Europeiska unionens
cybersäkerhetsbyrå
Agamemnonos 14,
Chalandri 15231| Attiki| Grekland
Tfn: +30 28 14 40 9711
E-post: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Testning av den europeiska hälso- och sjukvårdssektorns resiliens

Europeiska unionens cybersäkerhetsbyrå (Enisa) har anordnat en cybersäkerhetsövning för att testa hur angrepp på EU:s infrastruktur och tjänster på hälso- och sjukvårdsområdet kan hanteras.

För att säkerställa medborgarnas förtroende för medicinska tjänster och medicinsk infrastruktur som de har tillgång till bör hälso- och sjukvården alltid fungera. Om tjänsterna och infrastrukturen på hälso- och sjukvårdsområdet i Europa utsattes för ett större cyberangrepp, hur skulle vi reagera och samordna oss, både på nationell nivå och EU-nivå, för att begränsa omfattningen av incidenterna och förhindra en upptrappning?

Syftet med Cyber Europe 2022 var att besvara denna fråga med hjälp av ett fiktivt scenario. Första dagen genomfördes en desinformationskampanj med manipulerade laboratorieresultat och ett cyberangrepp på europeiska sjukhusnätverk. Andra dagen trappades scenariot upp till en EU-omfattande cyberkris med ett överhängande hot om offentliggörande av personliga medicinska uppgifter och ytterligare en kampanj som utformats för att skapa misstro mot ett medicinskt implantat genom ett påstående om sårbarhet.

Juhan Lepassaar, verkställande direktör för Europeiska unionens cybersäkerhetsbyrå, sade följande: *Komplexiteten i våra utmaningar står nu i proportion till komplexiteten i vår sammanlänkade värld. Jag är därför fast övertygad om att vi behöver samla allt vetande vi har i EU för att dela med oss av vår expertis och kunskap. Vi kan bara skydda våra tjänster och vår infrastruktur på hälso- och sjukvårdsområdet och i slutändan hälsan för alla EU-medborgare genom att stärka vår resiliens när det gäller cybersäkerhet.*

I den Europaomfattande övning som anordnades av Enisa deltog totalt 29 länder från både EU och Europeiska frihandelssammanslutningen (Efta) samt EU:s organ och institutioner, Enisa, Europeiska kommissionen, CERT-EU, Europol och Europeiska läkemedelsmyndigheten (EMA).

Över 800 cybersäkerhetsexperter arbetade med att övervaka systemens tillgänglighet och integritet under de två dagar som denna senaste omgång av Cyber Europe pågick.

Kan vi stärka cyberresiliensen inom EU:s hälso- och sjukvård?

De som deltog i den komplexa övningen var nöjda med hur incidenterna och de fiktiva angreppen hanterades.

Nu behöver processen och resultaten av de olika aspekterna av övningarna analyseras så att man får en realistisk förståelse av de potentiella luckor eller svagheter som kan kräva åtgärder för begränsning av incidenter. Att hantera sådana angrepp kräver olika nivåer av kompetens och processer som inbegriper effektivt och samordnat informationsutbyte samt utbyte av kunskap om specifika incidenter och om hur man övervakar en situation som håller på att trappas upp i händelse av ett utbrett angrepp. Rollen för EU:s nätverk av enheter för hantering av it-säkerhetsincidenter (CSIRT) och CyCLONe-gruppens standardprocesser behöver också granskas.

Den fördjupade analysen kommer att offentliggöras i erfarenhetsrapporten. Resultaten kommer att ligga till grund för framtida vägledning och ytterligare förbättringar som syftar till att stärka hälso- och sjukvårdssektorns resiliens mot cyberangrepp inom EU.

Om Cyber Europe-övningarna

Cyber Europe-övningarna är simuleringar av storskaliga cybersäkerhetsincidenter som utvecklas till EU-övergripande cyberkriser. Övningarna ger möjlighet att analysera svåra cybersäkerhetsincidenter och hantera komplexa situationer som rör driftskontinuitet och krishantering.

Enisa har redan anordnat fem Europaomfattande cyberövningar, som ägde rum år 2010, 2012, 2014, 2016 och 2018. Övningarna genomförs i regel vartannat år, men ställdes in 2020 på grund av covid-19-pandemin.

Internationellt samarbete mellan samtliga deltagande organisationer ingår i spelscenariot, där de flesta europeiska länder deltar. Simuleringen kan genomföras på många olika sätt: den kan handla om alltifrån en enskild analytiker till en hel organisation, med opt-in- och opt-out-scenarier, och deltagarna kan anpassa övningen till sina behov.

Mer information

Cyber Europe 2022

Cyberövningar – Enisa-ämne

Cyber Europe 2018 – erfarenhetsrapport

Kontakter:

För frågor som rör press och intervjuer, kontakta press(at)enisa.europa.eu