

STRATEGICZNE POROZUMIENIE IZRAELA I ZEA. WZAJEMNA CYBEROBRONA PRIORYTETEM

Izrael oraz Zjednoczone Emiraty Arabskie (ZEA) zacieśniają współpracę w zakresie cyberbezpieczeństwa w związku z wysoką aktywnością hakerów w regionie, w tym falą cyberataków ze strony Iranu. Głównym założeniem inicjatywy jest stworzenie środowiska obrony zbiorowej w sieci oraz mechanizmów rozwoju innowacyjnych rozwiązań w obu państwach. Nawiązanie porozumienia było możliwe dzięki normalizacji wzajemnych stosunków dyplomatycznych.

Oba państwa uznały, że obrona zbiorowa może być dużo bardziej skuteczna w cyberprzestrzeni niż w przypadku samodzielnych działań. W związku z tym zaledwie kilka tygodni po znormalizowaniu stosunków dyplomatycznych podjęto decyzję o nawiązaniu współpracy, która polegać będzie przede wszystkim na wykrywaniu zagrożeń w sieci, w tym wrogich operacji hakerskich. Ponadto mają powstać kanały wymiany informacji wywiadowczych między rządowymi specjalistami ds. cyberbezpieczeństwa.

„Grożą nam te same zagrożenia (na przykład ze strony Iranu – przyp. red.) ze względu na charakter regionu, nasze relacje i z powodu tego, kim jesteśmy - silnymi ekonomicznie i technologicznie krajami” – podkreślił Yigal Unna, szef izraelskiej National Cyber Directorate podczas webinarium z udziałem jego odpowiednika ze Zjednoczonych Emiratów Arabskich (ZEA) Mohameda al-Kuwaitiego. „Jestem bardzo optymistycznie nastawiony, ponieważ mamy wiele wspólnego” – dodał Yigal Unna, cytowany przez Agencję Reutera.

Rozpoczynając swoje przemówienie Yigal Unna zwrócił się do przedstawiciela ZEA w następujący sposób: „Mój bracie, cieszę się z tej wspaniałej okazji rozpoczęcia owocnej współpracy między nami”. Następnie wskazał, że oba kraje posiadają wiele cech wspólnych. „Nie są duże, mamy prawie taką samą populację, mamy wybitnych naukowców, wyedukowane społeczeństwo i kładziemy duży nacisk na zaawansowane technologie” – przytacza wypowiedź szefa izraelskiej National Cyber Directorate The Jerusalem Post.

Yigal Unna zaznaczył, że nareszcie udało się stworzyć warunki do wzajemnej współpracy, która, w jego opinii, przyniesie wiele korzyści każdej ze stron. „ZEA ma wiele do zaoferowania Izraelowi i Izrael ma wiele do zaoferowania ZEA” – stwierdził specjalista.

Z kolei Mohamed al-Kuwaiti podkreślił, że jego kraj jest narażony na wrogie operacje hakerskie, w tym kampanie ransomware, co jest związane z rozwojem sfery cyfrowej. Dlatego też nawiązanie współpracy w zakresie cyberbezpieczeństwa będzie miało pozytywny wpływ na jakość cyberobrony ZEA. „Izrael jest bardzo dobrze znany w branży technologicznej i to naprawdę pomoże” – podkreślił Mohamed al-Kuwaiti.

Przedstawiciele obu państw zwrócili uwagę na znaczenie wymiany danych na temat cyberzagrożeń. Zaprezentowali również koncepcję wspólnych ćwiczeń w obszarze cyberobrony, które mają przyczynić się do podniesienia standardów obu państw w zakresie ochrony sieci. Inicjatywa odzwierciedla coraz

większą rolę, jaką odgrywa cyberbezpieczeństwo w stosunkach dyplomatycznych.

