Cyber Europe 2018 – Paremmat valmiudet kyberkriisien varalta

Kyberturvallisuusvalmiuksia testattiin EU:n verkko- ja tietoturvaviraston kansainvälisessä harjoituksessa

Tavallisena arkipäivänä lentoaseman lähtöselvitysautomaatteihin ilmestyy yllättäen ilmoitus järjestelmähäiriöstä. Älypuhelinten matkailusovellukset lakkaavat toimimasta. Myöskään lähtöselvitysvirkailijoiden tietokoneet eivät toimi. Matkatavaroiden selvittäminen ei onnistu, eivätkä matkustajat pääse turvatarkastukseen. Kaikkialle syntyy valtavia jonoja. Lentoaseman lähtötaulujen mukaan kaikki lennot on peruutettu. Matkatavarahihnat ovat pysähtyneet, ja vain pieni osa lennoista pääsee lähtemään.

Radikaaliryhmittymä ilmoittaa ottaneensa lentoaseman kriittiset järjestelmät haltuunsa verkko- ja hybridihyökkäyksillä. Propagandakanaviensa välityksellä se levittää ääri-ideologista sanomaansa ja kehottaa kannattajiaan suoraan toimintaan.

Tämä skenaario oli lähtökohtana EU:n verkko- ja tietoturvaviraston (ENISA) pitämässä kansainvälisessä Cyber Europe 2018 -turvallisuusharjoituksessa 6.–7.6.2018. Tapahtumaan osallistui 900 kyberturvallisuuden asiantuntijaa 30 Euroopan maasta.

Cyber Europe 2018 -harjoituksen järjestämisessä oli ENISAn ohella mukana verkko- ja tietoturvallisuusviranomaisia ja -virastoja eri puolilta Eurooppaa. Tavoitteena oli parantaa kyberturvallisuusyhteisön valmiuksia havaita ja torjua laajoja turvallisuusuhkia verkossa ja tutkia sitä, miten turvallisuusongelmat leviävät maasta toiseen. Samalla organisaatiot pääsivät testaamaan sisäisiä jatkuvuus- ja kriisinhallintasuunnitelmiaan ja kriisiviestintää tiedotusvälineiden suuntaan. Harjoituksella vahvistettiin myös julkishallinnon ja yksityissektorin toimijoiden yhteistyötä.

Kaksipäiväistä turvallisuusharjoitusta johdettiin Ateenassa sijaitsevasta ENISAn päämajasta käsin. Harjoitus toteutettiin ENISAn kehittämällä Cyber Exercise Platform (CEP) -alustalla. Sen avulla luotiin integroitu virtuaaliympäristö, jossa simuloitiin tietoverkkoja uhkaavia vaaratilanteita ja uutissivustojen, sosiaalisen median kanavien, yritysten sivustojen ja turvallisuusalan blogien toimintaa. Osallistujat olivat joko omilla työpaikoillaan tai harjoitusta varten kootuissa kriisiryhmissä.

Harjoitusskenaario sisälsi todenmukaisia teknisiä ja muita ongelmatilanteita, joiden ratkaiseminen edellytti verkon ja haittaohjelmien analysointia sekä kyberrikostutkinta- ja stenografiamenetelmien käyttöä. Tilanteet oli suunniteltu niin, että ne voivat johtaa kriisiin kaikilla hallintotasoilla: niin organisaatioiden sisällä kuin paikallisella, kansallisella ja Euroopan tasolla.

”Teknologia tarjoaa valtavasti mahdollisuuksia kaikilla talouden aloilla, mutta se aiheuttaa yrityksille ja kansalaisille myös riskejä. Euroopan komission ja EU-maiden on tehtävä yhteistyötä ja hankittava tarvittavat valmiudet kyberhyökkäysten torjuntaan ja tietoverkkojen ja -järjestelmien suojaamiseen. Juuri tästä syystä ENISA aloitti Cyber Europe -harjoitukset kahdeksan vuotta sitten”, sanoo digitaalitaloudesta ja -yhteiskunnasta vastaava komissaari Mariya Gabriel.

