

Cyber Europe 2018 – Olgem valmis järgmiseks küberkriisiks

ELi küberturvalisuse amet ENISA korraldas rahvusvahelise küberõppuse

Kujutage ette järgmist olukorda. Lennujaamas on tavaline päev. Järsku ilmub lennule registreerimise kioskite ekraanidele teave, et süsteem ei tööta. Nutitelefonide reisirakendused ei tööta enam. Lennujaamatöötajad ei saa oma arvutites mitte midagi teha. Reisijad ei saa pagasit ära anda ega turvakontrollist läbi minna. Kõikjal on tohutud järjekorrad. Lennujaama infotahvritel näidatakse, et kõik lennud on tühistatud. Mingil teadmata põhjusel ei tööta pagasi väljastamine ja rohkem kui pooled lennud ei tohi õhku tõusta.

Väidetavalt on üks äärmusrühmitus võtnud elektrooniliste ja hübriidrünnetega üle lennujaama elutähtsad süsteemid. Rühmitus on juba tunnistanud, et nemad on intsidendi taga. Nüüd kutsuvad nad oma propagandakanalites inimesi üles tegutsema ja nende radikaalse ideoloogia omaks võtma.

Just selliste ärevate sündmustega pidid 30 riigi 900 küberturvalisuse spetsialisti 6. ja 7. juunil 2018 ELi seni kõige keerukama küberõppuse „Cyber Europe 2018“ ehk CE2018 käigus toime tulema.

Kahepäevast õppust juhtis ENISA oma peakorterist Ateenas, osalejad jäid oma tavapärasesse töökohtadesse või kogunesid kriisikeskustesse. ENISA juhtis õppust oma küberõppuste platvormi CEP kaudu, kuhu oli simulatsiooni tarvis integreeritud keskkonnana loodud virtuaalmaailm – see sisaldas intsidentidega seotud materjale, virtuaalseid uudisteportaale, sotsiaalmeediakanaleid, ettevõtete veebisaite ja turvalisusest kirjutavaid ajaveebe.

ELi küberturvalisuse amet ENISA korraldas õppuse CE2018 koostöös kogu Euroopa küberturvalisusasutuste ja -ametitega. Õppuse eesmärk on anda Euroopa küberturvalisusringkondadele võimalus veelgi suurendada mastaapsete ohtude kindlakstegemise ja elimineerimise alast suutlikkust ning parandada arusaamist intsidentide piiriülese leviku mehhanismidest.

Peamiselt aitas CE2018 organisatsioonidel katsetada toimepidevuse ja kriisiohje plaane, sealhulgas kriisikommunikatsiooni meedias, ning tugevdas riigiasutuste ja erasektori koostööd.

Õppused olid üles ehitatud reaalsest elust inspireeritud tehnilistele ja mittetehnilistele intsidentidele, millega toimetulek eeldas võrgu ja pahavara analüüsi, kriminalistikat ja steganograafiat. Kava kohaselt pidid stsenaariumi intsidendid eskaleeruma kriisiks kõigil võimalikel tasanditel: nii organisatsiooni ja kohalikul kui ka riigi ja Euroopa tasandil.

Digitaalmajanduse ja -ühiskonna volinik Mariya Gabriel tõdes, et tehnoloogia pakub kõigis majanduse sektorites lugematul hulgal võimalusi. „Kuid meie ettevõtteid ja kodanikke ähvardavad ka riskid,“ ütles volinik ja lisas: „Euroopa Komisjon ja liikmesriigid peavad tegutsema koos. Ennast tuleb varustada küberrünnete avastamiseks ning võrkude ja süsteemide kaitsmiseks vajalike töövahenditega. Sellistest kaalutlustest lähtudes tuli ENISA kaheksa aastat tagasi välja Cyber Europe'iga. Nüüdseks on sellest saanud üks suuremaid küberturvalisuse õppusi. Ühtlasi on tegu ELi tippsündmusega, mis toob kokku tuhandeid küberturbspetsialiste kogu Euroopast. Peaksime sellele edule toetudes edasi minema. Olen kindel, et saame ELi koostöömehhanisme veelgi edasi arendada, seda eeskätt suurtele küberintsidentidele reageerimise vallas.“

ENISA tegevdirektor Udo Helmbrecht selgitas: „Viimase kümne aasta jooksul on lennunduses astunud suur samm edasi areneva tehnoloogia maailma. Tänapäeval kasutatakse navigatsioonirakendusi, registreerutakse lennule internetis ja pagasi läbivaatamine on automatiseeritud. Nutivõimalused aitavad aega ja raha kokku hoida ja lihtsustavad reisijate elu. Aga nii nagu areneb tehnika, arenevad ka küberohud. Cyber Europe 2018 taoliste sündmustega tugevdab ENISA ELi küberturvalisust. See, kui Euroopa riigid ja organisatsioonid töötavad koos ühe meeskonnana, ongi tänapäevane vastus piirideta küberohtudele. Täna ENISA ja kõigi meie töötajate nimel kõiki Cyber Europe 2018 osalisi.“

Üldjoontes suutsid osalenud kõik intsidendid õigeks ajaks tulemuslikult lahendada. See näitab, et viimastel aastatel on Euroopa küberturvalisuse sektor küpsenud ja asjaosaliste valmisolek paranenud. Nüüd on ENISA-l ja osalenutel plaanis õppus tagantjärele läbi analüüsida, et teha kindlaks valdkonnad, kus on veel arenguruumi. Peagi avaldab ENISA õppuste kohta ka aruande.

Fakte

Osalenud riigid: 30; Austria, Belgia, Bulgaaria, Eesti, Hispaania, Horvaatia, Iirimaa, Itaalia, Küpros, Läti, Leedu, Luksemburg, Madalmaad, Malta, Norra, Poola, Portugal, Prantsusmaa, Rumeenia, Rootsi, Saksamaa, Kreeka, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Ühendkuningriik, Ungari.

Osalenud organisatsioonid: 300

Osalejate arv: rohkem kui 900 küberturbspetsialisti

Õppusel käsitletud intsidentide arv: 23 222

Täpsemalt Cyber Europe õppusest

Cyber Europe on õppus, mille käigus eskaleeruvad mastapsed simuleeritud küberturvalisuse intsidendid kogu ELi hõlmavaks küberkriisiks. Õppused annavad võimaluse analüüsida komplitseeritud küberintsidente ja tegeleda keerukate toimepidevuse ja kriisiohje küsimustega. Täna on ENISA korraldanud juba neli üleeuroopalist küberõppust: 2010., 2012., 2014. ja 2016. aastal.

Õppustel on kesksel kohal rahvusvaheline koostöö kõigi osalevate organisatsioonide vahel. Osalejate seas on enamik Euroopa riike. Õppimise seisukohast on tegemist paindliku üritusega: osalejad saavad tegevust kohandada vastavalt oma vajadustele – osaleda võib üks analüütik või terve organisatsioon, osaleda võib kõigis tegevustes või vaid mõnedes.