„Cyber Europe 2018” – pripremite se za sljedeću kiberkrizu

Agencija EU-a za kibersigurnost ENISA organizirala je međunarodnu vježbu u području kibersigurnosti

Zamislite ovu situaciju: uobičajen dan u zračnoj luci. Iznenada, uređaji za automatsku prijavu za let prikazuju poruku da je došlo do greške u sustavu. Putne aplikacije na pametnim telefonima prestaju raditi. Računala zaposlenika koji rade na šalterima za prijavu više ne rade. Putnici ne mogu niti prijaviti svoju prtljagu niti proći kroz sigurnosnu kontrolu. Svuda nastaju golemi redovi. Na ekranima zračne luke za prikaz informacija o letovima svi se letovi prikazuju kao otkazani. Iz nepoznatih razloga, preuzimanje prtljage više ne radi i više od pola letova mora se odgoditi.

Prema dostupnim informacijama skupina ekstremista preuzela je kontrolu nad ključnim sustavima zračne luke s pomoću digitalnih i hibridnih napada. Već su preuzeli odgovornost za taj incident i koriste svoje propagandne kanale da bi pozvali na djelovanje i privukli više ljudi da prihvate njihovu ekstremnu ideologiju.

To je intenzivan scenarij s kojim je 900 europskih stručnjaka za kibersigurnost iz 30 zemalja bilo suočeno 6. i 7. lipnja 2018. tijekom vježbe „Cyber Europe 2018” (CE2018), do sada najrazvijenije vježbe u području kibersigurnosti u EU-u.

ENISA je tu dvodnevnu vježbu organizirala u svojem sjedištu u Ateni u Grčkoj, a sudionici su ostali na svojim uobičajenim radnim mjestima ili su se okupili u skupinama za djelovanje u slučaju krize. ENISA je vježbu kontrolirala putem svoje platforme za kibervježbe Cyber Exercise Platform - CEP, koja je poslužila kao „virtualni univerzum” (integrirano okruženje) za simulirani svijet, uključujući materijal o incidentu, virtualna *web-mjesta* s vijestima, kanale socijalnih medija, *web-mjesta* poduzeća i sigurnosne blogove.

Cilj vježbe CE2018 koju je organizirala ENISA, Agencija EU-a za kibersigurnost u suradnji s tijelima i agencijama za kibersigurnost iz cijele Europe, bio je omogućiti europskoj kibersigurnosnoj zajednici daljnje jačanje njenih sposobnosti za prepoznavanje i rješavanje prijetnji velikog razmjera te omogućiti bolje razumijevanje širenja prekograničnog incidenta.

Najvažnije je da je vježba CE2018 bila usredotočena na to da organizacijama pomogne provjeriti njihove interne planove kontinuiteta poslovanja i planove za krizno upravljanje, uključujući medijsku komunikaciju u krizi, istovremeno jačajući suradnju između javnih i privatnih subjekata.

Scenarij je sadržavao tehničke i netehničke probleme inspirirane iskustvima iz stvarnog života za čije rješavanje su bili potrebni mrežna analiza i analiza zlonamjernog softvera, forenzika i steganografija. Incidenti u scenariju osmišljeni su tako da prerastu u krizu na svim mogućim razinama: organizacijskoj, lokalnoj, nacionalnoj i europskoj.

Povjerenica za digitalno gospodarstvo i društvo Mariya Gabriel izjavila je: „Tehnologija nudi bezbroj mogućnosti u svim sektorima naše ekonomije. No postoje i opasnosti za naše poslovne subjekte i za naše građane. Europska komisija i države članice moraju surađivati i opremiti se neophodnim alatima za otkrivanje kibernapada i zaštitu mreža i sustava. Tako je prije osam godina nastala ENISA-ina vježba „Cyber Europe”. Ona se razvila u jednu od glavnih vježbi u području kibersigurnosti i postala glavno događanje te vrste u EU-u koje objedinjuje stotine stručnjaka za kibersigurnost iz cijele Europe. Trebali bismo nastaviti

graditi na tom uspjehu i sigurna sam da možemo razviti dodatne mehanizme za suradnju u EU-u, a pogotovo kao odgovor na kiberincidente velikog opsega."

Prof. dr. Udo Helmbrecht, izvršni direktor ENISA-e, objasnio je: „Tijekom prethodnog desetljeća, sektor zrakoplovstva ostvario je enorman napredak u smjeru razvoja tehnologije. Sada možemo uživati u pogodnostima navigacijskih aplikacija, internetske prijave za let i automatskog pregleda prtljage. Pametna tehnologija štedi nam vrijeme i novac te olakšava život putnicima. No, paralelno s tehnologijom razvijaju se i kiberprijetnje. Organizacijom događaja kao što je Cyber Europe 2018. naša agencija jača razinu kibersigurnosti u EU-u. Suradnja europskih zemalja i organizacija koje djeluju kao jedan subjekt moderan je odgovor na kiberprijetnje koje ne poznaju granice. U ime ENISA-e i njezinog osoblja, želim čestitati svima koji su sudjelovali u vježbi Cyber Europe 2018."

Na kraju, sudionici su bili u stanju pravodobno i učinkovito ublažiti incidente. To pokazuje da se europski sektor kibersigurnosti tijekom zadnjih godina razvio i da su sudionici bitno bolje pripremljeni. ENISA i sudionici uskoro će započeti s popratnim radnjama nakon vježbe i analizirati poduzete mjere kako bi prepoznali područja u kojima je moguće ostvariti poboljšanja. ENISA će u dogledno vrijeme objaviti svoje konačno izvješće.

Kratki prikaz činjenica

Zemlje sudionice: 30, Austrija, Belgija, Bugarska, Hrvatska, Cipar, Češka, Danska, Estonija, Finska, Francuska, Njemačka, Grčka, Mađarska, Irska, Italija, Latvija, Litva, Luksemburg, Malta, Nizozemska, Norveška, Poljska, Portugal, Rumunjska Slovačka, Slovenija, Španjolska, Švedska, Švicarska, Ujedinjena Kraljevina

Organizacije sudionice: približno 300

Broj sudionika: više od 900 stručnjaka za kibersigurnost

Broj simuliranih incidenata: 23 222

O vježbama Cyber Europe

Vježbe „Cyber Europe" simulacije su kiberincidenata velikog opsega koji prerastu u kiberkrizu na razini EU-a. Te vježbe nude mogućnosti za analizu naprednih kiberincidenata i za rješavanje složenih situacija u pogledu poslovnog kontinuiteta i upravljanja krizama. ENISA je već organizirala četiri sveeuropske kibervježbe 2010., 2012., 2014. i 2016.

Međunarodna suradnja među svim organizacijama koje sudjeluju u vježbi sastavni je dio igre i u njoj sudjeluje većina europskih zemalja. Ta vježba pruža iskustvo fleksibilnog učenja: sudionici mogu prilagoditi vježbu svojim potrebama odlučujući hoće li u njoj sudjelovati samo jedan analitičar ili cijela organizacija, te u kojim će scenarijima sudjelovati, a u kojima ne.