Dziurawy system przeciwatomowy USA

18 grudnia 2018

Ujawniony właśnie kwietniowy raport Inspektora Generalnego Departamentu Obrony wykazał, że amerykański System Ochrony Rakietami Balistycznymi (BMDS) jest pełen dziur. Okazało się, że dane przekazywane przez system nie są szyfrowane, nie zainstalowano żadnego oprogramowania antywirusowego, brak jest wielostopniowych systemów uwierzytelniających, znaleziono za to dziury liczące sobie… 28 lat.

Raport powstał na podstawie audytu w pięciu przypadkowo wybranych miejscach, w których Missile Defense Agency (MDA) umieściła części wspomnianego systemu. BMDS ma za zadanie bronić terytorium USA przed atakiem atomowym. Z opublikowanego właśnie raportu dowiadujemy się, że „Armia, Marynarka Wojenna i MDA nie chronią sieci i systemów, które przetwarzają, przechowują i przesyłają informacje techniczne BMDS".

Osoby prowadzące audyt znalazły kilka problemów, a największy z nich był związany z uwierzytelnianiem się. Przepisy mówią, że każdy nowo zatrudniony pracownik MDA otrzymuje nazwę użytkownik i hasło dające mu dostęp do sieci BMDS. Dodatkowo dostaje też kartę dostępu, którą powinien aktywować i używać równolegle z nazwą użytkownika i hasłem jako drugi stopień uwierzytelniania. Procedury mówią, że wszyscy nowi pracownicy MDA muszą korzystać z wielostopniowego uwierzytelniania najpóźniej w ciągu dwóch tygodni od podjęcia pracy. Inspektorzy odkryli jednak, że w 3 na 5 badanych instalacji pracownicy nie używali dwustopniowego uwierzytelniania. Posługiwali się wyłącznie hasłami. Jeden z pracowników robił tak od… 7 lat, a w jednej z instalacji sieć nigdy nie została skonfigurowana pod kątem dwustopniowego uwierzytelniania.

Okazało się również, że w 3 zbadanych instalacjach

administratorzy systemu nie aktualizowali oprogramowania. Znaleziono w nim dziury, dla których łaty istnieją od 2013 roku, a nawet dziury z roku 1990.

Innym problemem był brak fizycznych zabezpieczeń. W dwóch instalacjach szafy z serwerami nie były zamknięte i łatwo było uzyskać do nich dostęp. Zatem gość, osoba odwiedzająca czy w końcu szpieg umieszczony przez wrogi kraj, mógł z łatwością podpiąć do serwera urządzenie ze złośliwym oprogramowanie. Gdy jednej z osób odpowiedzialnych za bezpieczeństwo zwrócono uwagę na otwarte szafy serwerów, ta odpowiedziała, że nie wiedziała, iż należy je zamykać, a poza tym do serwerowni i tak jest ograniczony dostęp. W innej bazie szafa nie była zamykana, pomimo tego, iż miała zainstalowany mechanizm ciągle informujący, że należy ją zamknąć.

Kolejnym problemem był brak szyfrowania danych na urządzeniach przenośnych. Pomiędzy bezpiecznymi sieciami, które nie są ze sobą w żaden sposób połączone, dane są przenoszone ręcznie na fizycznych nośnikach. Okazało się, że w trzech lokalizacjach nie były one szyfrowane. Odpowiedzialni za bezpieczeństwo stwierdzili, że to wina systemu, który nie ma ani możliwości ani odpowiednich zasobów, by szyfrować dane, oni nie dostali pieniędzy na systemy szyfrowania danych i używają oprogramowania, które nie zawsze spełnia wymagania Pentagonu. W jednej z baz osoby odpowiedzialne za bezpieczeństwo przyznały, że nie wiedziały, iż takie dane należy szyfrować, w innej stwierdziły, że nie mają nawet oprogramowania, które informowałoby o tym, że pracownik kopiuje jakieś dane, nie mówiąc o tym, że wymagałoby ono szyfrowania.

W jednej z baz nie było ponadto oprogramowania monitorującego sieć pod kątem ewentualnych ataków z zewnątrz.

Menedżerowie odpowiedzialni za bezpieczeństwo tłumaczyli, że winni niedociągnięć są ich przełożeni, którzy – mimo złożonych wniosków – nie przyznali pieniędzy na odpowiedni sprzęt i oprogramowanie.

Autorstwo: Mariusz Błoński
Na podstawie: ZDNet.com
Źródło: KopalniaWiedzy.pl