„Cyber Europe 2018“: pasirenkite kitai kibernetinei krizei

ES kibernetinio saugumo agentūra ENISA surengė tarptautines kibernetinio saugumo pratybas

Įsivaizduokite įprastą dieną oro uoste. Staiga registracijos automatai ima rodyti pranešimą apie sistemos gedimą. Nustoja veikti išmaniųjų telefonų kelionių programėlės. Registracijos stalų darbuotojai nebegali naudotis kompiuteriais. Keleiviai nebegali nei užregistruoti bagažo, nei atlikti saugumo patikros. Visur nusidriekia ilgiausios eilės. Oro uosto švieslentėse mirga informacija, kad visi skrydžiai atšaukti. Neaišku kodėl nustoja veikti bagažo atsiėmimo sistema ir negali pakilti daugiau kaip pusė lėktuvų.

Pranešama, kad surengusi skaitmeninius ir hibridinius išpuolius svarbiausių oro uosto sistemų kontrolę perėmė radikali grupuotė. Ji jau prisiėmė atsakomybę už incidentą ir savo propagandos kanalais ragina veikti, bandydama į savo pusę patraukti daugiau žmonių.

Tai buvo intensyvus iki šiol brandžiausių ES kibernetinio saugumo pratybų „Cyber Europe 2018“ („CE2018“) scenarijus, kurį įgyvendinant 2018 m. birželio 6–7 d. dalyvavo per 900 Europos kibernetinio saugumo specialistų iš 30 šalių.

Dviejų dienų pratyboms vadovavo ENISA iš būstinės Atėnuose (Graikijoje), o dalyviai arba liko savo įprastoje darbo vietoje, arba susirinko į krizės grupes. ENISA kontroliavo pratybas naudodamasi savo Kibernetinių pratybų platforma (CEP), kurioje buvo sukurtas sumodeliuotai situacijai skirtas „virtualus pasaulis“ (integruota aplinka), įskaitant incidento medžiagą, virtualias naujienų svetaines, socialinės žiniasklaidos kanalus, įmonių interneto svetaines ir tinklaraščius saugumo tema.

Pratybų „CE2018“, kurias surengė ES kibernetinio saugumo agentūra ENISA bendradarbiaudama su kibernetinio saugumo institucijomis ir agentūromis iš visos Europos, paskirtis buvo toliau stiprinti Europos kibernetinės bendruomenės gebėjimus nustatyti didelio masto grėsmes ir į jas reaguoti bei suteikti galimybę geriau suprasti, kokius padarinius toks incidentas gali sukelti kitose šalyse.

Svarbiausia tai, kad pagrindinis „CE2018“ tikslas buvo padėti organizacijoms išbandyti savo vidinius veiklos tęstinumo ir krizių valdymo planus, įskaitant ryšių su žiniasklaida palaikymą krizės atveju, bei sustiprinti viešųjų ir privačiųjų subjektų bendradarbiavimą.

Rengiant scenarijų buvo remiamasi tikrais techniniais ir netechniniais incidentais, kuriems pašalinti buvo reikalinga tinklų ir kenkimo programinės įrangos analizė, ekspertizė ir steganografija. Imituojami incidentai buvo parengti taip, kad peraugtų į krizę visais galimais lygmenimis: organizaciniu, vietos, nacionaliniu ir Europos.

Už skaitmeninę ekonomiką ir skaitmeninės visuomenės reikalus atsakinga Komisijos narė Mariya Gabriel teigė: „Technologijos suteikia daugybę galimybių visiems mūsų ekonomikos sektoriams, tačiau dėl jų taip pat kyla pavojų mūsų įmonėms ir piliečiams. Europos Komisija ir valstybės narės turi bendradarbiauti ir apsirūpinti būtinomis priemonėmis, kad nustatytų kibernetinius išpuolius ir apsaugotų tinklus ir sistemas. Todėl prieš aštuonerius metus pradėtos rengti ENISA pratybos „Cyber Europe“. Nuo to laiko išsiplėtė jų mastas ir išaugo svarba – jos tapo pagrindiniu šios srities renginiu ES, suburiančiu šimtus kibernetinio saugumo specialistų iš visos Europos. Turėtume remtis šia sėkminga veikla planuodami tolesnius veiksmus.

Esu įsitikinusi, kad galime dar labiau plėtoti ES bendradarbiavimo mechanizmus, visų pirma siekdami reaguoti į didelio masto kibernetinius incidentus.“

ENISA vykdomasis direktorius prof. dr. Udo Helmbrechtas paaiškino: „Pastarąjį dešimtmetį aviacijos sektoriaus šuolis, kalbant apie technologijų raidą, buvo didžiulis. Dabar galime naudotis navigacijos programėlių, registracijos internetu ir automatinės bagažo patikros teikiamais privalumais. Pažangiosios technologijos padeda sutaupyti laiko, lėšų, dėl jų žmonėms keliauti lengviau. Tačiau kartu su technologijų raida auga ir kibernetinės grėsmės. Organizuodama tokius renginius kaip „Cyber Europe 2018“, mūsų agentūra kelia kibernetinio saugumo lygį ES. Europos šalių ir organizacijų bendradarbiavimas tarsi jos būtų vienas subjektas yra šiuolaikinis atsakas į valstybių sienų nepaisančias kibernetines grėsmes. ENISA ir jos darbuotojų vardu norėčiau pasveikinti visus „Cyber Europe 2018“ dalyvius.“

Pratybų dalyviams pavyko sušvelninti incidentų padarinius laiku ir veiksmingai. Tai rodo, kad Europos kibernetinio saugumo sektorius per pastaruosius kelerius metus subrendo ir kad jo veikėjai yra daug labiau pasirengę. ENISA ir pratybų dalyviai netrukus pradės analizuoti veiksmus, kurių per jas imtasi, kad nustatytų tobulintinas sritis. ENISA tinkamu laiku paskelbs galutinę ataskaitą.

Faktai trumpai

Dalyvavusios šalys (30): Austrija, Belgija, Bulgarija, Kroatija, Kipras, Čekija, Danija, Estija, Suomija, Prancūzija, Vokietija, Graikija, Vengrija, Airija, Italija, Latvija, Lietuva, Liuksemburgas, Malta, Nyderlandai, Norvegija, Lenkija, Portugalija, Rumunija, Slovakija, Slovėnija, Ispanija, Švedija, Šveicarija, Jungtinė Karalystė.

Dalyvavusios organizacijos: 300

Dalyvių skaičius: daugiau kaip 900 kibernetinio saugumo specialistų

Sumodeliuotų incidentų skaičius: 23 222

Apie pratybas „Cyber Europe“

Pratybos „Cyber Europe“ yra didelės apimties kibernetinio saugumo incidentų, kurie tampa ES masto kibernetinėmis krizėmis, modeliavimas. Jos suteikia galimybių analizuoti sudėtingus kibernetinio saugumo incidentus ir priimti sprendimus, kaip elgtis komplikuotose veiklos tęstinumo ir krizių valdymo situacijose. ENISA jau surengė keturias europines kibernetines pratybas – 2010 m., 2012 m., 2014 m. ir 2016 m.

Per jas itin svarbus tarptautinis visų dalyvaujančių organizacijų bendradarbiavimas – pratybose dalyvauja dauguma Europos šalių. Tai lankstus mokymosi procesas: nuo atskiro analitiko iki visos organizacijos dalyviai gali pritaikyti pratybas prie savo poreikių, jie taip pat gali pasirinkti dalyvavimo arba nedalyvavimo scenarijus.