Pentagon pod ostrzałem cyberprzestępców

21 lipca 2011

STANY ZJEDNOCZONE. Napływają kolejne informacje o cyberatakach na amerykańskie serwery wojskowe. W ostatnim z nich łupem włamywaczy padły 24 tys. plików. Według F-Secure Departament Obrony USA planuje wdrożenie pierwszej oficjalnej cyberstrategii, opartej m.in. na współpracy z innymi krajami oraz firmami zewnętrznymi.

Zastępca sekretarza ds. obrony USA William J. Lynn poinformował o włamaniu hakerów z zagranicy do sieci jednego z koncernów zbrojeniowych współpracującego z rządem USA. Atak miał miejsce w marcu – podczas zaledwie jednego włamania skradziono 24 tys. wojskowych plików.

Według serwisu Huffington Post marcowe włamanie jest jednym z najbardziej dotkliwych cyberataków wycelowanych w Departament Obrony USA. Cyberprzestępcom po raz kolejny udało się przebić przez zasieki obronne Pentagonu i wykraść ważne informacje.

Choć zastępca sekretarza obrony zapewnił, że część wykradzionych podczas tego ataku danych nie stanowi tajemnicy, podkreślił też, że spory odsetek z nich dotyczy tajnych systemów Pentagonu, m.in. rozwiązań wykorzystywanych w samolotach, podsłuchów oraz komunikacji satelitarnej. „Środki obrony, które obecnie stosujemy, okazały się niewystarczające do powstrzymania wycieków wrażliwych informacji" – przyznał Lynn.

„Fakt, iż w ciągu ostatniej dekady intruzom z zagranicy udało się wykraść gigantyczne ilości danych z sieci firmowych koncernów zbrojeniowych, to dla nas znaczące zmartwienie" – stwierdził Lynn podczas konferencji ujawniającej pierwszą formalną cyberstrategię w historii Pentagonu.

Sieć amerykańskiego wojska i przemysłu zbrojeniowego znajduje się na celowniku nie tylko zwykłych przestępców i włamywaczy, ale także – a może nawet przede wszystkim – obcych wywiadów. W 2008 właśnie zagraniczna agencja wywiadowcza zaopatrzyła w złośliwy kod pamięć przenośną, umieszczoną potem w wojskowym laptopie podłączonym do sieci obsługiwanej przez Dowództwo Centralne USA, zajmujące się newralgicznymi terenami Bliskiego Wschodu, Afryki Północnej i Azji Środkowej. Kod rozprzestrzenił się zarówno w jawnych, jak i tajnych systemach.

W maju jeden z największych koncernów współpracujących z amerykańskim wojskiem – Lockheed Martin – przyznał, iż jego system został spenetrowany przez niezidentyfikowanych jak dotąd hakerów. Tymczasem w ostatni poniedziałek grupa haktywistów przełamała zabezpieczenia kolejnej firmy zbrojeniowej – Booz Allen Hamilton. Według władz przedsiębiorstwa ofiarą włamywaczy padło ok. 90 tys. wojskowych adresów e-mail i haseł.

Departament Obrony przyznaje, że cyberszpiegostwo jest ogromnym problemem dla amerykańskich sił zbrojnych. „Kradzież danych projektowych i informacji technicznych z serwerów koncernów współpracujących z rządem to cios w technologiczną przewagę, jaką mamy nad potencjalnymi przeciwnikami" – podkreślił Lynn.

„Nowa cyberstrategia to znaczny postęp w stosunku do dotychczasowych działań Pentagonu. Departament Obrony musi się w końcu otworzyć na pomoc z zewnątrz, bo jak widać, dotychczasowe wojskowe środki często nie wystarczaj do odpierania coraz zmyślniejszych ataków" – komentuje Michał Iwan, dyrektor zarządzający F-Secure Polska. W tym przypadku konsultacje z profesjonalistami z dziedziny bezpieczeństwa IT nie tylko nie są ujmą dla rządu USA, a wręcz jego obowiązkiem – dodaje.

Czego dotyczy nowa cyberstrategia Pentagonu? Według Huffington

Post sprowadza się ona raczej do działań obronnych niż zaczepnych. Pentagon ma się otworzyć na współpracę z innymi krajami i prywatnymi firmami w dziedzinie cyberbezpieczeństwa. Niektóre wojskowe operacje w znacznym stopniu opierają się na łączach dostawców internetu i globalnych łańcuchach dostaw, co zmniejsza bezpieczeństwo.

Pentagon ma też współpracować z Departamentem Bezpieczeństwa Krajowego w celu ochrony żywotnej infrastruktury (np. sieci energetycznych) przed atakami z sieci oraz przygotować się na odłączenie od internetu podczas misji bojowych na wypadek cyberataku sił wroga.

Opracowanie: paku
Źródło: Dziennik Internautów