Są dowody, że chińska armia cyberatakuje firmy z USA?

20 lutego 2013

Cyberataki na amerykańskie firmy wciąż przeprowadza chińska armia, a źródła ataków są powiązane z „jednostką 61398" – wynika z raportu opublikowanego przez firmę Mandiant. Raport ten doleje oliwy do ognia, który płonie od czasu, gdy amerykańskie gazety oskarżyły Chiny o włamania do swoich systemów.

Amerykanie od lat skarżą się na hackerów z Chin i zdarzało się już, że o ataki podejrzewano hackerów związanych z chińskim rządem. Tak było pod koniec 2009 roku, gdy doszło do ataków na infrastrukturę firmy Google. Przedstawiciele firmy twierdzili, że celem ataków były wybrane konta pocztowe działaczy na rzecz praw człowieka w Chinach. Pojawiła się wówczas groźba wyjścia Google z rynku chińskiego.

Kolejne tego typu napięcia pojawiły się na początku lutego. „New York Times" opublikował tekst, w którym opisał cyberataki na swoje systemy informatyczne. Ataki miały – według „Timesa" – związek z badaniem przez dziennikarzy fortuny zgromadzonej przez rodzinę Wen Jiabao, jednego z czołowych chińskich polityków. W tym samym czasie „Wall Street Journal" opublikował tekst o tym, że Chińczycy na większa skalę włamują się do systemów gazet, by pozyskiwać wrażliwe informacje np. o dziennikarskich źródłach.

Wczoraj nastąpiła kolejna odsłona tej historii. Amerykańska firma Mandiant, oferująca produkty w zakresie bezpieczeństwa informatycznego, opublikowała obszerny raport zawierający rzekomo dowody na to, że grupa hackerów o nazwie APT1 angażowała się w wieloletnią kampanię szpiegowania amerykańskich firm.

Mandiant twierdzi, że posiada dowody, iż grupa ATP1 jest

powiązana z Chińską Armią Ludowo-Wyzwoleńczą, a konkretnie z „jednostką 61398”, która ma być ciągle rosnącym organem wywiadu elektronicznego, znanym wcześniej jako Drugie Biuro 3 Departamentu Sztabu Generalnego ChALW. Jest to ponoć jednostka tajemnicza, o której istnieniu wiedzieli wcześniej przedstawiciele wywiadu. Oficjalnie niewiele o niej wiadomo.

Raport firmy Mandiant można pobrać ze strony www.mandiant.com/apt1, ale to nie wszystko. „New York Times” opublikował tekst na temat „jednostki 61398”. Temat chińskich ataków na amerykańskie firmy wrócił więc na dobre do prasy.

Władze Chin – komentując najnowsze doniesienia – powtarzają to, co mówiły wcześniej. Ich zdaniem Amerykanie nie mogą mieć żadnych dowodów na cyberataki, a stawianie tak poważnych oskarżeń przy braku dowodów jest wysoce nieodpowiedzialne.

Choć oskarżanie Chin o cyberataki nie jest nowością, to warto zauważyć, że w przeszłości również Pekin oskarżał o ataki Amerykę. Trudno powiedzieć, kto ma lepsze dowody. Wydaje się, że obydwie strony są zdolne do prowadzenia cyberwojny i obydwie strony mogą korzystać z tego, że cyberataku zawsze można się wyprzeć.

W przyszłości napięcia międzynarodowe, których źródeł są cyberataki, mogą być coraz częstsze, a ich znaczenie będzie rosło. Warto w tym miejscu przypomnieć doniesienia o robakach Stuxnet i Flame, które według prasy były amerykańsko-izraelską cybebronią przeciwko Iranowi.

Pojawiły się nawet doniesienia o tym, że amerykańska cyberbroń mogła szpiegować władze Francji, zamierzenie lub przez przypadek. Podobne wydarzenia mogą być nie lada wyzwaniem dla dyplomacji w przyszłości, bo przecież cyberataku można się wyprzeć, można go upozorować lub nawet wyprzeć się upozorowania…

Opracowanie: Marcin Maj
Źródło: Dziennik Internautów