23/2/2012

Chińscy hackerzy przez 9 lat (!) infiltrowali Nortel...

Autor: vi.curry | Tagi: atak, Chiny, fail, Hacked!, Nortel, włamania

Słownie: dziewięć. Tyle lat chińscy hackerzy przebywali w wewnętrznych systemach firmy Nortel Networks. Dostali się tam dzięki wykradzeniu haseł należących do siedmiu managerów i regularnie ściągali plany biznesowe, pocztę elektroniczną oraz inne ważne dla firmy dokumenty.

Co zrobił Nortel? Prawie nic...

Ale jeszcze ciekawsze jest to co zrobił Nortel po tym, jak dowiedział sie o włamaniu... Otóż firma zmieniła 7 "wykradzionych" haseł na inne. I tyle. Żadnej analizy powłamaniowej. Przerażające w tym wszystkim jest to, że z produktów Nortela korzystają jedni z największych ISP na świecie, a po odkryciu włamania Nortel nie zadał sobie trudu weryfikacji, czy jego produkty nie wzbogaciły się przez kilka lat infiltracji w backdoora...

Co gorsza, jak podaje WSJ, Nortel Networks zbankrutowała w 2009 i posprzedawała swoje fragmenty innym firmom. Jest więc szansa, że ci, którzy przejęli po Nortelu jakieś systemy, wraz z nimi przejęli także chińskich "przyjaciół"...

Przepis na idealny atak?

Ta historia pokazuje, że prawdziwe jest powiedzenie iż *szewc bez butów chodzi*. Warto też zauważyć, że w sytuacji coraz gorszej kondycji finansowej firmy tnie się przede wszystkim wydatki na bezpieczeństwo (bo "bezpieczeństwo to zawsze koszt").

Wniosek? Jeśli chcesz, żeby twój atak został "zwielokrotniony", to atakuj upadające firmy — one nie przejmują się bezpieczeństwem, a po ogłoszeniu upadłości jest duża szansa, że zostawione przez Ciebie backdoory zostaną wykupione przez inne firmy z danego sektora.