aut. Adam Lelonek 12.10.2017

JULIAN KING: SĄ PAŃSTWA, KTÓRE WYKORZYSTUJĄ SFERĘ CYBER DO ATAKÓW NA DEMOKRACJĘ (CYBERSEC 2017)

9 października w Krakowie podczas III Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2017 wystąpił komisarz ds. unii bezpieczeństwa sir Julian King. Tytuł jego wystąpienia to „Rzucenie światła na krajobraz zagrożeń cybernetycznych w Europie".

„W dobie Internetu jesteśmy coraz bardziej zależni od technologii na nim opartych, ale i staliśmy się bardziej podatni wobec tych, którzy są gotowi wykorzystywać te technologie aby próbować lub czynić nam szkody z powodów finansowych lub politycznych. Stajemy się coraz bardziej podatni na ryzyka w cyberprzestrzeni. Przykłady WannaCry i NotPetya są dosyć wymowne. To poważne ostrzeżenie dla rozumienia zagrożeń. Bezpieczeństwo online jest równie ważne jak offline. W darknecie można zlecić atak już za 5 USD" – powiedział komisarz.

> *Zagrożenia cybernetyczne są wśród głównych problemów dla 9 na 10 obywateli Unii Europejskiej. W darknecie można zlecić atak już za 5 USD.*
>
> *sir Julian King*

Dla przestępców, aktorów państwowych i niepaństwowych, życie nigdy jeszcze nie było tak łatwe. Tylko w 2016 roku Europejczycy padli ofiarą 2 mld naruszeń danych, a każdego miesiąca jeden z pięciu komputerów w przedsiębiorstwach został zaatakowany. Od 2016 r. miały miejsce ponad 4 tys. ataków ransomware każdego dnia. W porównaniu z 2015 r. – w 2016 odnotowaliśmy ich wzrost o 300%. Systemy lotnicze są atakowane średnio 1 tys. razy w miesiącu, a koszty przestępstw finansowych wynoszą 1 mld EUR tylko w państwach strefy euro. To pokazuje, jak szerokim instrumentarium dysponują aktorzy nie państwowi.

Wspomniał on, że Unia Europejska ma swoją strategię w tym obszarze od 2013 r. jednak biorąc pod

uwagę ewolucję zagrożeń, jest to już historia antyczna. Skala ataków to jest już endemiczna. UE chce wzmocnić obronność, zwiększyć wykrywalność oraz przygotować skuteczny system cyberobrony. Potrzebny jest do tego rozwój technologii, ale i zaawansowanie współpracy międzynarodowej państw członkowskich. Z kolei wyzwaniem jest to, że zagrożenia dynamicznie się modyfikują, ewoluują – pod względem swojej natury, ale i skali oddziaływania. „Chodzi już nie tylko o urządzenia elektronicznie, ale nasze domy, szpitale, infrastrukturę krytyczną, w tym elektrownie – na Ukrainie 600 tys. mieszkań nie miało prądu w zeszłym roku po ataku cybernetycznym" – stwierdził komisarz. Wspomniał on również, że według firmy Symantec grupa hakerów o nazwie Dragonfly wciąż ma potencjalnie możliwość sabotowania europejskich systemów energetycznych.

„Setki tysiące nowych urządzeń każdego roku pojawiają się na rynku, stają się częścią systemu, ale i padają ofiarami hakerów lub stają się botami. Wiele przedsiębiorstw, instytucji i prywatnych użytkowników nie przywiązują uwagi do kwestii bezpieczeństwa. Cyberbezpieczeństwo to już kwestia strategiczna, mogąca zakłócić funkcjonowanie państw. Dlatego też Komisja Europejska pracuje nad nowymi rozwiązaniami opartymi na 3 filarach: odporność (Resilience), odstraszanie (Deterrence) i obrona (Defence)" – dodał King.

W jego ocenie musimy stać się bardziej odporni, trudniejsi do zaatakowania i szybsi w odpowiedzi. Podkreślił on, iż Agencja UE ds. Bezpieczeństwa Cybernetycznego (EU Cybersecurity Agency), która została powołana w oparciu o istniejącą już Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (European Union Agency for Network and Information Security, ENISA) ma odpowiadać za koordynację i szybką, unijną odpowiedź na zagrożenia, przygotowanie nowych zaleceń i rekomendacji. W tym także i te już do etapu produkcji urządzeń, z zaleceniami dla producentów, aby na rynek trafiały produkty niepodatne na ataki, mające dostęp do aktualizacji.

Jak zauważył King: „Trzeba wzmocnić sferę energetyki czy transportu publicznego, które często mają różne regulacje w różnych państwach i mogą opierać się na rozwiązaniach odbiegających od najwyższych standardów, chociażby liczniki elektryczne w Wielkiej Brytanii i Francji".

> *95% ataków jest możliwa przez błędy ludzi. Cyberbezpieczeństwo zaczyna się w domu z higieną cybernetyczną, budowaniem bezpiecznych zwyczajów, to jest związane z edukacją. Odporność to właśnie wiedza i umiejętności. UE ma lukę w umiejętnościach – brakuje specjalistów. Do 2022 r. szacujemy, że będzie nam brakować 300 tys. specjalistów. Trzeba zainwestować w przygotowanie ekspertów. Wiele firm z sektora cyber polega na pracownikach spoza UE. Trzeba to zmienić. Do 2022 roku zostanie zainwestowane 1,8 mld euro, aby to zmienić, jednak trzeba zrobić jeszcze więcej.*
>
> *sir Julian King*

Zachód musi szybciej i lepiej odpowiadać – ataki z ostatnich lat pokazują, że trzeba szeroko współdziałać, potrzeba reakcji i działania różnych podmiotów, aby przeciwdziałać i reagować. W kwestii odstraszania niezwykle ważne będą zmiany systemów prawnych – kary dla aktorów państwowych, pozapaństwowych i innych. Mechanizm powinien być prosty: namierzenie, identyfikacja i skazanie. Na chwilę obecną jednak 90% śledztw z obszaru cyber ma problem z identyfikacją atakującego. Praca nad „dowodami cyfrowymi" (Digital Evidence) wymaga nowych rozwiązań, zwłaszcza pod kątem radzenia sobie z terroryzmem, cyberatakami i cyberprzestępstwami.

Komisarz zwrócił też uwagę, iż w całym procesie chodzi nie tylko kwestie finansowe, ale i polityczne.

> *Są aktorzy państwowi, którzy wykorzystują sferę cyber do podważania demokracji i jej instytucji, atakują państwa członkowskie, rozsiewają propagandę.*
>
> *sir Julian King*

Sfera cyber jest pełna wyzwań. Nowy Europejski Fundusz Obronny (European Defence Fund) ma też m.in. rozwinąć zdolności na odcinku cybernetycznym. Ponadto UE chce, aby prawo międzynarodowe obowiązywało w sferze cyber, aby była harmonizacja przepisów na poziomie międzynarodowym. Co więcej, Unia, zgodnie z zapewnieniami Kinga, będzie blisko współpracować z NATO na odcinku cyberobrony oraz cyberbezpieczeństwa.

Czytaj więcej: Zbrojeniówka w centrum polityki przemysłowej UE