Agencija Evropske unije
za kibernetsko varnost
Agamemnonos 14,
Chalandri 15231| Attiki| Grčija
Tel.: +30 28 14 40 9711
E-pošta: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: testiranje odpornosti evropskega sektorja za zdravstveno varstvo

Agencija Evropske unije za kibernetsko varnost (ENISA) je organizirala vajo na področju kibernetske varnosti, da bi preskusila odziv na napade na zdravstveno infrastrukturo in storitve v EU.

Da bi ohranili zaupanje državljanov v zdravstvene storitve in infrastrukturo, ki so jim na voljo, je treba zagotoviti neprekinjeno delovanje zdravstvenih storitev. Če bi bile zdravstvene storitve in infrastruktura v Evropi tarča obsežnega kibernetskega napada, kako bi se odzvali in usklajevali ukrepe na nacionalni in evropski ravni, da bi ublažili nastale incidente in preprečili razširitev krize?

To je bilo vprašanje, na katerega so želeli s pomočjo fiktivnega scenarija odgovoriti na vaji Cyber Europe 2022. Prvi dan vaje sta bila predstavljena kampanja dezinformiranja z manipuliranimi laboratorijskimi izvidi in kibernetski napad na evropske bolnišnične mreže. Drugi dan vaje se je po scenariju kriza razširila v kibernetsko krizo po vsej EU z neposredno nevarnostjo razkritja osebnih zdravstvenih podatkov, temu pa se je pridružila še kampanja, katere cilj je bil diskreditirati medicinski vsadljivi pripomoček s trditvijo o ranljivosti.

Izvršni direktor Agencije EU za kibernetsko varnost **Juhan Lepassaar** je dejal: *„Kompleksnost naših izzivov je sedaj sorazmerna s kompleksnostjo našega povezanega sveta. Zato trdno verjamem, da moramo zbrati vse obveščevalne podatke, ki jih imamo v EU, da bi lahko delili svoje strokovno znanje in izkušnje. Krepitev naše kibernetske odpornosti je edina pot naprej, če želimo zaščititi naše zdravstvene storitve in infrastrukturo ter navsezadnje zdravje vseh državljanov EU.“*

V vseevropski vaji, ki jo je organizirala agencija ENISA, je sodelovalo 29 držav iz Evropske unije in Evropskega združenja za prosto trgovino (EFTA), pridružile pa so se tudi agencije in

institucije EU, agencija ENISA, CERT-EU Evropske komisije, Europol in Evropska agencija za zdravila (EMA). Več kot 800 strokovnjakov za kibernetsko varnost je na tej zadnji dvodnevni vaji v okviru programa Cyber Europe združilo svoja znanja in izkušnje pri preverjanju razpoložljivosti in celovitosti obstoječih sistemov.

Ali lahko okrepimo kibernetsko odpornost sistema zdravstvenega varstva v EU?

Udeleženci, ki so sodelovali pri tej zahtevni vaji, so bili zadovoljni z načinom obravnave incidentov in odzivom na fiktivne napade.

Sedaj bo treba izvesti analizo postopkov in rezultatov različnih vidikov vaj, da bomo razumeli morebitne pomanjkljivosti ali slabosti sistema, ki bi lahko zahtevale blažilne ukrepe. Za obvladovanje tovrstnih napadov so potrebne različne ravni kompetenc in postopkov, ki vključujejo učinkovito in usklajeno izmenjavo informacij in znanja o posameznih incidentih ter metodah spremljanja kriznih razmer, ki se lahko v primeru vsesplošnega napada razširijo. Preučiti je treba tudi vlogo mreže skupin za računalniško varnost in odzivanje na incidente (CSIRT) na ravni EU in standardnih operativnih procesov (SOP) organizacijske mreže za povezovanje v kibernetski krizi (CyCLONe).

Poglobljena analiza bo objavljena v poročilu o nadaljnjem ukrepanju. Ugotovitve analize bodo lahko služile kot podlaga za prihodnje smernice in nadaljnje izboljšave za krepitev odpornosti zdravstvenega sektorja na kibernetske napade v EU.

O vajah v okviru programa Cyber Europe

Vaje Cyber Europe so simulacije obsežnih kibernetskih incidentov, ki lahko zajamejo vso EU. So priložnost za analizo naprednih kibernetskih incidentov ter spoprijem s kompleksnimi problemi na področju ohranjanja neprekinjenega poslovanja in kriznega upravljanja.

Agencija ENISA je v letih 2010, 2012, 2014, 2016 in 2018 organizirala pet vseevropskih vaj za kibernetsko varnost. Tovrstne vaje se običajno organizirajo vsaki dve leti, vendar pa je letu 2020 vaja bila odpovedana zaradi pandemije covida-19.

Samo jedro teh dogodkov je mednarodno sodelovanje med vsemi sodelujočimi organizacijami, pri čemer je treba poudariti, da v vajah sodeluje večina evropskih držav. Gre za prožno učno izkušnjo, bodisi za enega samega analitika bodisi za celotno organizacijo, s „vključevanjem“ in „izključevanjem“ scenarijev, pri čemer lahko udeleženci nalogo prilagodijo svojim potrebam.

Dodatne informacije

Cyber Europe 2022

Kibernetske vaje – tema agencije ENISA

Cyber Europe 2018 – Poročilo o nadaljnjem ukrepanju

Kontakt:

Novinarska vprašanja in zahteve za intervju lahko naslovite na press(at)enisa.europa.eu