Starptautiskas kibermācības "Cyber Europe 2018" – gatavošanās iespējamai kiberkrīzei

ES kiberdrošības aģentūras ENISA organizēja starptautiskas kiberdrošības mācības

Iedomājieties šādu situāciju: ir parasta diena lidostā. Pēkšņi automatizētās reģistrācijas automātos iestājas sistēmas atteice. Ceļošanas lietotnes viedtālruņos vairs nedarbojas. Darbinieki aiz reģistrācijas letes vairs nevar izmantot savus datorus. Ceļotāji nevar ne reģistrēt bagāžu, ne iziet drošības pārbaudi. Visur veidojas garas rindas. Lidostas displejos visi lidojumi parādās kā atcelti. Nezināmu iemeslu dēļ bagāžas izsniegšanas pakalpojums vairs nedarbojas, un vairāk nekā pusei lidaparātu ir jāpaliek uz zemes.

Seko paziņojums, ka radikāla grupa, īstenojot digitālus un hibrīdus uzbrukumus, ir pārņēmusi savā kontrolē lidostas kritiskās sistēmas. Tā jau ir uzņēmusies atbildību par incidentu un izmanto savus propagandas kanālus, lai izplatītu aicinājumu rīkoties un pamudinātu lielāku skaitu personu pieņemt radikālu ideoloģiju.

Šāds bija intensīvais scenārijs, ar kuru bija jātiek galā vairāk nekā 900 Eiropas kiberdrošības speciālistiem no 30 valstīm 2018. gada 6. un 7. jūnijā mācībās "CyberEurope 2018" (CE2018), kas ir līdz šim visaptverošākās ES kiberdrošības mācības.

Divu dienu pasākumu rīkoja ENISA no sava galvenā biroja Atēnās (Grieķija), savukārt dalībnieki palika savās parastajās darba vietās vai pulcējās krīzes centros. ENISA pārraudzīja mācības, izmantojot savu platformu mācībām tīklu un informācijas drošības jomā (CEP; angliski Cyber Exercise Platform), kura nodrošināja "virtuālu visumu" simulētai pasaulei, tostarp materiālus attiecībā uz incidentu, virtuālo ziņu tīmekļa vietnes, sociālo mediju kanālus, uzņēmumu tīmekļa vietnes un drošības blogus.

CE2018 mācības rīkoja ES kiberdrošības aģentūra (ENISA) sadarbībā ar visas Eiropas kiberdrošības iestādēm un aģentūrām. Mācību mērķis bija stiprināt Eiropas kiberdrošības kopienas spējas identificēt un novērst liela mēroga apdraudējumus, reaģēt uz tiem, kā arī labāk izprast incidentu pārrobežu ietekmi.

CE2018 mācību vissvarīgākais mērķis bija palīdzēt organizācijām pārbaudīt savus nepārtrauktas darbības un krīžu pārvaldības plānus, tostarp komunikāciju ar plašsaziņas līdzekļiem krīzes apstākļos, vienlaikus nostiprinot sadarbību starp publiskajām un privātajām struktūrām.

Scenārijā bija iekļauti ar reālo dzīvi saistīti tehniska un netehniska rakstura incidenti, kuru sakarā bija vajadzīga tīkla analīze un ļaunprogrammatūras analīze, kriminālistika un steganogrāfija. Scenārijs bija izveidots tā, ka incidenti pāraug visu iespējamo līmeņu krīzē: organizatoriskā, vietējā, valsts un Eiropas mēroga krīzē.

