MOBILNE CENTRUM CYBERBEZPIECZEŃSTWA IBM W WARSZAWIE

IBM pokazał w Warszawie mobilne centrum bezpieczeństwa. Ciężarówka IBM z naczepą skrywa nowoczesne centrum gotowe do wykrywania i reagowania na zagrożenia z sieci. IBM X-Force Command Cyber Tactical Operations Center (C-TOC) obecnie przemierza Europę z serią symulacji ataków hakerskich na żywo oraz wsparciem na żądanie w zakresie cyberbezpieczeństwa. Ważnym zadaniem mobilnego centrum IBM jest również edukacja i rozwój kompetencji w obszarze bezpieczeństwa.

IBM X-Force C-TOC to w pełni funkcjonalne Centrum Operacji Bezpieczeństwa na kołach, wzorowane na Centrach Operacji Taktycznych zarządzanych przez wojsko i zespoły do szybkiego reagowania na incydenty w sieci. Mobilne centrum w dużej naczepie ciężarówki posiada kontrolowane gestem „centrum dowodzenia", centrum danych oraz stanowiska dla ponad dwudziestu operatorów, analityków i pozostałych pracowników C-TOC.

"Projekt centrum powstał w USA, ale z myślą o Europie. Rozpoczęło ono pracę w tym regionie w styczniu. X-Force był już w Londynie, Amsterdamie, Madrycie, Sztokholmie – w sumie w 12 lokalizacjach" - zaznaczył w rozmowie z PAP dyrektor IBM ds. X-Force Command C-TOC Erno Doorenspleet.

"W tym momencie to jedyne takie mobilne centrum, jakie posiadamy. Stworzyliśmy je jako prototyp, by zobaczyć jak duży jest popyt na tego typu rozwiązania. Z tego, co usłyszałem zainteresowanie jest dość duże. Pod koniec sierpnia spojrzymy na dotychczasowe osiągnięcia pierwszego X-Force i zastanowimy się nad rozwinięciem projektu – być może drugim mobilnym centrum, a może zupełnie innym podejściem" - ocenił Doorenspleet.

Mobilne centrum IBM może pracować w różnych środowiskach. Posiada tryb automatycznego podtrzymania zasilania, własną łączność satelitarną i naziemną. Wszystko to tworzy sterylną i bezpieczną sieć do śledzenia i reagowania na zagrożenia. Jednocześnie C-TOC jest najnowocześniejszą platformą do prowadzenia szkoleń z zakresu cyberbezpieczeństwa.

Dawniej zespoły ds. cyberbezpieczeństwa skupiały się na wykrywaniu zagrożeń i ochronie przed incydentami. Jednak obecnie, wraz z rozwojem metod działania hakerów, firmy i organizacje coraz częściej dostrzegają potrzebę planowania i organizowania ćwiczeń na wypadek realnego ataku. Badanie dotyczące kosztów naruszenia bezpieczeństwa danych z 2018 roku wykazało, że firmy, które potrafią skutecznie reagować na ataki i podjąć kroki naprawcze w ciągu 30 dni, mogą zaoszczędzić ponad 1 mln USD na całkowitym koszcie naruszenia danych. Jednocześnie mniej niż 25% respondentów potwierdza, że ich firma posiada plan skoordynowanego reagowania na incydenty.

"Od stycznia przeszkoliliśmy już ponad 700 osób. Ciężarówka ma 18 stanowisk, więc widać, że projektem zainteresowała się już duża liczba firm. Przeciętny tydzień IBM X-Force to około dziesięciu

3,5-godzinnych sesji, po dwie dziennie" - wyliczał Doorenspleet.

"Obecnie nie ma znaczenia, z jakiego sektora jest firma. Wszystkie powinny przyjrzeć się swojej polityce cyberbezpieczeństwa, niezależnie czy odpowiadają za transakcje finansowe, tworzą produkty, czy świadczą usługi. Wszyscy muszą wiedzieć, jak reagować w sytuacji cyberataku" - wskazał dyrektor IBM.

Mobilne centrum cyberbezpieczeństwa IBM C-TOC może być wykorzystywane na wiele sposobów:

Symulacje cyberataków i stała gotowość: Udoskonalanie sposobów reagowania na skutki poważnych ataków w sieci ma coraz większe znaczenie. C-TOC pomaga firmom szkolić wewnętrzne zespoły techniczne i kryzysowe na wypadek incydentów. W tym celu prowadzone są symulacje oparte o prawdziwe scenariusze ataków hakerskich oraz strategie ochrony firmy i jej zasobów.

