Vaja Cyber Europe za leto 2018 – priprave na naslednjo kibernetsko krizo

Agencija za kibernetsko varnost ENISA organizirala mednarodno vajo v kibernetski varnosti

Zamislite si naslednji primer. Običajen dan na letališču. Avtomat za prijavo na let kar naenkrat javi sistemsko napako. Potovalne aplikacije na pametnih telefonih ne delujejo. Uslužbenci za prijavnimi okenci ne morejo več uporabljati svojih računalnikov. Potniki ne morejo ne oddati prtljage ne opraviti varnostnega pregleda. Vsepovsod velikanske vrste. Na letaliških prikazovalnikih so vsi leti preklicani. Iz neznanih razlogov je dvig prtljage nehal delovati in več kot polovica letal je prizemljenih.

Radikalna skupina naj bi z digitalnimi in hibridnimi napadi prevzela nadzor nad letališkimi kritičnimi sistemi. Prevzela je že odgovornost za incident ter po svojih propagandnih kanalih širi poziv k akciji in novači še več ljudi v svojo radikalno ideologijo.

Tak je bil napeti scenarij, pred katerega je 6. in 7. junija 2018 bilo postavljeno več kot 900 evropskih strokovnjakov za kibernetsko varnost iz 30 držav med vajo „Cyber Europe 2018“ (CE2018) – najbolj razvito vajo EU za kibernetsko varnost doslej.

Dvodnevno vajo je organizirala agencija ENISA na svojem sedežu v Atenah v Grčiji, medtem ko so udeleženci bodisi ostali na svojem običajnem delovnem mestu ali so se zbrali v kriznih celicah. ENISA je nadzirala vajo prek svoje platforme za kibernetsko vajo (CEP), ki je ustvarila „navidezni svet“ (integrirano okolje) za simulirano resničnost, vključno z materialom za incident, virtualnimi spletišči z novicami, družbenimi mediji, spletišči podjetij in spletnimi dnevniki o varnosti.

Agencija EU za kibernetsko varnost je v sodelovanju z organi in agencijami za kibernetsko varnost iz vse Evrope organizirala vajo CE2018, s katero naj bi evropski skupnosti kibernetske varnosti omogočila nadaljnjo krepitev zmogljivosti za odkrivanje in odpravljanje obsežnih groženj ter hkrati boljše razumevanje čezmejnega širjenja incidentov.

Še pomembnejše, vaja CE2018 je bila usmerjena v pomoč organizacijam pri preizkušanju notranjih načrtov neprekinjenega poslovanja in kriznega upravljanja, vključno z medijskim obveščanjem v kriznih razmerah, hkrati pa je tudi krepila sodelovanje med javnimi in zasebnimi subjekti.

Scenarij je vseboval tehnične in netehnične incidente, ki so jih navdihnili dogodki iz resničnega življenja ter ki so zahtevali analizo omrežja in zlonamerne programske opreme, forenziko in steganografijo. Incidenti v scenariju so bili zastavljeni tako, da bi lahko prerasli v krizo na vseh mogočih ravneh: organizacijski, lokalni, nacionalni in evropski.

Komisarka za digitalno gospodarstvo in družbo Marija Gabriel je dejala: „Tehnologija ponuja nešteto priložnosti v vseh sektorjih evropskega gospodarstva. Vendar obstajajo tudi tveganja za naša podjetja in državljane. Evropska komisija in države članice morajo sodelovati in se opremiti s potrebnim orodjem za odkrivanje kibernetskih napadov ter zaščito omrežij in sistemov. Zato je pred osmimi leti nastala vaja „Cyber Europe“ v ENISA. Razvila se je v pomembno vajo v kibernetski varnosti in postala osrednji dogodek EU, ki združuje stotine specialistov iz kibernetske varnosti iz vse Evrope. Graditi moramo na tem uspehu in prepričana sem, da lahko razvijemo nadaljnje mehanizme sodelovanja EU, zlasti za odzivanje na kibernetske incidente velikega obsega.“

Izvršni direktor ENISA prof. dr. Udo Helmbrecht je razložil: „V zadnjih desetih letih je letalski sektor naredil velikanski preskok v dobo tehnološkega razvoja. Sedaj lahko uživamo prednosti navigacijskih aplikacij, spletne prijave na let in samodejnega pregleda prtljage. Pametne tehnologije potnikom prihranijo čas, denar in olajšujejo življenje. Vendar tako, kot se razvija tehnologija, se razvijajo tudi kibernetske grožnje. Z dogodki, kot je vaja Cyber Europe 2018, naša agencija krepi raven kibernetske varnosti v EU. Na kibernetske grožnje, ki ne poznajo meja, se lahko sodobno odzovemo tako, da evropske države in organizacije delujejo družno kot en subjekt. V imenu agencije ENISA in njenega osebja čestitam vsem, ki so sodelovali v Cyber Europe 2018.“

Na koncu je udeležencem uspelo pravočasno in učinkovito ublažiti incidente. To kaže, da je evropski sektor kibernetske varnosti v zadnjih nekaj letih dozorel in so akterji veliko bolj pripravljeni. Po vaji bodo ENISA in udeleženci še preučili ravnanje med njo, da bi ugotovili področja, ki bi jih lahko izboljšali. ENISA bo nato objavila končno poročilo.

Povzetek dejstev

Sodelujoče države: 30, Avstrija, Belgija, Bolgarija, Hrvaška, Ciper, Češka, Danska, Estonija, Finska, Francija, Nemčija, Grčija, Madžarska, Irska, Italija, Latvija, Litva, Luksemburg, Malta, Nizozemska, Norveška, Poljska, Portugalska, Romunija, Slovaška, Slovenija, Španija, Švedska, Švica, Združeno kraljestvo

Sodelujoče organizacije 300

Število udeležencev: več kot 900 strokovnjakov za kibernetsko varnost

Število simuliranih incidentov: 23 222

O vaji Cyber Europe

Vaje Cyber Europe so simulacije obsežnih kibernetskih incidentov, ki lahko zajamejo vso EU. So priložnost za analizo naprednih kibernetskih incidentov ter spoprijem z zapletenimi razmerami za neprekinjeno poslovanje in krizno upravljanje. Agencija ENISA je že organizirala štiri vseevropske vaje za kibernetsko varnost leta 2010, 2012, 2014 in 2016.

V jedru igre je mednarodno sodelovanje med vsemi sodelujočimi organizacijami in večina evropskih držav sodeluje pri njej. Je prožna učna izkušnja: lahko vključuje od enega samega analitika do cele organizacije, vsebuje možnost pristopa k posameznim scenarijem ali odstopa od njih, udeleženci pa lahko prilagodijo vajo svojim potrebam.