U paneuropskoj vježbi „Cyber Europe 2022“ otpornost europskog zdravstvenog sustava testirali i hrvatski stručnjaci

Hrvoje Belani

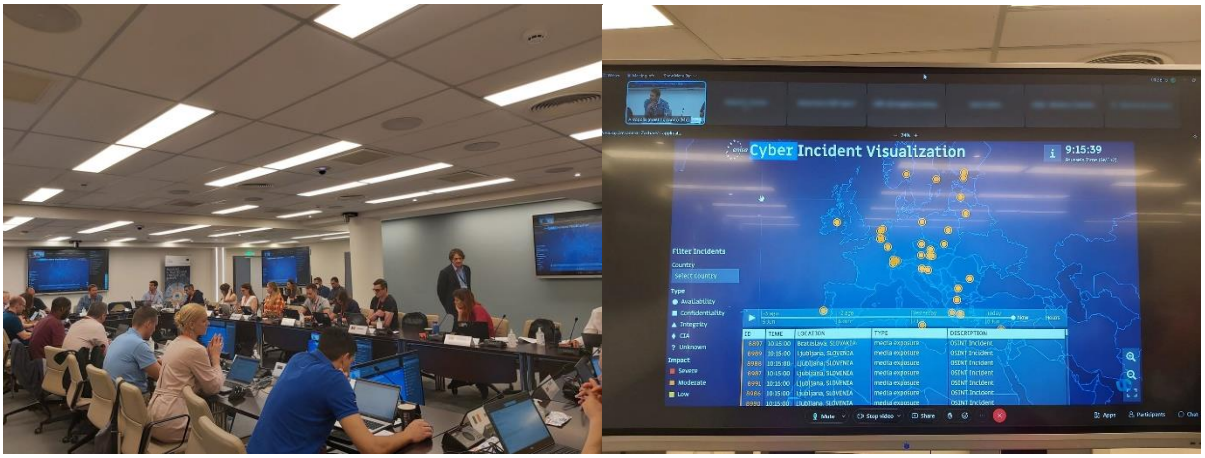
Ministarstvo zdravstva, Uprava za e-zdravstvo, Zagreb, Hrvatska

e-pošta: hrvoje.belani@miz.hr

Kako bi se osiguralo povjerenje građana u medicinske usluge i infrastrukturu koje su im dostupne, zdravstvene usluge moraju funkcionirati u svakom trenutku. Ako bi došlo do ozbiljnog kibernetičkog napada na zdravstvene usluge i infrastrukturu u Europi, kako bismo na to reagirali te koordinirali odgovor na nacionalnoj razini i na razini EU-a da se ograniče incidenti i spriječi eskalacija? Upravo se na to pitanje pokušalo naći odgovor u sklopu vježbe „Cyber Europe 2022“. Vježbe „Cyber Europe“ simulacije su kibernetičkih incidenata velikih razmjera koji eskaliraju u kibernetičke krize širom EU-a.

Agencija Europske unije za kibernetičku sigurnost (ENISA) organizirala je međunarodnu vježbu iz kibernetičke sigurnosti kako bi testirala odgovor na napade na infrastrukturu i usluge europskog zdravstvenog sustava (1). Paneuropska vježba „Cyber Europe 2022“ održana je 8. i 9. lipnja 2022. godine uz sudjelovanje 800 igrača, među kojima i predstavnika zdravstvenih ustanova svih država članica Europske unije (EU) i Europskog udruženja slobodne trgovine (EFTA).

Hrvatsku su predstavljali stručnjaci iz Kliničkog bolničkog centra Zagreb, Opće bolnice „Dr. Tomislav Bardek“ Koprivnica te Agencije za lijekove i medicinske proizvode (HALMED), koji su udaljenim pristupom putem platforme CEP (*Cyber Exercise Platform*) rješavali tehničke zadatke i analizirali simulirane incidente, a podršku su im kao lokalni treneri iz sjedišta ENISA-e pružali predstavnici Zavoda za sigurnost informacijskih sustava (ZSIS) i CARNET-ovog Nacionalnog CERT-a (*Computer Emergency Response Team*). Koordinaciju priprema za samu vježbu provela je Uprava za e-zdravstvo Ministarstva zdravstva.



Slika 1. Kadar s vježbe „Cyber Europe 2022“ iz ENISA-inog sjedišta u Grčkoj (lijevo); prikaz vizualizacije incidenata (desno) simuliranih tijekom prvog dana vježbe (izvor: ENISA Facebook)

Vježbe „Cyber Europe“, koje se održavaju u dvogodišnjem ritmu od 2010. godine, omogućavaju analizu naprednih incidenata u području kibernetičke sigurnosti te rješavanje složenih situacija u pogledu kontinuiteta poslovanja i upravljanja krizom. Ove godine, fiktivni scenarij obuhvatio je napad na infrastrukturu i usluge zdravstvenog sustava uz prijetnju objave osobnih medicinskih podataka u više zemalja Europske unije te kampanju dezinformiranja i diskreditiranja.

Prvi su se dan odvijali kampanja dezinformiranja manipuliranim rezultatima iz laboratorija te kibernetički napad usmjeren na mreže europskih bolnica. Drugog je dana prema scenariju došlo do eskalacije kibernetičke krize u cijelom EU-u uz izravnu prijetnju objave osobnih medicinskih podataka i još jedne kampanje čiji je cilj bio diskreditirati medicinski proizvod za implantaciju s tvrdnjom o ranjivosti.

