

SIECI PENTAGONU NICZYM SZWAJCARSKI SER. ETYCZNI HAKERZY UJAWNILI FAKTY

Etyczni hakerzy wykryli łącznie 238 luk w zabezpieczeniach infrastruktury informatycznej Pentagonu. Z tej liczby aż 102 uznano za krytyczne lub stanowiące wysokie ryzyko dla bezpieczeństwa narodowego USA.

Luki zostały wykryte podczas zawodów hakerskich „Hack the Army 3.0”, które rozpoczęły się w styczniu br. i trwały sześć tygodni. Udział w nich wzięło łącznie 40 „najwyżej klasy specjalistów, zarówno z sektora wojskowego, jak i podmiotów cywilnych” – wskazuje firma HackerOne, będąca jednym z organizatorów wydarzenia. Dla zwycięzców przeznaczono pulę nagród o wartości ponad 150 tys. dolarów

W czasie rywalizacji zadaniem ekspertów było zidentyfikowanie podatności w infrastrukturze informatycznej Pentagonu. Jak ustalono po zakończeniu zawodów, uczestnikom udało się wykryć łącznie 238 luk w zabezpieczeniach, z czego 102 zostały ocenione jako krytyczne lub o wysokim znaczeniu. Wymagały one natychmiastowej reakcji i likwidacji.

Trzecia edycja „Hack the Army” wpisuje się w szerszą strategię Departamentu Obrony USA mającą na celu wykrywanie i neutralizowanie cyberzagrożeń, które stanowią ryzyko dla bezpieczeństwa narodowego Stanów Zjednoczonych.

HackerOne

Głównym przedmiotem zmagania uczestników najnowszej edycji zawodów było kilkanaście domen istotnych z punktu widzenia sił zbrojnych USA, a także usługi przeznaczone do logowania i/lub uwierzytelniania. Jednym z celów stanowiły witryny z adresem: „.army.mil”.

Na naszym portalu [wskazywaliśmy](#), że cykl zawodów hakerskich rozpoczął się pod koniec 2016 roku, kiedy to z powodzeniem udało się uruchomić flagowy projekt Departamentu Obrony USA (DoD) „Hack the Pentagon bug bounty”. Stworzona przez amerykańską Defense Digital Service (DDS) inicjatywa miała z założenia pomóc Pentagonowi oraz siłom zbrojnym USA w przeprowadzaniu skutecznej oceny cyberbezpieczeństwa sieci i systemów.

Przypomnijmy, że w pierwszej edycji „Hack the Army” wzięło udział 371 etycznych hakerów. Wśród nich znalazło się 25 specjalistów działających na zlecenie rządu oraz 17 związanych z wojskiem. W efekcie wydarzenie to pozwoliło zidentyfikować, a następnie zlikwidować 118 luk w amerykańskich

zabezpieczeniach. Najlepsi hakerzy otrzymali około 100 tys. dolarów za swoje osiągnięcia.

Po sukcesie pierwszej edycji pod koniec 2019 roku zorganizowano kolejną – „[Hack The Army 2.0](#)”. Udział w niej wzięło 52 specjalistów z sześciu krajów, którzy finalnie znaleźli 146 luki w publicznie dostępnych witrynach armii USA. Nagroda dla najlepszych została ponad dwukrotnie zwiększona względem poprzedniej edycji i wyniosła 275 tys. dolarów.

Czytaj też: [Cyberwojna narzędziem polityki. Potęga tkwi w informacji](#)

