**aut. Szymon Palczewski** 19.07.2019

# NOWE ĆWICZENIA USCYBERCOM. CELEM PORTY MORSKIE

W ubiegłym miesiącu U.S. Cyber Command przeprowadziło symulację cyberataku wymierzonego w jeden z portów morskich. Wojskowi specjaliści z zakresu cyberbezpieczeństwa musieli poradzić sobie z działaniami hakerów wykorzystujących złośliwe oprogramowanie do zainfekowania sieci ośrodka handlowego o krytycznym znaczeniu.

Była to najnowsza edycja corocznego ćwiczenia „Cyber Flag", którego celem jest nauczenie personelu jak lepiej bronić przed cyberatakami wymierzonymi w infrastrukturę krytyczną.

Scenariusz zakończonego testu zakładał blokadę zdolności portu do rozładunku i przemieszczania towarów. Taka sytuacja może negatywnie wpłynąć na handel międzynarodowy. Dowództwo chciało w ten sposób sprawdzić swoją gotowość na tego typu cyberatak i znaleźć potencjalne luki, tak aby w przyszłości podnieść efektywność działania.

„Symulacja ma na celu sprawdzenie zdolności grupy i jej zdolności do współpracy w celu osiągnięcia najlepszych wyników prowadzonej misji" - podkreślił adm. John Mauger, odpowiedzialny za szkolenie w USCYBERCOM.

Według informacji Pentagonu ponad 650 specjalistów z zakresu cyberbezpieczeństwa, w tym przedstawicieli m.in. Cyber Mission Force, Marine Corps, państw sojuszniczych (FiveEyes), FBI czy Departamentu Bezpieczeństwa Wewnętrznego, zostało podzielonych na 20 zespołów. W ćwiczenie zaangażowane były również podmioty sektora prywatnego.

Około 100 ekspertów wcieliło się w rolę hakerów. Zgodnie ze scenariuszem cyberprzestępcy wykorzystali do ataku złośliwe oprogramowanie, aby za jego pomocą uruchomić określone operacje w wewnętrznych sieciach portu. Celem hakerów było sparaliżowanie możliwości rozładunku oraz transportu towarów.

Obecnie transport morski stają się popularnym celem cyberatków. Największa na świecie firma żeglugowa Maersk padła ofiarą wirusa NotPetya. W wyniku incydentu koncern utracił około 4000 serwerów, 45 000 komputerów oraz poniósł ogromne straty finansowe. To jedynie jeden z przykładów działalności hakerów wymierzonej w ten sektor.

Jak wskazuje  John Mauger, tegoroczna edycja „Cyber Flag" koncentrowała się na tzw, „polowaniu na przeciwników", zamiast skupiać się wyłącznie na ochronie zasobów. „Ze względu na możliwości, jakimi dysponują, chcemy być specjalistami w znajdywaniu przeciwnika" – wskazał przedstawiciel USCYBERCOM.

Tegoroczne ćwiczenie nie naśladowało działań żadnego konkretnego przeciwnika, jak to ma często miejsce. Zespoły wcielające się w rolę atakujących były skupione przede wszystkim na

cyberszpiegostwie oraz spowodowaniu zakłóceń w funkcjonowaniu portu. Miało to wywołać reakcję drugiej strony, która powinna wykryć zagrożenie, a następnie znaleźć i zneutralizować przeciwnika.