CYBEROBRONA PRIORYTETEM NATO NA KOLEJNE LATA [CYBERSEC 2019]

Włączenie obrony cyberprzestrzeni do głównych zadań NATO oraz konieczność podjęcia walki z zagrożeniami hybrydowymi przez rządy i biznes to najważniejsze wnioski płynące z wystąpień i dyskusji, które odbyły się podczas drugiego dnia jubileuszowej edycji Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2019 w Katowicach. Ścieżka poświęcona obronności zrealizowana została ze wsparciem merytorycznym Centrum Eksperckiego Kontrwywiadu NATO.

Drugi dzień CYBERSEC Forum rozpoczął się od spotkania z Generałem Robertem Spaldingiem, byłym doradcą Prezydenta Donalda Trumpa ds. Chin. Ekspert podzielił się swoją wiedzą na temat stosunków politycznych, gospodarczych oraz społecznych USA z Chinami, którą przedstawił w niedawno wydanej książce zatytułowanej „Stealth War: How China Took Over While Americas' Elite Slept". Szczególną uwagę poświęcił kwestiom związanym z rozwojem sieci 5G w Państwie Środka. Zwrócił uwagę również na problem ochrony danych osobowych.

„Brak wiedzy o tym, kto wykorzystuje Twoje dane, stwarza zagrożenie dla wolności" – podkreślił podczas swojego wystąpienia Robert Spalding.

Ścieżkę „Obrona" otworzył międzynarodowy autorytet ds. bezpieczeństwa, Generał Keith B. Alexander, były Dyrektor NSA, Założyciel i Prezes IronNet Cybersecurity, który m.in. odpowiadał za bezpieczeństwo Stanów Zjednoczonych Ameryki Północnej w administracji Prezydenta Baracka Obamy. Generał nadzorował zarówno ofensywne, jak i defensywne operacje kraju w cyberprzestrzeni oraz zajmował się tematem wojny cyfrowej. Obecnie jest jednym z najlepszych ekspertów na świecie, którzy posiadają tak pełne spojrzenie na szeroką naturę ewoluujących zagrożeń cyfrowych. W trakcie swojego wystąpienia Generał podkreślił konieczność współpracy międzynarodowej na rzecz zapewnienia bezpiecznej cyberprzestrzeni.

„Cyberbezpieczeństwo to nasza wspólna odpowiedzialność. Razem możemy wykrywać zagrożenia, reagować na nie i chronić społeczeństwo przed ich konsekwencjami" – podkreślił gen Keith B. Alexander.

Obrona cybernetyczna priorytetem NATO

Zapewnienie gwarancji wolności i bezpieczeństwa członków Sojuszu stoi obecnie przed rosnącą liczbą zagrożeń. W miarę rozwoju metod, poziomu szkodliwości i powszechności ataków, NATO włączyło cyberobronę do priorytetowych działań. Dlatego w trakcie odbywającej się na ten temat dyskusji panelowej pod hasłem „Bezpieczeństwo w ramach Sojuszu – wspólne wysiłki na rzecz zwiększenia cyfrowych możliwości obrony", biorący w niej udział eksperci zwracali uwagę na konieczność zwiększenia aktywności w ramach NATO, a także kompleksowego podejścia do kwestii opracowania odpowiednich standardów, rozwoju i wzmacniania reakcji na cyberzagrożenia.

Głównym wnioskiem wynikającym z panelu moderowanego przez płk. Roberta Balę, byłego Dyrektora Centrum Eksperckiego Kontrwywiadu NATO, jest konieczność rozwoju i wzmacniania cyberobrony oraz zdolności operacyjnej w tym zakresie zarówno przez Sojusz, jaki i poszczególne państwa członkowskie.

„NATO nie planuje rozwoju własnych zdolności cybernetycznych, wszystko będzie oparte na wkładach krajowych" – powiedział Antonio Missiroli, Asystent Sekretarza Generalnego NATO ds. pojawiających się wyzwań w zakresie bezpieczeństwa.

Zwalczanie zagrożeń w cyberprzestrzeni

Kolejna debata poświęcona zagrożeniom hybrydowym i ich roli w zmieniającym się cyfrowym świecie przyniosła pytania o związane z nimi konsekwencje zarówno dla obywateli, jak i sektora obronnego. Paneliści podkreślali konieczność podnoszenia świadomości na temat nowych rodzajów zagrożeń oraz wskazali kluczową rolę skutecznej współpracy między organizacjami krajowymi i międzynarodowymi, a także między biznesem i sektorem publicznym. Zaproszeni goście podzielili się swoimi przemyśleniami na temat tego, jak powinno wyglądać podejście strategiczne oraz wykorzystanie dostępnych narzędzi na tym polu.

O szczególnej odpowiedzialności sektora prywatnego wynikającej z rozwoju sektora nowych technologii opowiedział John Frank, Wiceprezes Microsoft ds. Relacji Rządowych dla Europy.

„To my przedstawiamy światu technologię. Dlatego musimy upewnić się, że nasze produkty są używane w sposób bezpieczny" - powiedział John Frank.

Potencjał białego wywiadu

Blok poświęcony tematom związanym z obronnością zamknęła debata dotycząca rosnącej roli białego wywiadu, czyli gromadzenia informacji z ogólnodostępnych źródeł (ang. Open Source Intelligence - OSINT). Prelegenci podkreślili, że dostęp do publicznych danych ma szansę wnieść dużą wartość dodaną w różnych sektorach, począwszy od rekonstrukcji spraw karnych, przez zwiększanie świadomości dotyczącej zagrożeń, aż po poszerzanie wiedzy wywiadowczej.

Tegoroczna jubileuszowa edycja V Europejskiego Forum Cyberbezpieczeństwa - CYBERSEC 2019 odbywa się pod hasłem „Securing the World's Digital DNA", nawołującym do kształtowania fundamentów cyfrowego świata w sposób, który zapewni jego bezpieczeństwo oraz warunki sprzyjające do dalszego rozwoju technologicznego i gospodarczego. Cyfrowe DNA odnosi się do sposobu tworzenia i wdrażania nowych rozwiązań oraz infrastruktury cyfrowej, a także produktów i usług, mając na uwadze cyberbezpieczeństwo i poszanowanie prywatności użytkowników w całym cyklu ich życia. Jest to jednocześnie długotrwałe zobowiązanie do promowania odpowiedzialnych i świadomych zachowań opartych na zasadzie „security and privacy by design".

Patronami medialnymi wydarzenia są: CyberDefence24.pl, Defence24.pl, BiznesAlert.pl, Computerworld, DLP Expert, Do Rzeczy, EURACTIV, Forsal.pl, GazetaPrawna.pl, ISBnews, IT Reseller, ITwiz, Manager Magazine, PAP, Polska Zbrojna, Polskie Radio Katowice, Radio Silesia, Sieci, Sztucznainteligencja.org.pl, TVP3 Katowice, TVS, wGospodarce.pl, Wirtualna Polska, wPolsce.pl, Wprost.