ĆWICZENIA "LOCKED SHIELDS" PRZYGOTOWANIEM DO PRZYSZŁYCH CYBERWOJEN

Zakończone przed paroma dniami tegoroczne manewry "Locked Shields" to największe międzynarodowe ćwiczenia cyberbezpieczeństwa. Wzięło w nich udział 550 specjalistów z 26 krajów. Ich znaczenie dla obronności państw NATO jest nie do przecenienia.

"Locked Shields", organizowane przez Centrum Doskonalenia Obrony Cybernetycznej NATO w Tallinnie (NATO CCD COE) to ćwiczenia, które podnoszą kwalifikacje specjalistów od cyberbezpieczeństwa. Mowa o ekspertach, którzy na co dzień zajmują się zabezpieczaniem sieci agencji narodowych oraz przedsiębiorstw prywatnych.

W tym roku ćwiczenia "Locked Shields" poświęcone były badaniu poziomu bezpieczeństwa fizycznie istniejących systemów, ponieważ to one mają największy wpływ na nasze życie i środowisko. Zespoły miały za zadanie utrzymanie sieci i serwisów fikcyjnego państwa – Berylii, która poddawana była atakom. W zakres zadań wchodziło m.in. raportowanie i reagowanie na incydenty, rozwiązywanie zaistniałych problemów, a także pokonywanie przeszkód natury prawnej i skuteczne informowanie mediów o sytuacji.

- Jeżeli nie rozumiesz w pełni, jak wyglądają cyberataki, nie możesz być przygotowany na nie. Dlatego ćwiczenia "Locked Shields" są tak wyjątkowe i naprawdę szkolą specjalistów w pełnym zakresie. Są strony odpowiadające za ataki oraz strony odpowiadające za obronę. To podnosi kompetencje każdej z nich. Łatwiej tego wszystkiego dokonać w zamkniętej przestrzeni, gdzie wszystko może być dokładnie przeanalizowane – mówi Mehis Hakkaj z firmy Clarified Security, szef grupy „Czerwonej".

Jak wyglądają ćwiczenia? Dyrektor techniczny ds. ćwiczeń w NATO CCD COE Aare Reintamm tłumaczy, że sieci używane do manewrów są zbudowane w sposób podobny do tych realnie istniejących. - Stosujemy technologie oraz urządzenia normalnie występujące np. w biurach. Mamy zainstalowaną infrastrukturę biura, maszyny z systemem Windows, SAP. Oprócz tego serwery z plikami do wymiany danych, serwery ze stronami WWW, telefony komórkowe. Wszystko to postawione i skonfigurowane w wirtualnej sieci, na której zostały przeprowadzone ćwiczenia.

Uczestnicy starają się naśladować zachowania występujące w prawdziwym świecie. Zawodnicy nie tylko muszą odpowiednio bronić swojej infrastruktury, ale także odpowiadać na reakcje prawne czy opinii publicznej, które są odpowiedzią na działania w sieci. - Ważna jest obecność takich komponentów w ćwiczeniach. Pozwalają one wtedy przygotować uczestników na realne zagrożenia – komentuje Thomas Svensson, specjalista ds. wstrzykiwania kodu i konsultant z zakresu cyberbezpieczeństwa.

Ekipa ze Słowacji została zwycięzcą tegorocznej edycji "Locked Shields". W ocenie jurorów najlepiej poradziła sobie też z zadaniem informowania opinii publicznej. Niemiecka drużyna z kolei okazała się bezkonkurencyjna w dziedzinie informatyki śledczej, rozwiązując problemy związane ze

wstrzykiwaniem kodu przez złośliwe oprogramowanie. Zespół NATO Computer Incident Response Capability (NCIRC) opracował najlepszą analizę prawną, natomiast Czesi zademonstrowali największą biegłość w zadaniach dotyczących scenariusza ćwiczeń.

- Myślę, że nie będzie w przyszłości wojen, w których nie będzie walk przeprowadzanych w cyberprzestrzeni. Strefa cyberwojen zostanie włączona na stałe we wszystkie współczesne i przyszłe konflikty. To oczywiście jest powód, dla których takie ćwiczenia jak Locked Shields mają miejsce – podsumowuje Sven Sakkov, Dyrektor NATO CCD COE.

Źródło: NATO CCDCOE