Cyberdefence 24

aut. Szymon Palczewski 11.01.2019

US NAVY WZMOCNI CYBERBEZPIECZEŃSTWO. PIERWSZYM KROKIEM WSPARCIE BADAŃ

Jak podaje Naval Air Systems Command, US Navy planuje wesprzeć badania w 36 obszarach, które mogą przyczynić się do poprawy bezpieczeństwa systemów uzbrojenia oraz ich odporności na cyberataki.

Bryson Bort, dyrektor generalny Scythe, stwierdził, że nie są to nowatorskie badania, ale „jest to pierwszy krok w kierunku kontroli jakości cyberbezpieczeństwa, który powinien był już zostać zrobiony" znacznie wcześniej.

Raporty Departamentu Obrony wskazują, że amerykańscy wojskowi nieustannie są nękani cyberatakami. W grudniu opublikowano informacje, że pracownicy Pentagonu nie podejmowali podstawowych kroków cyberbezpieczeństwa w celu ochrony kluczowych systemów, w tym odpowiedzialnych za rakiety balistyczne.

Broń będąca w dyspozycji Departamentu Obrony jest warta około 1,66 bilionów dolarów. Jednak jak wskazuje październikowy raport opracowany przez Government Accountability Office „prawie wszystkie" amerykańskie pociski, odrzutowce, okręty oraz inne elementy wyposażenia armii są podane na cyberataki.

US Navy zainteresowana jest badaniami nad „dynamiczną rekonfiguracją", czyli zmianami funkcjonowania routerów, list kontroli dostępu, parametrów systemy wykrywania włamań oraz reguł analizy wirtualnych zapór. Jak tłumaczą specjaliści National Institute of Standards and Technology – „Organizacje przeprowadzają dynamiczną rekonfigurację systemów informatycznych, na przykład, aby zatrzymać ataki, przekierować atakujących i wyizolować komponenty systemów, ograniczając w ten sposób zakres szkód spowodowanych naruszeniami".

Badania przeprowadzone przez Christiana Johnsona z University of Maryland udowodniły, że łącząc analizę predykcyjną z dynamiczną taktyką rekonfiguracji powstaje nowe podejście, które może doprowadzić do " rozwoju modeli uczenia się, które identyfikują określone rodzaje szkodliwego oprogramowania, takie jak na przykład oprogramowanie ransomware".

US Navy chce również skupić na większym zrozumieniu istoty cyberoszustw, aby w ten sposób móc lepiej zabezpieczyć swoje systemy przed tego typu działaniami. Według specjalistów Advanced Research Project, stosowanie oszukańczego oprogramowania oraz sprzętu w zakresie cyberbezpieczeństwa „jest wciąż w powijakach". Jak tłumaczą – „W wielu technikach brakuje rygorystycznych mierników skuteczności (…)informacje są niewystarczające do określenia, w jaki sposób defensywne oszustwo zmienia zachowanie napastnika".

US Navy rozpoczęła wdrażanie sztucznej inteligencji (AI) od powstania projektu Cyber Awakening Task Force w 2015 roku. Jak powiedział w 2002 roku Danelle Barrett, dyrektor ds. cyberbezpieczeństwa w

Defense Systems – „Widzimy, że im bardziej automatyzujemy nasze sieci, tym lepiej. Nasze mózgi nie mają zdolności intelektualnej do przetwarzania wszystkich tych informacji”.

Z kolei Ed Devinney, dyrektor ds. partnerstwa korporacyjnego, powiedział, że „rośnie zrozumienie i konsensus, że musimy działać z prędkością maszyny. Zwłaszcza, gdy mówimy o aktywnej obronie sieci”. Podsumowując wątek zaznaczył – „wszyscy lubią posługiwać się zwrotem <<sztuczna inteligencja>>, jednak nie ma zbyt wielu osób, którzy dobrze sobie radzą z AI”.