aut. Szymon Palczewski 26.03.2019

EKSPERCI SĄ ZGODNI. TO PAŃSTWA ODPOWIADAJĄ ZA CYBERATAKI NA SEKTOR FINANSOWY

Cyberataki wymierzone w instytucje finansowe coraz częściej łączone są z państwami narodowymi. Według raportu Carnegie Endowment for International Peace celem tego typu incydentów jest nie tylko kradzież danych czy pieniędzy.

Spośród 94 przypadków cyberataków zgłoszonych jako przestępstwa finansowe od 2007 roku, 23 incydenty zostały przeprowadzone przez podmioty sponsorowane przez państwo. Większość z nich pochodziła z Iranu, Rosji, Chin czy Korei Północnej.

Report podkreśla rosnące obawy o podatność systemów finansowych z punktu widzenia cyberbezpieczeństwa. Jerome Powell, przewodniczący U.S. Federal Reserve, oraz Haruhiko Kuroda, szef banku centralnego Japonii, zgodnie twierdzą, że cyberataki są obecnie największym ryzykiem dla instytucji finansowych.

„Teraz banki muszą bronić się nie tylko przed cyberprzestępcami i zakłóceniami politycznymi, które zwykle mają charakter tymczasowym, ale także kradzieżą na dużą skalę prowadzoną przez państwo narodowe" – wskazuje Tim Maurer, specjalista Carnegie Endowment for International Peace. – „Ta ewolucja zagrożenia zmusiła organy regulacyjne oraz przemysł na całym świecie do odwrócenia uwagi od ograniczania ryzyka specyficznego dla firmy, aby w coraz większym stopniu koncentrować się na ryzykach sektorowych i systemowych" – tłumaczy ekspert.

Raport Carnegie Endowment for International Peace prezentuje dwa przykładowe cyberataki, jakie miały miejsce w niedalekiej przeszłości. Pierwszym z nich jest styczniowa kampania hakerska przeprowadzona przez północnokoreańskich cyberprzestępców. Jej głównym celem była infiltracja sieci bankowatów Banco de Chile, a następnie kradzież 10 milionów dolarów. W zeszłym roku hakerzy Pjongjangu dokonali włamania do systemów indyjskiego Cosmos Bank pozyskując w ten sposób 13,5 miliona dolarów.

Drugim opisanym w raporcie incydentem jest cyberatak wymierzony w systemy Banku Bangladeszu. Północnokoreańscy hakerzy wykorzystali sieć SWIFT (przyp. red. Society for Worldwide Interbank Financial Telecommunication) do rozsyłania fałszywych zleceń przelewu do nowojorskiego oddziału amerykańskiego banku centralnego.

Należy pamiętać, że cyberataki sponsorowane przez państwo odnoszą się do operacji, które obejmują bezpośrednią lub pośrednią działalność państwa narodowego wspierającą określoną grupę hakerów.