aut. Szymon Palczewski 17.01.2020

HACK THE ARMY 2.0. ETYCZNI HAKERZY WZMACNIAJĄ SYSTEMY U.S. ARMY

Etyczni hakerzy wykryli luki oraz podatności w sieciach oraz systemach U.S. Army, które mogłyby zostać wykorzystane przez wrogów w celu sparaliżowania amerykańskich sił zbrojnych. Departament Obrony USA docenił wysiłki specjalistów, nagradzając najlepszych wysokimi nagrodami pieniężnymi. Zaangażowanie etycznych hakerów staje się stałym elementem, który Pentagon wykorzystuje do budowy nowej jakości cyberbezpieczeństwa.

W okresie od 9 października do 15 listopada 2019 roku w ramach wydarzenia „Hack the Army 2.0" sieci i systemy U.S. Army były poddane cyberatakom przeprowadzonym przez 52 hakerów – informuje serwis Business Wire. Według Departamentu Obrony USA (DoD) walka z hakerami nie jest niczym złym, a wręcz przeciwnie pozwala umocnić lub usprawnić narzędzia wykorzystywane do zapewnienia cyberbezpieczeństwa Stanów Zjednoczonych. Dlatego takie wydarzenia, jak druga edycja „Hack the Army" są korzystne z punktu widzenia rozwoju amerykańskich struktur wojskowych.

Najnowsza odsłona inicjatywy została zorganizowana przez Departament Obrony USA wraz z Defense Digital Service oraz platformą HackerOne. Główną ideą wydarzenia była możliwość odkrywania luk oraz błędów, które mogłyby w rzeczywistych warunkach wywołać ogromne zniszczenia oraz paraliż U.S. Army.

Według informacji zdobytych przez Forbes, podczas licznych symulacji zidentyfikowano 146 luk. Etycznym hakerom udostępniono ponad 60 różnego rodzajów zasobów, wykorzystywanych lub obsługiwanych przez siły zbrojne, w tym między innymi witryny internetowe „army.mil".

W wydarzeniu wzięło udział 52 hakerów z różnych stron świata, w tym Stanów Zjednoczonych, Kanady, Niemiec, Portugalii, Holandii czy Rumunii. Na nagrody dla najlepszych hakerów U.S. Army przeznaczyło pulę 275 000 USD, przy czym najwyższa indywidualna nagroda pieniężna wyniosła 20 000 USD – donosi Business Wire.

„Zaangażowanie hakerów ma kluczowe znaczenie dla wsparcia Departamentu Obrony USA we wzmacnianiu najlepszych praktyk cyberbezpieczeństwa, aby osiągnąć możliwie najwyższy poziom zabezpieczeń" – podkreślił ekspert DoD Alex Romero, cytowany przez Forbes.

Największą ilość nieprawidłowości oraz podatności w sieciach i systemach amerykańskiej armii odkryła Alyssa Herrera, specjalistka zajmująca się sprawami bezpieczeństwa aplikacji internetowych. W całym cyklu zmagań zajęła drugie miejsce, lecz pomimo braku zwycięstwa czuła ogromną radość i satysfakcję, że mogła pomóc U.S. Army w budowaniu lepszej jakości cyberbezpieczeństwa. „To ekscytujące wiedzieć, że słabości, które znajduję, mają na celu wzmocnienie armii" – podkreśliła laureatka „Hack the Army 2.0" na łamach Business Wire.

Inicjatywa organizowana przez Departament Obrony USA realnie przyczynia się do podnoszenia

poziomu cyberbezpieczeństwa amerykańskiej armii. Działalność etycznych hakerów pozwala U.S. Army zidentyfikować krytyczne luki oraz podatności, które mogłyby zostać wykorzystane przez przeciwnika, zwłaszcza w przypadku eskalacji napięcia. Należy mieć nadzieję, że wydarzenie będzie miało kolejne edycje w przyszłości.

Czytaj też: Amerykanie sprecyzowali zadania USCYBERCOM