NAJPOWAŻNIEJSZY CYBERATAK W HISTORII ONZ. KIEROWNICTWO ODPOWIEDZIALNE ZA INCYDENT

Pracownik Międzynarodowej Organizacji Lotnictwa Cywilnego ONZ (ICAO) podkreślił, że najpoważniejszy w historii cyberatak wymierzony w oenzetowską komórkę został przeprowadzony za pomocą komputera syna przewodniczącego rady tej organizacji.

Pod koniec lutego dziennikarze kanadyjskiego nadawcy publicznego CBC ujawnili, że w 2016 roku ICAO padła ofiarą ataku hakerów, a czterech pracowników jej zespołu informatycznego próbowało usunąć dowody swej wykazanej wtedy niekompetencji.

Siedzibą ICAO jest Montreal. W ostatnich dniach dziennikarze powrócili do tych wydarzeń informując, że dyrektor biura administracji i usług ICAO Vincent Smith zamierza publicznie oskarżyć sekretarz generalną ICAO Chinkę Fang Liu oraz przewodniczącego rady agencji Nigeryjczyka Olumuyiwę Benarda Aliu o nadużycia.

W czerwcu i lipcu Smith wysłał kilka szczegółowych raportów na temat cyberataku do 36-osobowej rady ICAO, wybieranej spośród przedstawicieli wszystkich 193 państw członkowskich.

CBC opisała te raporty, otrzymane „z poufnego źródła”. Nadawca skontaktował się też ze Smithem, który powiedział dziennikarzom, iż podczas redagowania raportów został „uprzedzony, że popełnia zawodowe samobójstwo”.

Smith otrzymał w lutym od szefa bezpieczeństwa systemów informatycznych ICAO Si Nguyen Vo maila z wiadomością, że laptop byłego pracownika ICAO Maxima Aliu został zainfekowany wirusem podczas jego wizyty w biurze organizacji w Pekinie w 2010 roku.

Jak ustaliło śledztwo ONZ, Maxim Aliu miał status administratora domenowego między kwietniem 2012 i styczniem 2015 roku. Jest on synem obecnego przewodniczącego rady ICAO.

Wysłany przez Vo mail określa Maxima Aliu jako "pacjenta zero". Opisuje jak przez jego laptop sieć ICAO została zainfekowana przez znaną jako Emissary Panda chińską grupę cynberszpiegowską, która ma powiązania z rządem ChRL.

Cyberatak odkrył 22 listopada 2016 roku analityk pracujący dla niezależnej agencji o nazwie Aviation Information Sharing and Analysis Center. Zawiadomił on osobę odpowiedzialną za bezpieczeństwo

informatyczne ICAO, że hakerzy przejęli kontrolę nad dwoma serwerami organizacji i używają ich do infekowania złośliwym oprogramowaniem stron internetowych obcych rządów. Dochodzenie w tej sprawie ICAO powierzyła oenzetowskiemu Międzynarodowemu Centrum Komputerowemu (ICC).

Jak powiedział CBC rzecznik ICAO William Raillant-Clark, przedstawiony w 2017 roku raport ICC wyklucza istnienie "pacjenta zero", jak również "nie przypisuje odpowiedzialności za naruszenie bezpieczeństwa konkretnej osobie lub urządzeniu".

Natomiast według Smitha, z raportu tego wynika, że atakujący wdarł się na konta administratora domenowego i administratora sieci, co pozwoliło hakerom uzyskać dostęp do maili i haseł ICAO. Starając się ustalić chronologię ataku Vo natrafił na kilka innych cyberwłamań, z których co najmniej jedno dotyczyło funduszy inwestycyjnych. Vo wykrył również, że między listopadem 2018 a styczniem 2019 roku w dokumentacji bezpieczeństwa wykasowano wszystkie informacje związane z włamaniami, między innymi na temat porcedur, standardów, planów działania i historii ataków.

W swych raportach dla rady ICAO Smith twierdził, że pod rządami sekretarz generalnej Liu organizacja ta stała się środowiskiem "toksycznym i wrogim", trapionym "nepotyzmem" i "faworytyzmem". Oskarżał Liu, że wbrew zaleceniom Biura Usług Nadzoru Wewnętrznego ONZ nie wszczęła dochodzenia wobec czterech osób, które "działały z zamiarem ukrycia źródła, natury i skutków włamania do sieci ICAO". Wskazywał też, że wobec tych osób jest "wciąż ich zwierzchnikiem bez jakiejkolwiek realnej władzy nad nimi".

W wygłoszonym na początku maja w Waszyngtonie przemówieniu przedstawiciel USA przy ICAO Thomas Carter zarzucił kierownictwu tej organizacji, że starało się zbagatelizować doniesienia o cyberataku jako rzekomo "przesadzone". Tymczasem systemy ICAO "stały się całkowicie dostępne dla zagranicznego czynnika państwowego, a dwa całkowicie niezależne śledztwa kryminalne udowodniły, że to prawda".

SZP/PAP