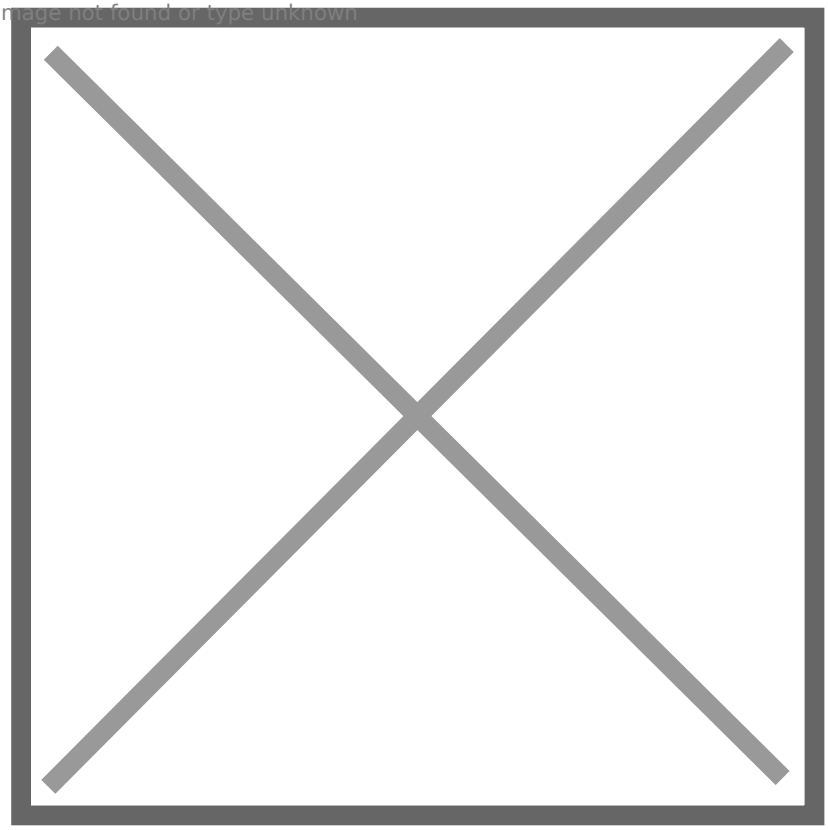
Hakerzy wykradli dokumentację F-35

#Lotnictwo wojskowe #Strategia i polityka 21 kwietnia 2009

Hakerzy, którzy włamali się do sieci USAF skopiowali kilka terabajtów danych dotyczących wielozadaniowego myśliwca nowej generacji F-35.

Image not found or type unknown



Pentagon i USAF prowadzą śledztwo w sprawie kradzieży danych dotyczących samolotu wielozadaniowego nowej generacji F-35. Jego oprogramowanie liczy ok. 7,5 mln linii, czyli ponad 3 razy więcej niż w najbardziej zaawansowanych myśliwcach obecnie eksploatowanych przez USAF. I właśnie część tego oprogramowania mogła wpaść w ręce hakerów. W przyszłości grozi to sytuacją, w której piloci nie będą mogli być do końca pewni danych wyświetlanych przez systemy pokładowe, w tym radiolokator, które będą mogły być łatwiej zakłócane.

O sprawie donosi Wall Street Journal. Kilku jego informatorów - obecnych i dawnych urzędników Pentagonu - twierdzi, że ataki na amerykańskie sieci informatyczne nasiliły się w ciągu ostatniego półrocza. Według oficerów odpowiedzialnych za bezpieczeństwo informatyczne, komputery, z których prowadzone są ataki, umieszczone są poza USA. Wskazują przy tym na ChRL, choć jednoznaczne ustalenie tożsamości hakerów jest w praktyce niemożliwe. Na pocieszenie informatorzy WSJ dodają, że najbardziej utajnione dane przechowywane są na komputerach odłączonych od Internetu.

Według szefa kontrwywiadu elektronicznego, Joela Brennera, sprawę ochrony danych dotyczących F-35 komplikuje konieczność współpracy z sojusznikami zagranicznymi. Nieoficjalnie wiadomo, że w ostatnim okresie zanotowano wyciek danych w Turcji i w innym, nieujawnionym kraju. Intruzi mieli dotrzeć w ten sposób do danych dotyczących systemu zbierania w czasie lotu danych potrzebnych do obsługi samolotu. Interesowali się też konstrukcją F-35, jego osiągami i systemami elektronicznymi. Ślady ich

działalności znaleziono też w systemach informatycznych kilku poddostawców głównych kontraktorów. Jakość zabezpieczeń mniejszych przedsiębiorstw bywa niższa niż w wypadku największych dostawców Pentagonu.

