USA BUDUJE PIERWSZĄ JEDNOSTKĘ CYBEROCHOTNIKÓW

Pierwsza jednostka cybernetycznych ochotników będzie funkcjonować w amerykańskim stanie Ohio. Ich zadaniem będzie neutralizacja cyberataków i przywracanie działania usług publicznych, jeśli sieci komputerowe padną ofiarą hakerów – podała agencja Bloomberga.

Agencja przypomniała, że na terenie stanu cyberprzestępcy zakłócili już w przeszłości funkcjonowanie lotniska, doprowadzili do wyłączenia telefonu informacyjno-pomocowego podczas zamieci śnieżnych oraz czasowo odcięli dostęp do akt policyjnych.

Nową taktyką obrony sieci ma być oddział cyberżołnierzy ochotników, który rozpocznie służbę na początku 2020 r. Mają być swego rodzaju lotną jednostką, pomagającą lokalnym władzom, gdy te zgłoszą atak na swoje systemy komputerowe. Ich podstawowym zadaniem będzie jak najszybsze przywrócenie normalnego funkcjonowania sieci i umożliwienie świadczenia usług w zwykłym trybie.

Działająca z ramienia władz Ohio jednostka specjalistów od zabezpieczeń ma być też pomocą dla władz miast, szkół czy lotnisk, które często nie mogą sobie pozwolić na dedykowany zespół cyberbezpieczeństwa lub nie mają tak wysokiej wiedzy technicznej.

Pomysł wzorowany jest na podobnym oddziale funkcjonującym w Michigan. Władze Ohio przyrównują metodę ich funkcjonowania do ochotniczej straży pożarnej. Dotychczas zgłosiło ok. 60 ochotników. Stan planuje przeznaczyć na projekt rezerwowców 100 tys. dolarów w roku fiskalnym 2020 i 550 tys. dolarów w kolejnym okresie rozliczeniowym.

Gubernator Ohio Mike'a DeWine'a zatwierdził plan cyberoddziału w październiku, po fali incydentów hakerskich na terytorium stanu. Jeszcze w 2018 r. hakerzy zaatakowali serwery policji miasta Riverside. W obecnym roku, podczas styczniowych zamieci śnieżnych, wyłączony został zaś w Akron tzw. numer 311, służący do zgłoszeń i informowania obywateli o działaniu usług publicznych innych niż służby ratunkowe. W kwietniu port lotniczy Cleveland-Hopkins po ataku nie mógł zaś wyświetlać na tablicach informacji o lotach i bagażu.

"Obserwujemy obecnie znaczący wzrost inwestycji w cyberobronność" – wskazał wiceprezes firmy analitycznej Moody’s Investors Service, Orlie Prince. "Rządy stanowe testują swoje systemy, by mieć pewność, że mogą wypełniać swoje funkcje nawet po ataku hakerskim. Próby tego typu włamań są nieustanne" – dodał.

Bloomberg przypomniał, że po zeszłotygodniowym ataku ransomware, polegającym na zaszyfrowaniu plików na 500 serwerach i żądaniu za nie okupu, nadal podnosi się administracja Luizjany. W Atlancie koszty tegorocznych ataków z sieci szacuje się na miliony dolarów, w Baltimore blokada systemu informatycznego uniemożliwiła zbieranie opłat za wodę i podatków od nieruchomości, a w wyniku innej akcji hakerów w stanie Oklahoma skradzione zostały pieniądze z funduszu emerytalnego

Nie są to odosobnione przypadki, bo tylko w obecnym roku przeprowadzono aż 91 ataków internetowych na jednostki administracyjne w USA. To prawie dwukrotność zgłoszeń w porównaniu z 2018 r. – wynika z danych firmy cyberbezpieczeństwa Recorded Future.

Prawodawcy stanowi zaproponowali w 2019 r. blisko 300 nowych ustaw i uchwał dot. bezpieczeństwa informatycznego – jeszcze w 2015 r. zgłoszono zaś jedynie 65 tego typu projektów.

Bloomberg wskazał, że stany mają różne strategie walki z hakerami. Stan Waszyngton prowadzi regularne audyty bezpieczeństwa dla władz lokalnych, by pomóc im znaleźć podatności w ich systemach komputerowych. Nevada i Montana zaostrzyły zaś zasady na jakich można uzyskać dostęp do danych studentów tamtejszych uczelni.