Cyberdefence 24

aut. Adam Lelonek 02.11.2017

NOWE REGULACJE UE POZWOLĄ KRAJOM CZŁONKOWSKIM NA UZNANIE CYBERATAKU ZA AKT WOJNY

Nowe ramy prawne opracowywane przez Unię Europejską mają „w poważnych okolicznościach" umożliwić kwalifikację cyberataku ze strony wrogich podmiotów jako aktu wojny. Będzie to tożsame z usankcjonowaniem odpowiedzi na atak z wykorzystaniem broni konwencjonalnej.

W połowie września Rada Europejska postanowiła rozwijać ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne (Joint EU Diplomatic Response to Malicious Cyber Activities), czyli zestaw narzędzi dla dyplomacji cyfrowej. Mają być one mocnym środkiem odstraszania przeciwko państwom znanym ze swojej działalności prowadzenia ofensywnych operacji cybernetycznych, takich jak Rosja czy Korea Północna.

Jak głosi oficjalny komunikat prasowy w tej sprawie: „UE uznaje, że cyberprzestrzeń oferuje znaczne możliwości, ale stawia także stale zmieniające się wyzwania przed politykami zewnętrznymi UE. Ponadto UE jest zaniepokojona rosnącą zdolnością i gotowością podmiotów państwowych i niepaństwowych do realizowania swoich celów za pomocą szkodliwych działań cybernetycznych. Działania takie mogą być w świetle prawa międzynarodowego aktami bezprawnymi i skutkować wspólną unijną reakcją dyplomatyczną. UE przypomina, że państwa nie powinny świadomie dopuszczać do wykorzystywania swojego terytorium do działań, które są bezprawne w świetle prawa międzynarodowego i opierają się na technologiach informacyjnych i komunikacyjnych (ICT). Ramy wspólnej unijnej reakcji dyplomatycznej są częścią szerszego podejścia UE do dyplomacji elektronicznej, które pomaga zapobiegać konfliktom, zmniejszać zagrożenia dla bezpieczeństwa cybernetycznego oraz zwiększać stabilność w stosunkach międzynarodowych. Ramy mają zachęcać do współpracy, ułatwiać łagodzenie bezpośrednich i długoterminowych zagrożeń oraz długofalowo wpływać na zachowanie potencjalnych agresorów".

W tym samym czasie planami działań w tej sprawie zajęła się również Komisja Europejska.

Czytaj więcej: Plan skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych

Jak wynika z najnowszych, nieoficjalnych informacji, nowe zapisy mają dać zaatakowanym państwom członkowskim nie tylko możliwość obrony w ramach istniejących rozwiązań wynikających z prawa

międzynarodowego, ale także upoważnić je do wsparcia UE i rządów jej państw członkowskich zgodnie z paragrafem 7 Artykułu 42 Traktatu o Unii Europejskiej. Chodzić tu będzie także o presję dyplomatyczną, publiczne potępienie oraz sankcje.

> *W przypadku gdy jakiekolwiek Państwo Członkowskie stanie się ofiarą zbrojnej agresji na jego terytorium, pozostałe Państwa Członkowskie mają w stosunku do niego obowiązek udzielenia pomocy i wsparcia przy zastosowaniu wszelkich dostępnych im środków, zgodnie z artykułem 51 Karty Narodów Zjednoczonych. Nie ma to wpływu na szczególny charakter polityki bezpieczeństwa i obrony niektórych Państw Członkowskich.*
>
> *Art. 42, § 7 TUE*

Jak informuje The Telegraph, dokument nie będzie precyzyjnie definiował limitów dla koordynacji czy działań wspierających. Wspomina się tylko, że sama Unia Europejska nie będzie mogła wypowiedzieć wojny. Anonimowy informator przekazał brytyjskiej gazecie natomiast, iż jednym z głównych celów nowych regulacji ma być odstraszanie - potencjalny atakujący ma być mniej skłonny do wrogich działań, znając ich aktualne konsekwencje, a strategia odpowiedzi na ataki ma pokazać, jak Unia poważnie podchodzi do cyberzagrożeń.

W zeszłym tygodniu Minister ds. bezpieczeństwa narodowego Wielkiej Brytanii Ben Wallace poinformował, że nie ma wątpliwości, iż za atakiem WannaCry stała Korea Północna. Wcześniej świat obiegła informacja, iż niezidentyfikowana grupa hakerów znana jako Dragonfly atakowała i weryfikowała systemy zabezpieczeń w amerykańskim sektorze energetycznym. Pokazuje to także, jak poważnym wyzwaniem pozostaje kwestia atrybucji ataku.

Czytaj więcej: USA: zwiększone zagrożenie atakami hakerskimi w przemyśle i energetyce

Eksperci podkreślają, że to nowy, ważny krok na poziomie międzynarodowym. Unia Europejska podąża drogą rozpoczętą przez NATO i wysyła jasny sygnał, że wrogie działania w cyberprzestrzeni będą rozpatrywane podobnie do ataku konwencjonalnego. Wszystko wskazuje na to, iż UE i NATO zacieśniają współpracę w tym obszarze. Połączenie potencjałów 28 krajów członkowskich w tej sferze, systemów ochrony prawnej oraz sił specjalnych może diametralnie zwiększyć poziom cyberbezpieczeństwa. Wielu pozostaje jednak sceptycznych odnośnie możliwości odstraszenia od wrogich działań Korei Północnej. Pozostaje też pytanie o działalność aktorów niepaństwowych, którzy

są coraz częściej wykorzystywani przez rządy i służby specjalne.