

CROSSED SWORD ZAKOŃCZONE. CZŁONKOWIE NATO TRENOWALI ZDOLNOŚCI W OBSZARZE CYBER

Doskonalenie umiejętności współdziałania tradycyjnych oddziałów wojskowych i tych odpowiedzialnych za działanie w cyberprzestrzeni było głównym celem 6. edycji ćwiczeń Crossed Sword zorganizowanych przez NATO CCDCOE i łotewski CERT. Jak wypadli członkowie NATO w tym teście?

W Rydze odbyła się 6 edycja ćwiczeń z obszaru bezpieczeństwa Crossed Sword zorganizowane przez NATO Cooperative Cyber Defence Centre of Excellence oraz łotewski CERT. Wzięło w nich udział ponad 120 ekspertów IT, członków oddziałów wojskowych odpowiedzialnych za działania w cyberprzestrzeni, operatorzy sił specjalnych oraz policjanci.

Wydarzenie wyewoluowało z czysto technicznych warsztatów do ćwiczeń, gdzie sprawdza się zdolności do działania w cyberprzestrzeni oraz tradycyjnego prowadzenie operacji wojskowych. Nacisk został położony na sprawdzenie współpracy pomiędzy żołnierzami działającymi w środowisku wirtualnym i tymi, którzy walczą w klasycznym środowisku operacyjnym. Głównym zadaniem uczestników było wykrywanie, zapobieganie i odpowiedź na działania przeciwnika w kontekście pełnowymiarowych operacji w cyberprzestrzeni.

Dyrektor CCD COE pułkownik Tarien powiedział, że głównym uczestnikiem ćwiczeń są członkowie Red Teamów, operatorzy sił specjalnych oraz, co jest nowością, członkowie dowództw odpowiedzialnych za operacje w cyberprzestrzeni. Dodał, że Crossed Swords jest unikalne, ponieważ łączy ze sobą działania w wielu domenach przeprowadzane przez osoby pochodzące z różnych państw. W tym roku położono nacisk na połączone operacje, których efekt miał zostać wzmocniony poprzez działania w cyberprzestrzeni. Scenariusz ćwiczeń był mocno eksperymentalny, ale zarazem dążył do jak największego realizmu oraz miał być prawdziwym wyzwaniem dla uczestników.

Lauri Luht, dyrektor odpowiedzialny za kwestie techniczne w CCDCOE powiedział, że po raz pierwszy w historii ćwiczeń, uczestnicy z 6 państw utworzyli dowództwo odpowiedzialne za operacje w cyberprzestrzeni. Głównym zadaniem ćwiczeń było zrozumienie współpracy pomiędzy jednostkami z różnych środowisk oraz sposób łączenia działań w cyberprzestrzeni z konwencjonalnymi operacjami.

Crossed Swords skupi się również na technicznych aspektach cyberbezpieczeństwa. Uczestnicy przeprowadzają testy penetracyjne, cyfrową analizę śledczą oraz pracują nad świadomością operacyjną. Część z nich weźmie później udział jako członkowie Red Teamów podczas zbliżających się ćwiczeń Locked Shield. Crossed Swords łączy razem ekspertów technicznych, specjalistów od zbierania danych oraz operatorów sił specjalnych, którzy współpracują w celu osiągnięcia jednego celu. Wysoki poziom trudności problemów do rozwiązania oraz interdyscyplinarna natura ćwiczeń powodują, że Crossed Swords to jeden z najbardziej wymagających zmagających. W tym roku wzięło w nich

udział 120 uczestników z 26 państw.

Dr Rain Ottis komentując ćwiczenia powiedział, że uczestnicy muszą podjąć decyzję dotyczące środków jakie mają zostać wykorzystane do osiągnięcia konkretnych efektów. Konieczne jest znalezienie najbardziej korzystnego podejścia. W trakcie Crossed Swords, uczestnicy mają możliwość eksperymentowania oraz możliwość popełniania błędów. To jest najskuteczniejszy rodzaj nauki – dodał.

Zgodził się z tym stwierdzeniem pomysłodawca ćwiczeń doktor Bernhards Blumbergs z CERT.LV, który dodał, że porażki są najlepszą lekcją. Jego zdaniem charakter ćwiczeń, które stawiają przed uczestnikami takie zadania jak np. atrybucja ataków oraz wymagają współpracy jednostek z wielu różnych obszarów i państw zmuszają uczestników do wyjścia z tzw. strefy komfortu. To wtedy proces uczenia się jest najefektywniejszy – zakończył.

Kolejnym atutem ćwiczeń jest bliska współpraca z sektorem prywatnym, który aktywnie uczestniczy w wydarzeniu oraz dostarcza cennych wskazówek odnośnie współpracy z wojskiem. Ich nowoczesne technologie oraz wiedza są kluczowe, aby ćwiczenia w jak największym stopniu odpowiadały prawdziwym wyzwaniom.