Cyberatak na Lockheed Martin

31 maja 2011

Amerykańska firma zbrojeniowa Lockheed Martin potwierdziła, że była celem znaczącego cyberataku, który miał miejsce w poprzednim tygodniu.

Mimo że firma nie zdradziła zbyt wielu szczegółów dotyczących ataku, to rzecznik prasowy Lockheed Martina zapewnia, że zagrożenie zostało wykryte bardzo szybko i programistom odpowiedzialnym za bezpieczeństwo udało się uchronić wszystkie wrażliwe dane. Pentagon nadal pracuje nad dokładnym ustaleniem, które systemy bezpieczeństwa zostały złamane w korporacji, która na cały świat sprzedaje myśliwce, okręty marynarki wojennej oraz inne, warte wiele miliardów dolarów, technologie wojskowe. Z dotychczasowych doniesień wynika, że wpływ ataku na amerykańską obronność jest minimalny i Departament Obrony USA nie spodziewa się, aby był to początek czegoś większego.

Atak hakerów rozpoczął się 21 maja i według rzecznika

Lockheeda został powstrzymany „niemal natychmiast”. Przedstawiciele korporacji zapewniają, że system pozostał nietknięty i żadne dane klientów, pracowników, czy prowadzonych badań nie zostały ujawnione. Nadal jednak trwają pracę nad przywróceniem pracownikom normalnego dostępu do serwerów.

Lockheed Martin jest największą firmą produkującą samoloty na świecie. To z ich fabryk wyjeżdżają odrzutowce F-16, F-22 i F-35. Kiedy cztery lata temu hakerzy włamali się do plików programu „Joint Fighter” korporacja zdecydowanie unowocześniła swoje zabezpieczenia. Według Josha Shaula, eksperta z nowojorskiej firmy Application Security, obecny atak będzie miał podobny efekt i to nie tylko jeśli chodzi o Lockheeda, ale także inne firmy z branży zbrojeniowej.

Tymczasem w Australii rząd ostrzegł wszystkie większe firmy, aby uszczelniły wszystkie swoje wirtualne zabezpieczenia i spodziewały się natężonych prób ataku z zagranicznych źródeł. Porada pojawiła się po tym, jak prezes największej firmy energetycznej w kraju potwierdził, że ataki na jego serwery nie ustają, a co więcej, przeprowadzane są z coraz większą zaciętością.

Don Voelte, prezes Woodside Petroleum, mówi wprost: „Powszechnie wiąże się cyberataki z Chinami, ale tak naprawdę próby włamania odbywają się z terenów wschodniej Europy, Rosji, po prostu z każdej strony.

Opracowanie: lltr
Zdjęcie: Matt Hintsa
Na podstawie: BBC
Nadesłano do „Wolnych Mediów”