Den Europæiske Unions Agentur
for Cybersikkerhed
Agamemnonos 14,
Chalandri 15231| Attiki|
Grækenland
Tlf.: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Afprøvning af modstandsdygtigheden i det Europæiske sundhedsvæsen

Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) tilrettelagde en cybersikkerhedsøvelse for at teste, hvordan angreb på EU's infrastrukturer og tjenester på sundhedsområdet håndteres.

For at sikre at borgerne har tillid til de lægetjenester og den infrastruktur, de har adgang til, bør sundhedstjenesterne altid fungere. Hvis tjenesterne og infrastrukturerne på sundhedsområdet i Europa blev udsat for et større cyberangreb, hvordan ville vi så reagere og koordinere indsatsen på både nationalt plan og EU-plan for at begrænse hændelserne og forhindre en eskalering?

Det er det spørgsmål, Cyber Europe 2022 forsøgte at finde svar på ved hjælp af et opdigtet scenarie. Den første dag omfattede en desinformationskampagne med manipulerede laboratorieresultater og et cyberangreb rettet mod europæiske hospitalsnetværk. På anden dagen eskalerede scenariet til en EU-dækkende cyberkrise med en overhængende trussel om offentliggørelse af medicinske oplysninger, og der blev gennemført en anden kampagne, der havde til formål at miskreditere medicinsk implantabelt udstyr med en påstand om, at det udgjorde en sårbarhed.

Juhan Lepassaar, administrerende direktør for EU's Agentur for Cybersikkerhed, sagde: *"Kompleksiteten i vores udfordringer er nu proportional med kompleksiteten i vores sammenbundne verden. Jeg er derfor overbevist om, at vi er nødt til at samle alle de efterretninger, vi har i EU, for at dele vores ekspertise og viden med hinanden. At styrke vores modstandsdygtighed over for cybertrusler er den eneste måde, hvorpå vi kan beskytte vores sundhedstjenester og -infrastrukturer og i sidste ende alle EU-borgeres sundhed."*

Den fælleseuropæiske øvelse, der blev tilrettelagt af ENISA, omfattede i alt 29 lande fra både Den Europæiske Union og Den Europæiske Frihandelssammenslutning (EFTA) samt EU's agenturer og institutioner, ENISA, Europa-Kommissionen, CERT-EU, Europol og Det

Europæiske Lægemiddelagentur (EMA). Over 800 cybersikkerhedseksperter arbejdede med at overvåge systemernes tilgængelighed og integritet i løbet af de to dage, den seneste udgave af Cyber Europe varede.

Kan vi styrke cyberrobustheden inden for EU's sundhedssystem?

De, der deltog i den komplekse øvelse, var tilfredse med den måde hændelserne og de fiktive angreb blev håndteret på.

Nu skal processen og resultaterne af de forskellige aspekter af øvelserne analyseres for at få en realistisk forståelse af potentielle mangler eller svagheder, som kan kræve afbødende foranstaltninger. At håndtere sådanne angreb kræver forskellige kompetenceniveauer og processer, hvilket omfatter effektiv og koordineret informationsudveksling, udveksling af viden om specifikke hændelser, og om hvordan man overvåger en situation, der er ved at eskalere under et generelt angreb. Det er også nødvendigt at se nærmere på den rolle, EU's CSIRT-netværk og CyCLONe-gruppens standarddriftsprocesser (SOP'er) spiller.

Den mere indgående analyse vil blive offentliggjort i en opfølgende rapport. Resultaterne vil danne grundlag for fremtidige retningslinjer og yderligere forbedringer, som skal styrke sundhedsvæsenets modstandsdygtighed over for cyberangreb i EU.

Om Cyber Europe-øvelser

"Cyber Europe"-øvelser er simuleringer af omfattende cybersikkerhedshændelser, der eskalerer til cyberkriser i hele EU. Øvelserne giver mulighed for at analysere avancerede cybersikkerhedshændelser og håndtere komplekse situationer, der vedrører forretningskontinuitet og krisestyring.

ENISA har allerede afholdt fem fælleseuropæiske cyberøvelser i 2010, 2012, 2014, 2016 og 2018. Arrangementet finder normalt sted hvert andet år, men blev aflyst i 2020 på grund af covid-19-pandemien.

Internationalt samarbejde mellem alle deltagende organisationer indgår i spilscenariet, som de fleste europæiske lande deltager i. Det handler om en fleksibel læringsproces, der omfatter alt fra en enkelt analytiker til en hel organisation, med opt-in- og opt-out-scenarier, og hvor deltagerne kan tilpasse øvelsen til deres behov.

Mere information

Cyber Europe 2022

Cyber Exercises – ENISA-emne

Cyber Europe 2018 – opfølgende rapport

Kontakt:

For spørgsmål, der vedrører presse og interviews, kontakt press(at)enisa.europa.eu