Euroopan unionin
kyberturvallisuusvirasto
Agamemnonos 14,
Chalandri 15231| Attiki| Kreikka
Puh.: +30 28 14 40 9711
Sähköposti:
info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Euroopan terveydenhuoltoalan häiriönsietokyvyn testaaminen

Euroopan unionin kyberturvallisuusvirasto (ENISA) järjesti kyberturvallisuusharjoituksen, jossa testattiin valmiuksia reagoida EU:n terveydenhuollon infrastruktuureihin ja palveluihin kohdistuviin hyökkäyksiin.

Jotta voidaan varmistaa kansalaisten luottamus saatavilla oleviin terveydenhuoltopalveluihin ja infrastruktuuriin, terveyspalvelujen tulisi toimia kaikkina aikoina. Jos Euroopan terveyspalvelut ja -infrastruktuurit olisivat suuren kyberhyökkäyksen kohteena, miten lievittäisimme ongelmia ja estäisimme tilanteen kärjistymistä kansallisesti ja EU:ssa?

Tähän kysymykseen pyrittiin saamaan vastaus Cyber Europe 2022 -harjoituksissa kuvitteellisen skenaarion avulla. Ensimmäisenä päivänä esiteltiin disinformaatiokampanja laboratoriotulosten manipuloinnista ja verkkohyökkäys, joka kohdistui eurooppalaisiin sairaalaverkkoihin. Toisena päivänä skenaario kärjistyi EU:n laajuiseksi kyberkriisiksi, jossa oli välitön uhka ihmisten terveystietojen vuotamisesta. Kyberkriisiin liittyi myös kampanja, jonka tarkoituksena oli horjuttaa implantoitavan lääkinnällisen laitteen luotettavuutta väitteillä siihen liittyvästä haavoittuvuudesta.

EU:n kyberturvallisuusviraston pääjohtaja **Juhan Lepassaar** totesi: *”Haasteidemme monimutkaisuus on nyt suhteessa verkottuneen maailman monimutkaisuuteen. Tämän vuoksi uskon vahvasti, että meidän on koottava yhteen kaikki tiedot EU-alueella asiantuntemuksemme jakamiseksi. Kyberturvallisuuden sietokyvyn vahvistaminen on ainoa tapa edetä, jos haluamme suojella terveyspalvelujamme ja -infrastruktuurejamme ja viime kädessä kaikkien EU:n kansalaisten terveyttä.”*

ENISAn järjestämään Euroopan laajuiseen harjoitukseen osallistui yhteensä 29 maata sekä Euroopan unionista että Euroopan vapaakauppaliitosta (EFTA) sekä EU:n virastoja ja

toimielimiä, ENISA, Euroopan komission CERT-EU-ryhmä, Europol ja Euroopan lääkevirasto (EMA). Yli 800 kyberturvallisuusasiantuntijaa seurasi järjestelmien käytettävyyttä ja eheyttä kahden päivän ajan viimeisimmässä Cyber Europe -harjoituksessa.

Voidaanko EU:n terveydenhuollon kyberuhkien sietokykyä vahvistaa?

Monitahoisen harjoituksen osanottajat olivat tyytyväisiä siihen, miten häiriötilanteita käsiteltiin ja miten kuvattuihin hyökkäyksiin reagoitiin.

Nyt on analysoitava harjoitusten prosessia ja eri näkökohtien tuloksia, jotta saadaan realistinen käsitys mahdollisista puutteista tai heikkouksista, jotka saattavat edellyttää riskejä vähentäviä toimia. Tällaisiin hyökkäyksiin reagointi edellyttää eritasoisia valmiuksia ja prosesseja, kuten tehokasta ja koordinoitua tietojenvaihtoa, tiedon jakamista erityisistä vaaratilanteista ja keinoja seurata kärjistymässä olevaa tilannetta, jos kyseessä on tavanomainen hyökkäys. Lisäksi on tarkasteltava EU:n tason tietoturvaloukkauksiin reagoivan ja niitä tutkivan CSIRT-verkoston roolia ja EU-CyCLONe-verkoston vakiotoimintaprosesseja.

Perusteellisempi analyysi julkaistaan harjoituksesta saatuja kokemuksia koskevassa raportissa. Tulokset ovat pohja tulevalle ohjeistukselle ja lisäparannuksille EU:n terveydenhuoltoalan häiriönsietokyvyn vahvistamiseksi kyberhyökkäyksiä vastaan.

Taustatietoa Cyber Europe -harjoituksista

Cyber Europe -harjoituksissa simuloidaan laajamittaisia kyberhäiriötilanteita, jotka voivat kasvaa koko EU:n kattaviksi kyberturvallisuuskriiseiksi. Harjoitusten avulla voidaan analysoida monimutkaisia häiriötilanteita ja testata organisaatioiden kykyä varmistaa toimintansa jatkuvuus ja hallita kriisitilanteita.

ENISA on aiemmin järjestänyt viisi Euroopan laajuista kyberharjoitusta vuosina 2010, 2012, 2014, 2016 ja 2018. Tapahtuma järjestetään yleensä joka toinen vuosi, mutta vuoden 2020 tapahtuma peruttiin covid-19-pandemian vuoksi.

Osallistuvien organisaatioiden kansainvälinen yhteistyö on olennainen osa harjoitusta, jossa on osallistujia useimmista Euroopan maista. Harjoitus on joustava oppimiskokemus niin yksittäisille analyytikoille kuin kokonaisille organisaatioille. Siihen sisältyy opt-in- ja opt-out-skenaarioita, ja osallistujat voivat räätälöidä harjoituksen omien tarpeidensa mukaan.

Lisätietoja

Cyber Europe 2022

Kyberturvallisuusharjoitukset – ENISA

Cyber Europe 2018 – Raportti harjoituksista saaduista kokemuksista

Yhteydenotot:

Lehdistöön ja haastatteluihin liittyvissä kysymyksissä ota yhteyttä osoitteeseen press(at)enisa.europa.eu