aut. Szymon Palczewski 20.05.2020

IZRAEL SPARALIŻOWAŁ NAJWIĘKSZY PORT W IRANIE?

Analiza cyberataku przeprowadzonego na największy irański port morski Shahid Rajaee wskazuje, że stanowił on izraelską odpowiedź na wcześniejsze incydenty ze strony Teheranu. Tel Awiw realizuje strategię „odwet za odwet". Sytuacja na Bliskim Wschodzie staje się coraz poważniejsza i jesteśmy coraz bliżej konfliktu w cyberprzestrzeni pomiędzy Iranem i Izraelem.

Incydent zablokował część urządzeń odpowiedzialnych za kontrolę wymiany towarów w największym irańskim porcie. W tym miejscu warto podkreślić, że Shahid Rajaee to nowo wybudowany obiekt położony w nadmorskim mieście Bandar Abbas, nad Cieśniną Ormuz.

Incydent wywołał nagłe przeciążenie sieci i systemów w terminalu portu. Urządzenia odpowiedzialne za kontrolę przepływu statków oraz towarów uległy awarii w tym samym momencie – informuje The Washington Post. Dziennik posiada również zdjęcia satelitarne przedstawiające kilometrowe korki prowadzące do portu oraz liczne statki czekające na rozładunek.

Warto również podkreślić, że w tym samym czasie irański okręt wojenny „Konarak" uległ zniszczeniu podczas prowadzenia operacji w pobliskich wodach. W wyniku incydentu zginęło 19 marynarzy a obrażenia odniosło kolejne 15 osób. Jak wówczas informowaliśmy, szybko pojawiły się analizy mówiące, że cyberatak na port Shahid Rajaee mógł odegrać rolę w katastrofie irańskiego okrętu.

W odpowiedzi na rosnące napięcie Mohammad Rastad, wiceszef resortu dróg i rozwoju Iranu, zdecydował się na wydanie publicznego oświadczenia i w rozmowie z krajową agencją prasową ILNA potwierdził doniesienia o cyberataku, wskazując, że incydent dotknął przede wszystkim wiele prywatnych systemów operacyjnych. „Niedawny cyberatak nie przeniknął do systemów portu oraz organizacji morskiej (PMO)" – wyjaśnił przedstawiciel irańskiego rządu. – „Organizacja jest dobrze chroniona, ale nadal musi stale wzmacniać i aktualizować warstwy ochrony, aby zminimalizować ryzyko kolejnego cyberataku".

Czytaj też: Na Bliskim Wschodzie rozgrywa się cyberwojna. Każdy dzień to nowy incydent

Stanowisko Teheranu w sprawie szkód związanych z cyberatakiem odbiega od stanu faktycznego. Zagraniczni specjaliści wskazują, że incydent wywołał znacznie poważniejsze zakłócenia niż podnosi Iran i najprawdopodobniej został przeprowadzony przez izraelskie jednostki – donosi The Washington Post, powołując się na wiedzę amerykańskiego eksperta monitorującego sytuację. Specjalista pragnął pozostać anonimowym ze względu na swoje bezpieczeństwo.

Cyberatak został przeprowadzony z wielką precyzją, a w jego wyniku nastąpił całkowity chaos. Informator amerykańskiego dziennika posiadał dostęp do tajnych dokumentów i jednoznacznie

stwierdził, że za cyberatak najprawdopodobniej odpowiada Izrael. W związku z tym incydent należy uznać za operacje odwetową za irańskie złośliwe działania wymierzone w izraelską infrastrukturę cywilną.

Jak informowaliśmy wcześniej, Teheran odpowiada za cyberatak ukierunkowany w systemy wodociągowe Izraela. Hakerzy uderzyli między innymi w układ odpowiedzialny za kontrolę nasycenia wody chlorem. Parę dni później incydent stał się jednym z tematów posiedzenia izraelskiego gabinetu bezpieczeństwa. Dla Tel Awiwu irański cyberatak na infrastrukturę wodociągową stanowi przejaw eskalacji napięcia, zwłaszcza że celem była infrastruktura cywilna.

Najnowsza kampania wskazuje, że Izrael przyjął strategię „odwet za odwet" w odpowiedzi na irańskie operacje w cyberprzestrzeni. Podobne podejście jest realizowane przez izraelskie wojsko w zakresie konwencjonalnych działań – wskazuje The Times of Israel.

„Cyberatak na port Shahid Rajaee w Iranie był izraelską odpowiedzią na incydent, który Irańczycy przeprowadzili przeciwko Izraelowi dwa tygodnie wcześniej" – podkreślił anonimowy informator The Washington Post. – „Izrael ma nadzieję, że Irańczycy na tym poprzestaną. Zaatakowali komponenty infrastruktury wodnej. Tak naprawdę nie spowodowali szkód, ale przekroczyli bezpieczną linię i Izrael musiał się zemścić".

Pomimo że irański cyberatak był nieskuteczny, ponieważ został odparty przez zespół cyberbezpieczeństwa, to jednak został potraktowany przez Izrael za bardzo poważne naruszenie ogólnie przyjętych zasad i „przekroczenie czerwonej linii".

W tym miejscu warto przypomnieć, że podczas operacji Iran wykorzystał amerykańskie serwery, aby włamać się do izraelskich sieci i podjąć próbę dalszych złośliwych działań w celu naruszenia systemów infrastruktury cywilnej. Stany Zjednoczone zapewniają swoim sojusznikom wsparcie w zakresie cyberbezpieczeństwa, jednak w tej sprawie Biały Dom odmówił komentarza.

Czytaj też: Cyberatak na infrastrukturę wodociągową w Izraelu