Agencja Unii Europejskiej
ds. Cyberbezpieczeństwa
Agamemnonos 14,
Chalandri 15231| Attiki| Grecja
Tel.: +30 28 14 40 9711
e-mail: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Testowanie odporności europejskiego sektora opieki zdrowotnej

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) zorganizowała ćwiczenia w zakresie cyberbezpieczeństwa w celu przetestowania reakcji na ataki na infrastrukturę i służby opieki zdrowotnej w UE.

Aby zapewnić zaufanie obywateli do dostępnych im usług medycznych i infrastruktury medycznej, służby zdrowia powinny sprawnie działać przez cały czas. Gdyby usługi i infrastruktura zdrowotna w Europie stały się przedmiotem poważnego ataku cybernetycznego, jak wyglądałaby nasza reakcja i koordynacja działań zarówno na szczeblu krajowym, jak i unijnym, aby ograniczyć liczbę incydentów zapobiec ich eskalacji?

Na to pytanie uczestnicy ćwiczeń Cyber Europe 2022 próbowałli udzielić odpowiedzi w oparciu o fikcyjny scenariusz. Program pierwszego dnia obejmował kampanię dezinformacyjną dotyczącą manipulowania wynikami laboratoryjnymi oraz cyberataków wymierzonych w europejskie sieci szpitalne. Scenariusz drugiego dnia zakładał ogólnounijny kryzys cybernetyczny w połączeniu z bezpośrednim zagrożeniem wycieku medycznych danych osobowych oraz kolejną kampanię mającą na celu dyskredytację wyrobu medycznego do implantacji pod rzekomym zarzutem jego słabości.

Dyrektor wykonawczy Agencji Unii Europejskiej ds. Cyberbezpieczeństwa **Juhan Lepassaar** stwierdził: *„ Nasze wyzwania są obecnie tak samo złożone, jak nasz połączony świat. Dlatego też głęboko wierzę, że musimy zgromadzić wszystkie dane wywiadowcze, którymi dysponujemy w UE, aby dzielić się fachową wiedzą. Wzmocnienie naszej odporności w zakresie cyberbezpieczeństwa jest jedyną właściwą drogą, jeśli chcemy chronić nasze służby i infrastrukturę opieki zdrowotnej, a docelowo zdrowie wszystkich obywateli UE.”*

Ogólnoeuropejskie ćwiczenia zorganizowane przez ENISĘ zgromadziły łącznie 29 państw, zarówno z Unii Europejskiej, jak i Europejskiego Stowarzyszenia Wolnego Handlu (EFTA), a także agencje i instytucje UE, ENISA, CERT-UE Komisji Europejskiej, Europol i Europejską Agencję Leków (EMA). W ciągu dwóch dni najnowszej edycji Cyber Europe ponad 800 ekspertów ds. cyberbezpieczeństwa wzięło udział w działaniach mających na celu monitorowanie dostępności i integralności systemów.

Czy możemy wzmocnić cyberodporność unijnej opieki zdrowotnej?

Uczestnicy biorący udział w złożonych ćwiczeniach byli zadowoleni ze sposobu postępowania z incydentami i reakcji na fikcyjne ataki.

Obecnie należy przeprowadzić analizę procesu i wyników różnych aspektów ćwiczeń w celu uzyskania realistycznego zrozumienia potencjalnych luk lub słabości, które mogą wymagać środków łagodzących. Radzenie sobie z takimi atakami wymaga różnych poziomów kompetencji i procesów, które obejmują skuteczną i skoordynowaną wymianę informacji, dzielenie się wiedzą na temat konkretnych incydentów oraz sposób monitorowania sytuacji, która może eskalować w przypadku ogólnego ataku. Należy również przeanalizować rolę sieci CSIRT (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego) na szczeblu UE i standardowych procesów operacyjnych grupy CyCLONe.

Pogłębiona analiza zostanie opublikowana w sprawozdaniu z działań następczych. Ustalenia te posłużą jako podstawa przyszłych wytycznych i dalszych usprawnień w celu wzmocnienia odporności sektora opieki zdrowotnej na cyberataki w UE.

O ćwiczeniach Cyber Europe

Ćwiczenia Cyber Europe to organizowane na dużą skalę symulacje incydentów cyberbezpieczeństwa, które przeradzają się w ogólnounijne kryzysy cyberbezpieczeństwa. Ćwiczenia te stanowią okazję do przeanalizowania zaawansowanych cyberincydentów i zareagowania na trudne sytuacje zakłócające ciągłość działania i wymagające zarządzania kryzysowego.

ENISA zorganizowała już pięć ogólnoeuropejskich ćwiczeń w dziedzinie cyberbezpieczeństwa w latach 2010, 2012, 2014, 2016 i 2018. Odbywają się one zazwyczaj co dwa lata, ale edycja 2020 została odwołana ze względu na pandemię COVID-19.

Nieodłącznym elementem ćwiczeń jest współpraca międzynarodowa wszystkich uczestniczących organizacji –w tej współpracy bierze udział większość państw europejskich. Jest to elastyczne doświadczenie szkoleniowe: od jednego analityka do całej organizacji, ze scenariuszami opt-in i opt-out, gdzie uczestnicy mogą dostosować ćwiczenie do swoich potrzeb.

Dalsze informacje

Cyber Europe 2022

Ćwiczenia cybernetyczne – temat ENISA

Cyber Europe 2018 – raport z działań

Kontakt:

Pytania dotyczące prasy i wywiadów prosimy kierować na press(at)enisa.europa.eu