DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Comunicat de presă: Directoratul a participat la exercițiul cibernetic Cyber Europe 2022, care testează reziliența sectorului european al sănătății

București, 9 iunie 2022

Directoratul Național de Securitate Cibernetică (DNSC) a participat în perioada 8-9 iunie 2022 la exercițiul de securitate cibernetică Cyber Europe 2022, organizat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA). Obiectivul principal al ediției din 2022 a fost testarea răspunsului la atacurile asupra infrastructurilor și serviciilor de sănătate ale UE.

Pentru a asigura încrederea cetățenilor în serviciile și infrastructurile medicale care le stau la dispoziție în Europa, serviciile de sănătate trebuie să funcționeze fără întrerupere. În situația în care acestea ar fi supuse unui atac cibernetic major, cum am reacționa și cum am coordona răspunsul nostru, atât la nivel național, cât și la nivelul UE, pentru a atenua incidentele și a împiedica o escaladare a situației? Aceasta este întrebarea la care a încercat să răspundă Cyber Europe 2022, utilizând un scenariu fictiv.

În prima zi a avut loc o campanie de dezinformare, folosind rezultate de laborator manipulate și un atac cibernetic asupra rețelelor spitalicești europene. În cea de-a doua zi, scenariul s-a transformat într-o criză cibernetică la nivelul UE, cu amenințarea iminentă de publicare a datelor medicale cu caracter personal, iar într-o altă campanie s-a încercat discreditarea unui dispozitiv medical implantabil, exploatând vulnerabilitatea acestuia.

„Cyber Europe 2022 reprezintă o oportunitate excelentă de a consolida reziliența cibernetică a sectorului medical la nivel național și la nivelul UE, în modul de exercițiu, prin adresarea provocărilor generate de scenariile avansate de atacuri cibernetice. Pentru Directoratul Național de Securitate Cibernetică eforturile pentru asigurarea unui nivel ridicat de maturitate și reziliență cibernetică a sectorului sănătății reprezintă una dintre prioritățile de top pentru acest an”, a precizat **Dan Cîmpean**, Director al DNSC.

Totodată, directorul executiv al ENISA, **Juhan Lepassaar**, a declarat: „Complexitatea provocărilor la care trebuie să facem față este în prezent proporțională cu complexitatea lumii conectate în care trăim. Din acest motiv, sunt ferm convins că trebuie să colectam toate informațiile de care dispunem în UE pentru a ne împărtăși expertiza și cunoștințele. Consolidarea rezilienței noastre în materie de securitate cibernetică este singura cale de urmat dacă dorim să ne protejăm serviciile și infrastructurile de sănătate și în cele din urmă, sănătatea tuturor cetățenilor UE.”

Exercițiul paneuropean organizat de ENISA a reunit în total 29 de țări, atât din Uniunea Europeană, cât și din Asociația Europeană a Liberului Schimb (AELS), precum și din agențiile și instituțiile UE - ENISA, CERT-UE al Comisiei Europene, Europol și Agenția Europeană pentru Medicamente (EMA). Peste 800 de experți în domeniul securității cibernetice s-au ocupat de monitorizarea disponibilității și integrității sistemelor pe parcursul celor două zile in cadrul acestei ultime ediții a Cyber Europe.

Putem consolida reziliența cibernetică a sectorului sănătății din UE?

Participanții la acest exercițiu complex au fost mulțumiți de modul în care au fost soluționate incidentele și de răspunsul la atacurile fictive.

Acum urmează a fi efectuată analiza procesului și a rezultatelor diferitelor aspecte ale exercițiilor pentru a se ajunge la o înțelegere realistă a eventualelor lacune sau puncte slabe care ar putea

necesita măsuri de diminuare a riscurilor. Gestionarea unor astfel de atacuri necesită niveluri diferite de competențe și procese diferite, care includ schimbul de informații eficient și coordonat, schimbul de cunoștințe cu privire la incidente specifice și modul de monitorizare a unei situații în curs de escaladare în cazul unui atac generalizat. De asemenea, trebuie analizat rolul CSIRT Network (rețeaua structurilor de tip CSIRT/CERT) la nivelul UE și procedurile standard de operare ale grupului CyCLONe.

Această analiză aprofundată va fi publicată în raportul post-exercițiu. Rezultatele analizei vor servi drept bază pentru orientări viitoare și pentru îmbunătățiri suplimentare în vederea consolidării rezilienței sectorului sănătății din UE împotriva atacurilor cibernetice.

Despre exercițiile Cyber Europe

Exercițiile „Cyber Europe" sunt simulări de incidente de securitate cibernetică la scară largă care, dacă ar fi reale, s-ar putea transforma în crize cibernetice la nivelul întregii UE. Exercițiile oferă ocazia de a analiza incidente grave de securitate cibernetică și de a rezolva situații complexe, permițând în același timp continuitatea activității și de management al crizelor.

Încă de la înființare, DNSC (CERT-RO înainte de septembrie 2021) a participat la toate edițiile exercițiului paneuropean organizat de ENISA (2012, 2014, 2016 și 2018), având rolul de coordonator național. De obicei, evenimentul are loc o dată la doi ani, dar evenimentul din 2020 a fost anulat din cauza pandemiei de COVID-19.

Cooperarea internațională între toate organizațiile participante este inerentă exercițiului, cu majoritatea țărilor europene participând la acesta. Exercițiul este o experiență de învățare flexibilă: de la un singur analist la o întreagă organizație, cu scenarii de participare și neparticipare și în care participanții pot personaliza exercițiul în funcție de nevoi.

Informații suplimentare

Cyber Europe 2022

Tema Exerciții cibernetice – ENISA

Cyber Europe 2018 – Raport post-exercițiu

Persoană de contact pentru presă: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866