieczeństwa badań naukowych i m.in. wzywają do podjęcia działań zaradczych. Podobne głosy pojawiają się także w związku z trwającymi pracami nad założeniami *Framework Programme 10*, w ramach których podkreślane jest wielowątkowe znaczenie bezpieczeństwa badań naukowych.
3. Rośnie także potrzeba zwiększenia poziomu innowacyjności rozwiązań dla cyberbezpieczeństwa sieci i systemów ICT, który Polska może osiągnąć wyłącznie poprzez uruchomienie odpowiedniego programu badań podstawowych w dyscyplinie naukowej cyberbezpieczeństwo, wraz z badaniami z innych dziedzin, co wynika z

interdyscyplinarnego charakteru cyberbezpieczeństwa. Niewystarczająca liczba projektów w obszarze badań podstawowych skutkuje brakiem badań stosowanych i wdrożeń do przemysłu cyberbezpieczeństwa, który w Polsce wciąż nie jest wystarczająco rozwinięty względem krajów Europy Zachodniej. W opinii Rady ds. Cyfryzacji, jest to działanie konieczne dla zapewnienia cyberbezpieczeństwa w skali całego państwa.

4. Z uwagi na aktualnie stosunkowo niski poziom cyberbezpieczeństwa w sektorze naukowo-badawczym, a także dotychczasowe nieuwzględnienie tego sektora w wysiłkach państwa na rzecz zwiększenia cyberbezpieczeństwa sieci i systemów teleinformatycznych sektora naukowo-badawczego, po stronie polskich uczelni i ośrodków naukowo-badawczych pojawia się istotna luka kompetencji i dostępnych środków finansowych, która uniemożliwia im osiągnięcie oczekiwanego przepisami i adekwatnego do skali zagrożeń poziomu zabezpieczeń.
5. W opinii Rady ds. Cyfryzacji konieczne jest pilne podjęcie wspólnych działań międzyresortowych, zmierzających do systemowego wsparcia cyberbezpieczeństwa sektora naukowo-badawczego. Działania te powinny objąć m.in. przygotowanie Strategii cyberbezpieczeństwa w uczelniach wyższych, a także stworzenie dedykowanego programu **"Cyberbezpieczna Uczelnia"** – jako odrębnego funduszu dla wsparcia uczelni. Wsparcie finansowe z zasady obejmowałoby konieczność alokowania środków wyłącznie na rozwój zdolności, zakup sprzętu i oprogramowania, podnoszących poziom cyberbezpieczeństwa uczelni. Z uwagi na kierunek, w jakim zmierzają regulacje prawne w zakresie cyberbezpieczeństwa, w ramach programu premiowane byłoby tworzenie uczelnianych i regionalnych Security Operations Centers (SOC). Potrzebne jest także przeprowadzenie analizy wykonalności dla stworzenia i udostępnienia podmiotom akademickim **publicznego rozwiązania klasy SIEM**, co znacznie mogłoby wpłynąć na optymalizację wydatków publicznych. Konieczne jest również uwzględnienie uczelni wyższych wśród podmiotów uprawnionych do korzystania ze wsparcia **Funduszu Cyberbezpieczeństwa**, a także przeznaczenie środków finansowych na **wypracowanie kompleksowych wytycznych dla uczelni wyższych w zakresie podniesienia kompetencji w obszarze cyberbezpieczeństwa**. Należy pilne wesprzeć działania, które postuluje projekt nowelizacji UKSC, w tym dot. tworzenia **CSIRT sektorowego do spraw nauki i badań naukowych.**
6. Rada ds. Cyfryzacji postuluje także przygotowanie projektu kształcenia przez uczelnie wyższe społeczeństwa, jak i specjalistów poszukiwanych na rynku cyberbezpieczeństwa - wysoko wykwalifikowanych informatyków, zwłaszcza w obszarach krytycznych, jak sztuczna inteligencja i cyberbezpieczeństwo, co także powinno być wsparte dedykowanym programem finansowania tego typu działań. Jest to w zgodzie z postulatami zawartymi w Apelu i Uchwale Komitetu Informatyki PAN z 10 marca b.r., mówiącymi o potrzebie większych inwestycji "w kształcenie kadr w technologiach

informatycznych. Ponadto, należy wziąć pod uwagę rekomendacje Komitetu Informatyki PAN, m.in. dotyczące ustanowienia[1]:

- przestrzeni do przechowywania danych, z zapewnieniem silnej kontroli dostępu i odporności na zniszczenie i manipulacje, z wykorzystaniem szyfrowania E2E oraz replikacji,
- narzędzi do bezpiecznej edycji materiałów naukowych (wraz z możliwością jednoczesnej edycji, automatyczną korektą językową itp.),
- narzędzi do bezpiecznego przetwarzania danych (np. narzędzia statystyczne),
- narzędzi do bezpiecznej komunikacji (telekonferencje, czat) w trybie szyfrowania E2E.

Zwracamy również uwagę na potrzebę systemowej zmiany w podejściu do ochrony danych naukowych i badawczych o podwójnym zastosowaniu.

7. Rada wspiera działania podejmowane przez Zespół ds. Cyberbezpieczeństwa Konferencji Rektorów Akademickich Szkół Polskich (KRASP) i postuluje stworzenie szerokiej platformy dialogu na temat cyberbezpieczeństwa uczelni wyższych. Rada ds. Cyfryzacji deklaruje swoją gotowość do udziału w dalszej debacie i działaniach KRASP, zmierzających do stworzenia środków i narzędzi wdrożenia cyberbezpieczeństwa w sektorze naukowo-badawczym.
8. Rada postuluje przyśpieszenie procesów legislacyjnych związanych z wdrożeniem dyrektywy NIS2 oraz stworzenia procedur i instytucji odpowiedzialnych za cyberbezpieczeństwo uczelni i placówek naukowo-badawczych, w tym w formule Information Sharing and Analysis Center (ISAC).

Rada postuluje podjęcie kroków zmierzających do zainicjowania działań skutkujących wypracowaniem systemowego wsparcia w zakresie budowy cyberbezpieczeństwa sektora naukowo-badawczego. Jednocześnie, Rada rekomenduje zainicjowanie prac nad stworzeniem sektorowej strategii cyberbezpieczeństwa, poprzez powołanie zespołu ekspertów, którzy w krótkim czasie przygotują rekomendacje dotyczące cyberbezpieczeństwa uczelni wyższych, a także wypracowanie kompleksowych wytycznych dla uczelni wyższych w zakresie podniesienia kompetencji w obszarze cyberbezpieczeństwa.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/

PODPIS ZAUFANY
AGNIESZKA
JANKOWSKA
31.03.2025 14:42:44 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym

[1] https://ki.pan.pl/app/uploads/2024/12/List_otwarty_KI_PAN.pdf;
https://ki.pan.pl/app/uploads/2025/03/Uchwala_2025_01_zalacznik.pdf.