Raport Pentagonu z ubiegłego miesiąca także wskazuje na ChRL jako prowadzącą najbardziej intensywne działania szpiegowskie w Internecie. Zdaniem amerykańskich ekspertów, Chińczycy znacząco wzmacniają swój potencjał militarny, cały czas niewielki w zakresie wyposażenia konwencjonalnego. Ambasada ChRL stanowczo odżegnała się od wszelkich form cyberataków, twierdząc, że USA prowadzą walką propagandową w stylu zimnowojennym.

Administracja George W. Busha zaplanowała wydanie w ciągu kilku lat 17 mld USD na bezpieczeństwo w sieci. Barack Obama zamierza zwiększyć te wydatki, tnąc jednocześnie budżety na inne przedsięwzięcia.

Pentagon tylko w ciągu ostatnich 6 miesięcy musiał przeznaczyć dodatkowo ok. 100 mln USD na przeciwdziałanie cyberatakom. Pieniądze zostały przeznaczane na nowe oprogramowanie i szkolenie obsługi sieci informatycznych. Poinformował o tym na początku kwietnia gen. bryg. John Davis z US Strategic Command, odpowiedzialny za cyberbezpieczeństwo.

Przedstawiciele Pentagonu, a także głównych wykonawców F-35, w tym Lockheed Martina odmówili skomentowania informacji WSJ.

Pentagon i USAF prowadzą śledztwo w sprawie kradzieży danych dotyczących samolotu wielozadaniowego nowej generacji F-35. Jego oprogramowanie liczy ok. 7,5 mln linii, czyli ponad 3 razy więcej niż w najbardziej zaawansowanych myśliwcach obecnie eksploatowanych przez USAF. I właśnie część tego oprogramowania mogła

wpaść w ręce hakerów. W przyszłości grozi to sytuacją, w której piloci nie będą mogli być do końca pewni danych wyświetlanych przez systemy pokładowe, w tym radiolokator, które będą mogły być łatwiej zakłócane.

O sprawie donosi Wall Street Journal. Kilku jego informatorów - obecnych i dawnych urzędników Pentagonu - twierdzi, że ataki na amerykańskie sieci informatyczne nasiliły się w ciągu ostatniego półrocza. Według oficerów odpowiedzialnych za bezpieczeństwo informatyczne, komputery, z których prowadzone są ataki, umieszczone są poza USA. Wskazują przy tym na ChRL, choć jednoznaczne ustalenie tożsamości hakerów jest w praktyce niemożliwe. Na pocieszenie informatorzy WSJ dodają, że najbardziej utajnione dane przechowywane są na komputerach odłączonych od Internetu.

Według szefa kontrwywiadu elektronicznego, Joela Brennera, sprawę ochrony danych dotyczących F-35 komplikuje konieczność współpracy z sojusznikami zagranicznymi. Nieoficjalnie wiadomo, że w ostatnim okresie zanotowano wyciek danych w Turcji i w innym, nieujawnionym kraju. Intruzi mieli dotrzeć w ten sposób do danych dotyczących systemu zbierania w czasie lotu danych potrzebnych do obsługi samolotu. Interesowali się też konstrukcją F-35, jego osiągami i systemami elektronicznymi. Ślady ich działalności znaleziono też w systemach informatycznych kilku poddostawców głównych kontraktorów. Jakość zabezpieczeń mniejszych przedsiębiorstw bywa niższa niż w wypadku największych dostawców Pentagonu.

Raport Pentagonu z ubiegłego miesiąca także wskazuje na ChRL jako prowadzącą najbardziej intensywne działania szpiegowskie w Internecie. Zdaniem amerykańskich ekspertów, Chińczycy znacząco wzmacniają swój potencjał militarny, cały czas niewielki w zakresie wyposażenia konwencjonalnego. Ambasada ChRL stanowczo odżegnała się od wszelkich form cyberataków, twierdząc, że USA prowadzą walką propagandową w stylu zimnowojennym.

Administracja George W. Busha zaplanowała wydanie w ciągu kilku lat 17 mld USD na bezpieczeństwo w sieci. Barack Obama zamierza zwiększyć te wydatki, tnąc jednocześnie budżety na inne przedsięwzięcia.

Pentagon tylko w ciągu ostatnich 6 miesięcy musiał przeznaczyć dodatkowo ok. 100 mln USD na przeciwdziałanie cyberatakom. Pieniądze zostały przeznaczane na nowe oprogramowanie i szkolenie obsługi sieci informatycznych. Poinformował o tym na początku kwietnia gen. bryg. John Davis z US Strategic Command, odpowiedzialny za cyberbezpieczeństwo.

Przedstawiciele Pentagonu, a także głównych wykonawców F-35, w tym Lockheed Martina odmówili skomentowania informacji WSJ.