Wsparcie bezpieczeństwa na miejscu: IBM C-TOC powstał z myślą o jego wykorzystywaniu jako Centrum Operacji Bezpieczeństwa na żądanie dla klientów. Jednym z możliwych przykładów jego zastosowania jest wsparcie imprez sportowych lub innych dużych wydarzeń, które mogą wymagać dodatkowych zasobów z obszaru cyberbezpieczeństwa.

Edukacja: C-TOC oferuje jedną z najbardziej realistycznych symulacji związanych z bezpieczeństwem cybernetycznym w branży. Jego możliwości są prezentowane podczas wizyt na uczelniach i podczas wydarzeń branżowych. To również szansa na przekonanie młodych osób do związania swojej kariery zawodowej z obszarem cyberbezpieczeństwa.

Oczekiwania względem cyberbezpieczeństwa wciąż rosną

IBM Security określa gotowość i reagowanie na incydenty jako niedostatecznie rozwinięty obszar wartego 114 mld USD rynku cyberbezpieczeństwa. W 2016 roku IBM zainwestował 200 mln USD w nowe centra reagowania, usługi i oprogramowanie. Od tego czasu w angażujących szkoleniach z zakresu cyberbezpieczeństwa w centrum w Cambridge (USA) wzięło udział ponad 2000 osób. Po uruchomieniu centrum X-Force C-TOC szkolenia są kierowane bezpośrednio do klientów.

Budowę mobilnego centrum IBM C-TOC poprzedziły konsultacje z dziesiątkami ekspertów z różnych branż, od ratowników medycznych po oficerów wojskowych. C-TOC, przy wsparciu wiedzy eksperckiej IBM z zakresu bezpieczeństwa, pozwala uczestnikom symulacji kryzysowej sprawdzić się w roli lidera – przez odejście od codziennej rutyny organizacyjnej i wejście w strukturę zarządzania kryzysowego, tak żeby być przygotowanym na każdy ruch ze strony cyberprzestępcy.

Szkolenie w C-TOC obejmuje również „Laboratorium najlepszych praktyk cybernetycznych” z realnymi przykładami opartymi na doświadczeniach klientów. Mobilne centrum IBM daje firmom możliwość uczestnictwa w angażującej i realistycznej symulacji cyberataku, która sprawdza reakcję zespołu w sytuacji kryzysowej. Oto niektóre przykłady scenariuszy ataku:

Ox Response Challenge to symulacja opracowana z myślą o kadrze kierowniczej. Szerokie grono interesariuszy działa w realistycznym środowisku kooperacji, w którym zespół musi odpowiednio zareagować na atak w wymiarze technicznym, prawnym, PR i komunikacji.

OpRed Escape. Uczestnik symulacji wciela się w rolę cyberprzestępcy i uczy się myśleć jak haker. Staje na pozycji atakującego. Uczy się, jak przestępcy włamują się do sieci i zdobywa praktyczne doświadczenie ze stosowania złośliwego oprogramowania.

Cyber War Game: w tym scenariuszu uczestnicy symulacji wykrywają atak cybernetyczny kierowany przez grupę hakerów na fikcyjną korporację. Pracując w symulowanej sieci korporacyjnej C-TOC,

uczestnicy korzystają z narzędzi technicznych do identyfikacji zagrożeń i ich neutralizacji, a także do budowania planu reakcji i rozwijania umiejętności przywódczych i zarządzania kryzysowego.

Uzupełniające operacje cyberbezpieczeństwa

IBM zaprojektował C-TOC również z myślą o szybkim rozszerzeniu wsparcia na miejscu u klientów, w sytuacjach gdy ich potrzeby w zakresie cyberbezpieczeństwa szybko wzrosną. Cyberprzestępcy nieustannie poszukują ważnych wydarzeń i momentów, które sprzyjają atakom, wykorzystując zwiększone zainteresowanie, transfery pieniężne i aktywności w sieci, tak aby uzyskać jeszcze większe korzyści.

Podczas dużych imprez coraz częściej obok gotowości służb ratunkowych czy gwarancji bezpieczeństwa publicznego pojawia się także potrzeba zapewnienia cyberbezpieczeństwa. W takich przypadkach IBM może udostępnić mobilne centrum C-TOC, aby na miejscu pomóc nie tylko w przygotowaniu, ale także w zapewnieniu izolowanej sieci i kontroli bezpieczeństwa.

Umiejętności i podnoszenie świadomości

Niedobór specjalistów ds. cyberbezpieczeństwa stanowi poważną przeszkodę w branży. Według prognoz do 2022 roku niedobór pracowników z takimi umiejętnościami może wynieść blisko 2 miliony osób. Zachęcanie młodych ludzi do rozwoju kariery zawodowej w tym obszarze, a także podnoszenie kwalifikacji obecnych specjalistów ds. cyberbezpieczeństwa to kolejne dwa ważne zadania, przed którymi stoją specjaliści IBM Security.

Źródło: PAP/IBM