

## CYBERWEEK W TEL AWIWIE

---

**W Tel Awiwie w dniu 17.06 rozpoczęła się konferencja Cyber Week organizowana przez Interdyscyplinarne Centrum Badań nad Cyber Blawatnika na Uniwersytecie w Tel Awiwie. Konferencja co roku przyciąga ponad 3000 uczestników, którzy biorą udział w ponad 60 wydarzeniach o różnym zakresie tematycznym.**

Cyber Week co roku porusza tematy cyberbezpieczeństwa w różnych branżach - zarówno gospodarki oraz bankowości, ochrony danych osobowych, postępu technologicznego i bezpieczeństwa narodowego - i z różnej perspektywy. Motywem przewodnim większości paneli jest spojrzenie w przyszłość i próba antycypowania, jakie zagrożenia dopiero się pojawią. Jak często wspomina Major Generał Itzhak Ben-Israel, jeden z gospodarzy wydarzenia, jedno pokolenie w cyberbezpieczeństwie to pół roku - postęp technologiczny napędza zarówno innowacyjność, jak i zagrożenia. Z tego względu próby przewidzenia, co wydarzy się za pięć lub dziesięć lat są niemożliwe do zrealizowania. Paneliści próbują wybiegać myślami w przyszłość i sugerować - jaka jest przyszłość cyberzagrożeń, Sztucznej Inteligencji, e-gospodarki.

Podczas pierwszego panelu konferencji poświęconemu przyszłości cyberbroni, Generał Ehud Schneerson podkreślił, że według niego cyberatak będzie następnym 11 września, który doprowadzi do zmiany w pojmowaniu przez nas cyberprzestrzeni, oraz spowoduje wzmożenie wysiłków na rzecz zabezpieczenia poszczególnych państw przed atakami cyber. Jednocześnie sugerował, że to sektor energetyki będzie w najbliższym czasie najbardziej narażony na ataki, które mogą okazać się niebezpieczne dla dużej części populacji cywilnej państwa. Generał Yaakov Amidror podkreślił, że zwłaszcza w zakresie cyberbezpieczeństwa ważna jest współpraca międzynarodowa i wsparcie ze strony sojuszników. Z kolei Generał Yaron Rosen zaznaczył, że nawet małe państwa o interesach na poziomie regionalnym nie mogą sobie pozwolić na brak zaangażowania na poziomie globalnym w przypadku cyberbezpieczeństwa. Rosen zauważył, że państwa narodowe są kontestowane zarówno przez inne kraje, jak i przez podmioty pozapaństwowe z wykorzystaniem cyber. Zwrócił równocześnie uwagę, że budowa efektywnego systemu cyberbezpieczeństwa to nie tylko stworzenie podmiotów oraz systemów, to również wypracowanie i przetestowanie procedur reagowania.

Z polskiej perspektywy, jak podkreśla Koordynator Programu Cyberbezpieczeństwo Fundacji im. Kazimierza Pułaskiego Patrycja Chomicka, wypracowanie rozwiązań z zakresu systemu cyberbezpieczeństwa jest nie tylko potrzebne, ale i naglące. Ze względu na wrażliwość polskiej infrastruktury krytycznej oraz zagrożenia, które mogą nadejść ze wschodu, Polska powinna czerpać z izraelskich doświadczeń, które są obecnie testowane w ramach CERTów pod bezpośrednim nadzorem Narodowego Dyrektoriatu Cyber. Ze względu na duże zaufanie podmiotów prywatnych oraz skutecznie przetestowane procedury, incydenty z zakresu cyberbezpieczeństwa są nie tylko wcześniej wykrywane, ale również zgłaszane i izolowane, żeby ograniczyć ich szkodliwość. Jest to niewątpliwie dobry przykład, który powinien zostać wdrożony nie tylko w Polsce, ale również innych państwach należących do UE i NATO, żeby wzmocnić obie organizacje.

Konferencja Cyber Week gości co roku nie tylko przedstawicieli sektora prywatnego oraz naukowców,

jest to również miejsce spotkań wojskowych oraz przedstawicieli administracji, zarówno izraelskiej, jak i zagranicznej. W tym roku udział w konferencji miał pojawić się w agendzie Minister Przemysłu i Technologii Jadwigi Emilewicz, która w ciągu ostatnich miesięcy nawiązała dobrą współpracę z Izraelem na poziomie promocji innowacyjności oraz przemysłu obu państw.

Patrycja Chomicka

Koordinator Programu Cyberbezpieczeństwo Fundacji im. Kazimierza Pułaskiego