Cyberdefence 24

aut. Szymon Palczewski 13.05.2020

NA BLISKIM WSCHODZIE ROZGRYWA SIĘ CYBERWOJNA. KAŻDY DZIEŃ TO NOWY INCYDENT

Iran potwierdził informację o cyberataku, który miał miejsce w największym porcie morskim położonym w cieśninie Ormuz. Analiza incydentu wykazała, że mógł on mieć wpływ na późniejszą katastrofę z udziałem irańskiego okrętu wspierającego marynarkę wojenną. Sytuacja miała miejsce kilka dni po tym, jak Izrael skrytykował Teheran za cyberatak na infrastrukturę cywilną tego państwa. „Cyberatak na infrastrukturę wodociągową stanowi eskalację napięcia" – podkreślają władze Tel Awiwu. Czy właśnie obserwujemy wymianę ciosów pomiędzy Iranem i Izraelem na Bliskim Wschodzie?

Przedstawiciele irańskiego rządu poinformowali o operacji hakerskiej wymierzonej w port Shahid Rajaei, znajdujący się w mieście Bandar Abbas. Wskazują, że cyberprzestępcy infiltrowali sieci a ich działania uszkodziły część urządzeń – donosi serwis ZDNet.

Zaatakowany port jest największym tego typu obiektem w cieśnienie Ormuz. Irańczycy podkreślają, że pomimo zniszczenia pewnej liczby sprzętu cyberatak należy rozpatrywać w kategoriach niepowodzenia.

Początkowo przedstawiciele lokalnych władz zaprzeczali doniesieniom o incydencie, pomimo czasowego zamknięcie portu. Jednak z czasem, pod presją mediów, przyznano, że operacja hakerska rzeczywiście miała miejsce – informuje ZDNet.

W tym miejscu warto podkreślić, że w weekend irański okręt wsparcia marynarki wojennej „Konarak" uległ zniszczeniu podczas prowadzenia operacji w pobliskich wodach. W wyniku incydentu zginęło 19 marynarzy a obrażenia odniosło kolejne 15 osób. Szybko pojawiły się analizy mówiące, że cyberatak mógł odegrać rolę w katastrofie irańskiego okrętu.

W związku z rosnącym napięciem władze państwowe zdecydowały się na przyjęcie oficjalnego stanowiska i wystosowanie publicznego oświadczenia. „Niedawny cyberatak nie przeniknął do systemów, ale był w stanie infiltrować i uszkadzać szereg prywatnych sieci operacyjnych w porcie" – zaznaczył wiceminister transportu drogowego i rozwoju Mohammad Rastad w rozmowie z irańską agencją prasową Ilna.

Przedstawiciel władzy nie przedstawił żadnych informacji na temat potencjalnego źródła incydentu. Wskazał jedynie, że należy podjąć dalsze kroki w celu poprawy jakości cyberzabezpieczeń w miejscach szczególnie wrażliwych. „Nadal należy stale wzmacniać i aktualizować warstwy ochrony, aby zminimalizować ryzyko cyberataku" – podkreślił Mohammad Rastad.

Region cyberwojny

Na Bliskim Wschodzie wzrosła rola zarówno cyberataków jak i cyberbezpieczeństwa, co wynika z

faktu, że region ten jest istotnym punktem eksperymentów z udziałem nowych systemów uzbrojenia – od dronów po pociski balistyczne.

W ciągu ostatnich kilku lat Iran starał zwiększyć się swoje zdolności „cyberwojenne" poprzez utworzenie specjalistycznych jednostek wspieranych przez Korpus Strażników Rewolucji Islamskiej (ang. Islamic Revolutionary Guard Corps – IRGC) – donosi The Jerusalem Post. Lokalne media wskazują, że irańskie cyberoddziały „szukają okazji" do przeprowadzenia złośliwych operacji. Jedną z nich było zabójstwo generała IRGC Qasem Soleimaniego przez Stany Zjednoczone. Odpowiedzią Teheranu były działania w cyberprzestrzeni wymierzone w amerykańskie sieci, w tym systemy agencji rządowych.

Rozwój zdolności Iranu sięga 2010 roku, kiedy to Teheran musiał zareagować na operację z wykorzystaniem wirusa Stuxnet. Od tego czasu Persowie regularnie próbują zwiększyć swoje możliwości prowadzenia działań w cyberprzestrzeni i wykorzystywanie tajnych działań do realizacji swojej nowej strategii. Pod dowództwem IRGC, Hosseinem Salamim, Iran przedstawił swój konflikt ze Stanami Zjednoczonymi i ich sojusznikami, w tym Izraelem, jako przykład wojny totalnej, obejmującej nie tylko konwencjonalne środki walki, ale też cyberzdolności.

Odnosząc się do bieżącej sytuacji, 5 maja br. Mohaammad Rastad zorganizował obchód pokazowy po porcie Shahid Rajaei, aby pochwalić się ukończeniem dwóch ważnych terminali kontenerowych – informuje The Jerusalem Post. Iran próbował w ten sposób obejść sankcje i zwiększyć zyski w czasie pandemii i spadających cen ropy.

Kilka dni później port stał się celem cyberataku. Jeden z incydentów przyczynił się do powstania problemu obliczeniowego podczas manewrów z udziałem irańskiego okrętu, który następnie uległ zniszczeniu. Początkowo nie sądzono, że sytuacja może być powiązana z działalnością hakerów.

Warto podkreślić, że Iran nie jest jedynie ofiarą cyberoperacji, ale sam w wielu przypadkach jest agresorem. Przykładem może być cyberatak wymierzony w izraelską infrastrukturę wodociągową. Jak informowaliśmy wcześniej, hakerzy uderzyli między innymi w układ odpowiedzialny za kontrolę nasycenia wody chlorem. Incydent był jednym z tematów posiedzenia gabinetu bezpieczeństwa Izraela.

Zdaniem specjalistów nie był to pierwszy tego typu incydent. Cyberprzestępcy od dłuższego czasu interesują się infrastrukturą wodociągową oraz energetyczną, które należą do podmiotów kluczowych państwa.

Dla Izraela irański cyberatak na infrastrukturę wodociągową stanowi przejaw eskalacji napięcia, zwłaszcza że celem była infrastruktura cywilna – donosi The Jerusalem Post. Trey Yingst, dziennikarz amerykańskiej stacji Fox News, poinformował za pomocą Twittera, że podczas operacji Iran wykorzystał amerykańskie serwery, aby włamać się do izraelskich sieci. Dodał, że Waszyngton odmówił komentarza w tej sprawie. „Przedstawiciel Departamentu Energii USA (DoE) odmówił komentarza na temat wszelkich szczegółów związanych z >trwającym dochodzeniem< (…) DoE rutynowo gromadzi i udostępnia informacje partnerom z sektora prywatnego, aby chronić USA i sojuszników przed cyberatakami" – czytamy w komunikacie dziennikarza.

Czytaj też: Cyberatak na infrastrukturę wodociągową w Izraelu