”Vuosien mittaan harjoitus on laajentunut huomattavasti, ja siitä on tullut EU:n päätapahtuma kyberturvallisuuden alalla. Siihen osallistuu useita satoja tietoverkkoturvallisuuden asiantuntijoita koko Euroopasta. Tätä kiinnostusta on syytä hyödyntää. Olen vakuuttunut, että voimme kehittää EU:n

yhteistyömekanismeja vielä pidemmälle, jotta laajoja kyberturvallisuusongelmia voidaan torjua entistä tehokkaammin", Gabriel jatkaa.

ENISAn pääjohtaja Udo Helmbrecht varoittaa teknologian kehityksen kääntöpuolista. "Viime vuosikymmenen aikana ilmailualan tekniikka on kehittynyt valtavin harppauksin. Nykyään käytössä on lukemattomia sovelluksia ja järjestelmiä, joiden avulla voi esimerkiksi navigoida, tehdä lähtöselvityksen verkossa tai tarkastaa matkatavaroita automaattisesti. Älyteknologia säästää aikaa ja rahaa ja helpottaa matkustajien elämää. Mutta tekniikan kehittyessä kehittyvät myös verkkoturvallisuusuhat."

"Cyber Europe 2018 -harjoituksen kaltaisia tapahtumia järjestämällä ENISA parantaa EU:n kyberturvallisuutta. Euroopan maiden ja erimaalaisten organisaatioiden yhteistyö on nykyaikana oikea tapa torjua kyberuhkia, koska ne eivät rajoitu yksittäisiin maihin. ENISAn ja sen henkilöstön puolesta kiitän kaikkia, jotka olivat mukana Cyber Europe 2018 -tapahtumassa", Helmbrecht sanoo.

Harjoituksessa kävi ilmi, että osanottajat pystyivät puuttumaan vaaratilanteisiin tehokkaasti ja riittävän ajoissa, niin että pahimmat mahdolliset uhkakuvat eivät toteutuneet. Tämä osoittaa, että Euroopan kyberturvallisuussektorin toimijoiden valmiudet ovat viime vuosina parantuneet.

ENISA ja osallistujat tekevät vielä harjoituksen jälkianalyysin mahdollisten kehityskohteiden kartoittamiseksi. Sen jälkeen ENISA laatii harjoituksesta loppuraportin.

Numerotietoa Cyber Europe 2018 -harjoituksesta

Osallistujamaat: 30 maata (Alankomaat, Belgia, Bulgaria, Espanja, Irlanti, Italia, Itävalta, Kreikka, Kroatia, Kypros, Latvia, Liettua, Luxemburg, Malta, Norja, Portugali, Puola, Ranska, Romania, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tšekki, Unkari, Viro ja Yhdistynyt kuningaskunta)

Mukana olleet organisaatiot: 300

Osallistujien määrä: yli 900 kyberturvallisuuden ammattilaista

Häiriösyötteiden määrä: 23 222

Cyber Europe -harjoitukset – taustatietoa

Cyber Europe -harjoituksissa simuloidaan laajamittaisia kyberturvallisuuspoikkeamia, jotka voivat kasvaa koko EU:n kattaviksi verkko- ja tietoturvakriiseiksi. Harjoitusten avulla voidaan analysoida monimutkaisia ongelmatilanteita ja testata organisaatioiden kykyä varmistaa toimintansa jatkuvuus vakavien kriisien aikana. ENISA on aiemmin järjestänyt Euroopan laajuiset verkkoturvallisuusharjoitukset vuosina 2010, 2012, 2014 ja 2016.

Tapahtumissa on ollut osallistujia useimmista Euroopan maista. Organisaatioiden kansainvälinen yhteistyö on harjoitusten olennainen osa. Harjoitukset ovat joustavia: yksittäiset osallistujat ja kokonaiset organisaatiot voivat muokata harjoituksia tarpeidensa mukaan valitsemalla eri skenaarioista sopivimmat.