Paneuropska vježba u organizaciji ENISA-e obuhvatila je ukupno 29 zemalja Europske unije i Europskog udruženja slobodne trgovine (EFTA) te agencije i institucije EU-a, ENISA-u, Europsku komisiju, CERT-EU, Europol i Europsku agenciju za lijekove (EMA). Sudionici ove složene vježbe bili su zadovoljni načinom rješavanja incidenata i odgovorima na fiktivne napade.

Slika 2. Logotip vježbe „Cyber Europe 2022“ (lijevo); jedan od grafičkih prikaza (desno) za promidžbu ovogodišnje vježbe (izvor: ENISA Facebook)

Nakon vježbe slijedi analiza postupka i ishoda različitih aspekata vježbe za realno utvrđivanje mogućih nedostataka ili slabosti za koje bi mogle biti potrebne adekvatne mjere. Rješavanje takvih napada zahtijeva različite razine kompetencija i postupaka koji uključuju učinkovitu i koordiniranu razmjenu informacija, razmjenu znanja o određenim incidentima i način praćenja situacije koja bi lako mogla eskalirati u slučaju općeg napada. Također je potrebno razmotriti ulogu na razini EU-a u mreži tima za odgovor na računalne sigurnosne incidente i standardne operativne postupke skupine CyCLONe (*Cyber Crises Liaison Organisation Network*) (2).

Detaljnija analiza bit će objavljena u izvješću o naknadnim aktivnostima, kakvo je objavljeno i nakon prethodne vježbe, identificiravši izazove i glavne zaključke, te davši korisne preporuke za sudionike (3). Rezultati će predstavljati osnovu za buduće smjernice i daljnja poboljšanja za jačanje otpornosti zdravstvenog sektora na kibernetičke napade u EU-u. Međunarodna suradnja među svim sudionicima sastavni je dio vježbe u kojoj sudjeluje većina europskih zemalja. Vježba predstavlja iskustvo fleksibilnog učenja: od jednog analitičara do cijele organizacije, s mogućnostima sudjelovanja ili nesudjelovanja u pojedinim aktivnostima, pri čemu sudionici vježbu mogu prilagoditi svojim potrebama.

ENISA je već organizirala pet paneuropskih vježbi u području kibernetičke sigurnosti 2010., 2012., 2014., 2016. i 2018. Obično se održavaju svake dvije godine, no 2020. su bile otkazane zbog epidemije bolesti COVID-19. Izvršni direktor Agencije EU-a za kibernetičku sigurnost, Juhan Lepassaar, izjavio je po završetku ovogodišnje vježbe: „Složenost naših izazova razmjerna je složenosti našeg povezanog svijeta. Stoga čvrsto vjerujem da moramo skupiti sve obavještajne podatke koje imamo u EU-u za razmjenu naše stručnosti i znanja. Jačanje naše kibernetičke otpornosti jedini je put naprijed želimo li zaštititi svoje zdravstvene usluge i infrastrukturu te u konačnici zdravlje svih građana EU-a."

ENISA je Agencija Europske unije za kibernetičku sigurnost osnovana 2004. godine s ciljem postizanja visoke zajedničke razine kibernetičke sigurnosti u cijeloj Europi (ENISA, 2022.). Razmjenom znanja, izgradnjom kapaciteta i informiranjem ENISA zajedno sa svojim ključnim dionicima radi na jačanju povjerenja u povezano gospodarstvo kako bi se povećala otpornost infrastrukture Unije te kako bi se u konačnici ostvarila digitalna sigurnost europskog društva i građana (4).

Podsjetimo ovom prilikom da je na sjednici Izvršnog odbora HDMI-a održanoj 25. svibnja 2021. godine donesena formalna odluka o osnivanju Radne skupine za informacijsku i kibernetičku sigurnost (IKS) (5). U prošlom broju biltena HDMI-a objavljen je prvi zajednički rad članova Radne skupine kojem je cilj bio SWOT analizom procijeniti stanje informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske, uključujući i domove zdravlja i bolničke ustanove, na temelju javno dostupnih informacija i saznanja autora (6).

Prvi sastanak Radne skupine IKS održan je 9. lipnja 2022. godine, a kao tema od posebnog interesa prepoznata je osmišljavanje i organizacija radionica (treninga) za zdravstvene djelatnike iz područja informacijske i kibernetičke sigurnosti tijekom 2023. godine. Stoga se ovim putem pozivaju zainteresirani članovi HDMI-a javiti se voditelju Hrvoju Belaniju na adresu e-pošte hrvoje.belani@miz.hr.

Literatura

1. ENISA. Dostupno na: https://www.enisa.europa.eu/about-enisa/about/hr, pristup 10. lipnja 2022.
2. EU CyCLONe. Dostupno na: https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management, pristup 10. lipnja 2022.
3. ENISA. Cyber Europe 2018 – After Action Report. December 20, 2018. Dostupno na: https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report, pristup 10. lipnja 2022.
4. Uredba (EU) br. 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agenciji Europske unije za kibernetičku sigurnost) te o kibernetičkoj sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibernetičkoj sigurnosti). Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32019R0881&from=EN, pristup 10. lipnja 2022.
5. Belani H. Radna skupina za informacijsku i kibernetičku sigurnost (IKS). Bilten Hrvatskog društva za medicinsku informatiku (Online) [Internet]. 2021 [pristupljeno 10.06.2022.];27(2):38-41. Dostupno na: https://hrcak.srce.hr/260279
6. Belani H, Kern J, Protrka N, Fišter K, Hercigonja-Szekeres M. SWOT analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske. Bilten Hrvatskog društva za medicinsku informatiku (Online) [Internet]. 2022 [pristupljeno 10.06.2022.];28(1):1-13. Dostupno na: https://hrcak.srce.hr/273451