„Pomoże nam to (współpraca – przyp. red.) w odstraszeniu wrogich podmiotów” – podkreślił al-Kuwaiti, prezentując swoje stanowisko w odniesieniu do nawiązania porozumienia dotyczącego wzajemnej współpracy na rzecz cyberbezpieczeństwa.

Doron Hadar, dowódca izraelskiej wojskowej jednostki ds. sytuacji kryzysowych, wskazał podczas wirtualnej konferencji, że radzenie sobie z atakami ransomware i innymi operacjami hakerskimi „nie jest sytuacją z gatunku: >wygrana/przegrana<, lecz >porażka/mniej dotkliwa porażka<”. Podkreślił również, że dzięki współpracy i aktywnemu dialogowi można poradzić sobie z cyberzagrożeniami i wyjść z nich bez większych strat.

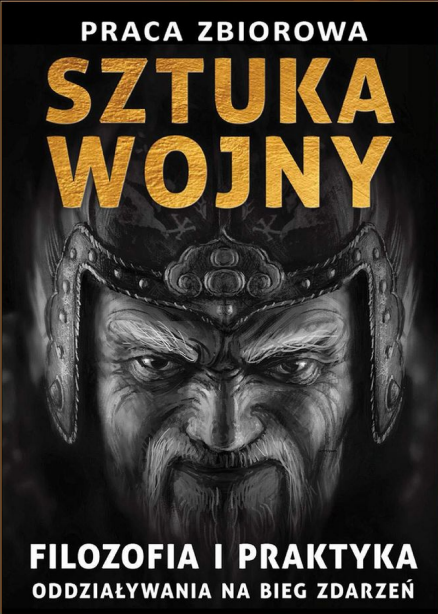
Dzięki obecności licznych firm technologicznych, w których pracują byli hakerzy wojskowi, Izrael od dawna jest uznawany za cyberpotęgę – informuje serwis CyberScoop. Wielu specjalistów z tego państwa nie tylko odpowiada za ochronę sieci w kraju, lecz także stanowią podstawę zagranicznych podmiotów, w tym na przykład koncernów w Stanach Zjednoczonych.

Izrael przeznaczają miliardy dolarów na technologie cyberbezpieczeństwa rocznie i jest siedzibą wielu gigantów branży takich jak NSO Group (firma będąca twórcą oprogramowania szpiegowskiego Pegasus). Nie jest to bez znaczenia, ponieważ rząd ZEA od lat wykorzystuje produkty NSO Group do prowadzenia własnych działań.

Zjednoczone Emiraty Arabskie są obecnie uznawane za regionalne centrum technologiczne, co przyciąga największe koncerny branży IT, w na przykład Microsoft. Zdaniem Agencji Reutersa, rząd ZEA przyjął ofensywne nastawienie do operacji w wirtualnej domenie, werbując byłych amerykańskich pracowników wywiadu do rozwijania narodowych zdolności hakerskich.

Mohamed al-Kuwaiti nazwał normalizację stosunków z Izraelem jako „krok naprzód” dla rządu ZEA, który dąży do cyfryzacji państwa oraz rozwoju sztucznej inteligencji. Zjednoczone Emiraty Arabskie wyceniły w zeszłym roku swój rynek cyberbezpieczeństwa na 490 milionów dolarów.

Czytaj też: [„Cybernajemnicy” na usługach Teheranu. Głównym celem USA i Izrael](#)



PRACA ZBIOROWA
SZTUKA WOJNY

FILOZOFIA I PRAKTYKA
ODDZIAŁYWANIA NA BIEG ZDARZEŃ

Wojna to konfrontacja dwóch ludzkich woli

Nowy przekład traktatu Sun Zi

Wśród współautorów wykładów i komentarzy m.in.

- prof. Jerzy Bralczyk • gen. Jarosław Kraszewski
- prof. Witold M. Orłowski • płk Leszek Elak • NAVAL
- płk Andrzej „Wodzu” Kruczyński

Sklep.Defence **24**

[Z oferty Sklepu Defence24 - zapraszamy!](#)