aut. Szymon Palczewski 09.08.2019

CYBERODSTRASZANIE TO MIT. WIRTUALNA BROŃ SŁUŻY DO INNYCH CELÓW

Współcześnie cały świat jest zaangażowany w dyskusję na temat cyberataków. Pojawiają się pytania, czy należy uznać je za akt wojny i czy można w odpowiedzi na incydent użyć konwencjonalnych sił zbrojnych. Pentagon w 2011 roku odpowiedział stanowczo: tak. Sytuacja jednak nie jest taka prosta.

„Bardzo łatwo jest wypowiedzieć takie słowa, jednak robi się coś innego" – powiedział dyrektor firmy zajmującej się cyberbezpieczeństwem F-Secure Mikko Hypponen podczas konferencji Black Hat USA. W przytoczonej przez serwis Fifthdomain wypowiedzi ekspert stwierdził, że największym problemem w kontekście cyberataków jest ich atrybucja. Źródło incydentu, zwłaszcza jeśli odpowiada za niego aktor państwowy, nie jest łatwe do ustalenia. W związku z tym odpowiedź za pomocą konwencjonalnych środków jest bardzo ryzykowna.

„Skąd właściwie wiadomo, kto jest jego (przyp. red. cyberataku) autorem? A jeśli twój wróg wie, że zareagujesz konwencjonalnymi siłami, będzie starał się maskować swoje działania" – stwierdził Mikko Hypponen, cytowany przez Fifthdomain. – „Wówczas podejmie wszelkie środki, aby wykryty cyberatak sprawiał wrażenie, że pochodzi od kogoś innego".

W tym miejscu specjalista posłużył się przykładem Rosji. Zaznaczył, że hakerzy tego państwa wykorzystują chińską wersję Microsoft Word do przeprowadzania złośliwych kampanii. Według Mikko Hypponena cyberbroń staje się powoli bronią idealną – „Jest tania i skuteczna".

Jak wskazuje Fifthdomain, sposób reakcji na cyberatak może być różny w zależności od danego państwa. Przedstawiciel F-Secure przytoczył przykład izraelskiego nalotu na budynek, w którym rzekomo mieściła się siedziba hakerów Hamasu. „W tym przypadku Izraelczycy jednak wiedzieli dokładnie z kim walczą. Mieli wystarczającą wiedzę na temat miejsca, skąd fizycznie pochodzą cyberataki. Jednak w większości przypadków tak nie jest" – wyjaśnił Mikko Hypponen.

Według eksperta hakerzy posiadają wiele sposób na to, aby ukryć źródło incydentu, dlatego też uważa, że nie należy używać konwencjonalnych sił i środków w odpowiedzi na cyberatak – informuje Fifthdomain. Wyjątek stanowi otwarty konflikt, w którym od początku wiadomo, kto w nim uczestniczy i kogo uznaje się za wroga.

Cyberodstraszanie to mit

Odstraszanie może być skuteczne w przypadku broni nuklearnej. Wiadomo kto i ile posiada głowic oraz jakie są możliwe środki ich przenoszenia. Inaczej jest w cyberprzestrzeni. O podatnościach, lukach lub słabościach zabezpieczeń wiedzą jedynie hakerzy, dlatego też państwa nie znają w stu procentach siły i możliwości swoich wrogów.

„Cyberbroń, jak dotąd, nie miała siły odstraszającej, ponieważ nie wiadomo, kto co ma. A więc nie ma

siły odstraszającej broń, o której nikt nic nie wie. Kiedy inwestujesz miliony w tego typu broń, nikt nie wie, że ją masz”” – zaznaczył Mikko Hypponen. Według specjalisty cyberbroń szybko staje się przestarzała ze względu na nieustanny rozwój technologii. „Działają tylko przez ograniczony czas. Potem stają się bezużyteczne i trzeba się ich pozbyć” – wskazał specjalista. Kontynuując swą wypowiedzieć zaznaczył, że tylko jedno jest pewne – „Wszystkie bogate kraje rozwijają swoją cyberobronę oraz ofensywne zdolności w cyberprzestrzeni. Wszyscy tak robią”.