Ekonomikas un digitālās sabiedrības komisāre Marija Gabriela paziņoja: "Tehnoloģijas piedāvā neskaitāmas iespējas visās mūsu ekonomikas nozarēs. Tomēr tās rada arī risku mūsu uzņēmumiem un iedzīvotājiem. Eiropas Komisijai un dalībvalstīm ir jāsadarbojas, lai sev nodrošinātu nepieciešamos instrumentus, kas ļauj identificēt kiberuzbrukumus, un aizsargāt tīklus un sistēmas. Šādā kontekstā pirms astoņiem gadiem tika izveidotas ENISA mācības "Cyber Europe". Tās ir pārtapušas par plašām kiberdrošības mācībām un kļuvušas par svarīgu ES notikumu kiberdrošības jomā, kurš pulcina kiberdrošības speciālistus no visas Eiropas. Mums ir jāizmanto šie panākumi, un es esmu pārliecināta, ka varam vēl vairāk padziļināt ES sadarbības mehānismus, jo īpaši attiecībā uz spēju reaģēt masīvu kiberincidentu gadījumā."

Profesors Dr. Udo Helmbrehts (Udo Helmbrecht), ENISA izpilddirektors, precizēja: "Pēdējo desmit gadu laikā aviācijas nozare ir izdarījusi milzīgu lēcienu tehnoloģiju ērā. Mēs šodien izmantojam daudzas navigācijas lietotnes, tiešsaistes reģistrāciju un automatizētu bagāžas kontroli. Viedas tehnoloģijas ļauj ietaupīt laiku un naudu, un tās atvieglina ceļotāju dzīvi. Tomēr, attīstoties tehnoloģijām, pieaug arī kiberdraudi. Pateicoties tādiem pasākumiem kā "Cyber Europe 2018", mūsu aģentūra stiprina kiberdrošības līmeni Eiropas Savienībā. Eiropas valstīm un organizācijām ir jāsadarbojas kā vienam veselumam — tā ir mūsdienīga atbilde kiberdraudiem, kuri nepazīst robežu. ENISA un tās darbinieku vārdā apsveicu visus, kas piedalījās mācībās "Cyber Europe 2018".

Visbeidzot, dalībnieki spēja laikus un efektīvi mazināt incidentu ietekmi. Tas liecina, ka pēdējos gados Eiropas kiberdrošības nozare ir attīstījusies un ka tās dalībnieki ir daudz labāk sagatavoti. ENISA un dalībnieki drīzumā veiks turpmākās darbības saistībā ar mācībām un analizēs veiktos pasākumus, lai novērtētu, kurās jomās ir vajadzīgi uzlabojumi. Vēlāk ENISA publicēs galīgo ziņojumu.

Fakti īsumā

Iesaistītās valstis: 30 — Austrija, Beļģija, Bulgārija, Horvātija, Kipra, Čehija, Dānija, Igaunija, Somija, Francija, Vācija, Grieķija, Ungārija, Īrija, Itālija, Latvija, Lietuva, Luksemburga, Malta, Nīderlande, Norvēģija, Polija, Portugāle, Rumānija, Slovākija, Slovēnija, Spānija, Zviedrija, Šveice, Apvienotā Karaliste

Organizācijas, kuras piedalījās: 300

Dalībnieku skaits: vairāk nekā 900 kiberdrošības speciālisti

Simulēto inicidentu skaits: 23 222

Par "Cyber Europe" mācībām

"Cyber Europe" mācības ir tādu vērienīgu kiberincidentu simulācijas, kas izvēršas par ES mēroga kiberkrīzēm. Šīs mācības dod iespēju analizēt sarežģītus kibernētiskus incidentus un izkļūt no komplicētām darbības nepārtrauktības un krīžu pārvaldības situācijām. ENISA ir sarīkojusi četras Eiropas mēroga kiberdrošības mācības — 2010., 2012., 2014. un 2016. gadā.

Starptautiskā sadarbība starp visām iesaistītajām organizācijām ir raksturīga šo mācību iezīme, lielākā daļa Eiropas valstu tajās piedalījās. Tas elastīgs mācību process: gan analītiķiem, gan veselai organizācijai, ar iespēju piedalīties vai nepiedalīties pēc izvēles. Dalībnieki var pielāgot mācības savām vajadzībām.