

## JULIAN KING: WZMOCNIENIE UNIJNEJ CYBEROBRONY KLUCZOWE DLA BEZPIECZEŃSTWA

---

Wzmocnienie unijnych struktur cyberobrony jest kluczowe dla wspólnego bezpieczeństwa. Hakerzy nie znają dziś granic, dlatego współpraca międzynarodowa powinna być priorytetem - stwierdził w rozmowie z PAP komisarz ds. unii bezpieczeństwa, sir Julian King.

Zdaniem komisarza, wzrasta różnorodność zagrożeń w cyberprzestrzeni, z którymi przyjdzie się w najbliższym czasie mierzyć zarówno strukturom państwowym, jak i biznesowym. "Cyberataki stają się coraz bardziej wyrafinowane, często łączą się z innymi zagrożeniami w sferze informacyjnej, które motywowane są czysto politycznie" - stwierdził sir Julian King.

Komisarz przypomniał, że 2017 roku odnotowano ponad 4 tys. ataków typu ransomware (szyfrujących komputery za pomocą złośliwego oprogramowania celem wyłudzenia okupu - PAP) dziennie, nie licząc aktywności tzw. trojanów, ataków DDoS (ang. distributed denial of service, polegających na skierowaniu zmasowanego ruchu celem odcięcia dostępu do usługi internetowej - PAP), botnetów, a także rosnącej liczby kradzieży tożsamości, aktywności w dziedzinie inżynierii społecznej, czy wreszcie - prób wywarcia wpływu na procesy demokratyczne.

"Celem cyberprzestępców były banki, instytucje rządowe i infrastruktura krytyczna. Wszystkie one były atakowane tak ze względów politycznych, jak i finansowych. Częstym błędem jest również zainteresowanie bezpieczeństwem struktur IT po fakcie ataku, co najczęściej ma miejsce w szybko rosnącym sektorze Internetu Rzeczy" - powiedział King.

W rozmowie z PAP komisarz wskazał na konieczność wzmocnienia unijnych struktur do spraw cyberobrony, których celem miałyby być wsparcie poszczególnych państw członkowskich, jak i koordynacja współpracy pomiędzy nimi. Zdaniem Kinga, kluczowa jest wymiana informacji pomiędzy państwami członkowskimi a strukturami Wspólnoty, ale też bliższe partnerstwo publiczno-prywatne w zakresie obronności w cyberprzestrzeni, oraz wsparcie finansowe dla badań i rozwoju w dziedzinie.

"W miarę, jak wszystko wokół nas staje się coraz bardziej usieciowione, musimy pilnie podjąć pracę nad wdrożeniem podejścia do bezpieczeństwa, które rozpoczyna się jeszcze na etapie projektowym (ang. security by design). Właśnie tym motywujemy propozycję wspólnych ram certyfikujących na poziomie unijnym, co pozwoli zarówno osobom prywatnym, jak i firmom sprawniej dokonywać oceny odporności na cyberataki produktów i usług, z których korzystają" - powiedział.

King zaznaczył, że wzmocnianie odporności na cyberataki to tylko częściowe rozwiązanie problemu. Jego zdaniem, potrzebne jest również działanie, które zniechęci cyberprzestępców do podejmowania ataków. "Organy ścigania powinny mieć narzędzia właściwe do radzenia sobie z przestępstwami w sieci, oraz mieć łatwy dostęp do materiałów dowodowych w formie cyfrowej. Niebawem zaproponujemy rozwiązania, które będą mogły przyspieszyć proces uzyskiwania takiego dostępu do danych w śledztwach międzynarodowych" - stwierdził.

Komisarz zwrócił również uwagę na problem, jakim jest niedostateczna liczba wyszkolonych w zakresie cyberbezpieczeństwa specjalistów, mogących wspierać działania na rzecz cyberobronności. Odniósł się także do dalszych zmian w prawie, które mają na celu wzmocnienie roli istniejących instytucji unijnych (takich jak agencja bezpieczeństwa informacyjnego ENISA, która po zmianach miałaby przekształcić się w Europejską Agencję Cyberbezpieczeństwa). Zdaniem Kinga, główną rolą tej instytucji powinno być wspieranie państw członkowskich w zakresie rozwijania ich zdolności do cyberobrony, a także wdrażanie dyrektywy NIS (dotyczącej bezpieczeństwa sieci i systemów informacyjnych - PAP). "Agencja powinna także odgrywać ważną rolę w procesie certyfikacji i być w przyszłości ważnym partnerem dla Europolu" - dodał.

"Musimy więcej inwestować w rozwój umiejętności i kompetencji technologicznych" - powiedział PAP komisarz ds. unii bezpieczeństwa. "Europa stoi obecnie przed deficytem specjalistów z dziedziny cyberbezpieczeństwa, który do 2022 roku może osiągnąć rozmiary 350 tys. brakujących osób" - stwierdził King. "Baza ekspertów i specjalistów jest niezwykle ważną sprawą w procesie budowy zdolności obronnych. Sprawy cyberprzestrzeni muszą być priorytetyzowane w programach nauczania i w kształceniu zawodowym. Musimy się upewnić, że Unia Europejska będzie zdolna utrzymać swoje możliwości w zakresie zapewnienia bezpieczeństwa dla cyfrowej ekonomii, infrastruktury, a także społeczeństwa i demokracji" - dodał komisarz King.