Radna skupina za informacijsku i kibernetičku sigurnost (IKS)

Hrvoje Belani
Ministarstvo zdravstva, Zagreb, Hrvatska
e-pošta: hrvoje.belani@miz.hr

Informacijska sigurnost je *stanje povjerljivosti, cjelovitosti i raspoloživosti podatka* (ponekad se koristi i pojam dostupnost, iako se ne radi o sinonimu) koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i te primjene standarda poput ISO 27001. Dakle, informacijska sigurnost treba postojati bez obzira koristimo li ili ne koristimo informacijsko-komunikacijske tehnologije u poslovanju. Ako ih koristimo, tada su nam potrebne konkretne mjere kibernetičke sigurnosti. Prema jednoj od definicija, kibernetička sigurnost je sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka kao i mrežnih i informacijskih sustava u kibernetičkom prostoru. Kibernetički prostor je pak virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na internet.

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[1] i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[2] doneseni su 2018. godine kao rezultat obveze svake države članice EU za prijenosom zahtjeva propisanih tzv. NIS direktivom[3] u nacionalno zakonodavstvo. Ovim se propisima želi osigurati visoka razina kibernetičke sigurnosti u pružanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, a među osam obuhvaćenih sektora je i onaj zdravstveni sektor. Navedenom Uredbom utvrđuju se mjere za postizanje visoke razine kibernetičke sigurnosti tzv. operatora ključnih usluga, način njihove provedbe, kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti i druga bitna pitanja za obavješćivanje o incidentima. Sam Zakon definira kriterije za identifikaciju operatora ključnih usluga u zdravstvenom sektoru, a to može biti bilo koji javni ili privatni subjekt koji zadovoljava barem jedan od kriterija za pružanje neke od ukupno devet ključnih usluga u zdravstvenom sektoru:

- Primarna zdravstvena zaštita,
- Sekundarna zdravstvena zaštita,
- Tercijarna zdravstvena zaštita,
- Transfuzijska medicina i transplantacija organa,
- Zdravstveno osiguranje i prekogranična zdravstvena zaštita,

[1] https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_64_1305.html
[2] https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_68_1399.html
[3] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016L1148

- Sigurnost hrane,
- Zaštita od opasnih kemikalija,
- Distribucija i sigurnost lijekova i medicinskih proizvoda,
- Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara.

U provedbi navedenih propisa identificiran je ukupno 31 operator ključnih usluga u zdravstvenom sektoru, među kojima su klinički bolnički centri, kliničke bolnice i klinike, najveći domovi zdravlja i županijski zavodi za hitnu medicinu, neke opće bolnice, ali i zdravstveni zavodi i agencije. No, ustanova u zdravstvu RH je daleko više, a sve one trebaju imati uspostavljene mjere informacijske i kibernetičke sigurnosti kako bi prikladno zaštitile svoje podatke i resurse.

S druge strane, ulaganje u informacijsku i kibernetičku sigurnost redovito nije među prioritetima donositelja odluka, a nerijetko se taj posao i dužnosti svrstavaju isključivo u djelokrug informatike, što znatno ograničava mogućnosti za učinkovitu i trajnu uspostavu mjera na razini cijele ustanove. Stoga je potrebno na temelju postojećih propisa, i najboljih stručnih praksi i znanstvenih dostignuća, doprinijeti razvoju ovih područja u zdravstvu RH. Jedan od načina je okupljanje stručnjaka, istraživača i praktičara koji će izradom smjernica, preporuka i prijedloga politika pomoći stručnom osoblju u zdravstvenim ustanovama, pospješiti edukaciju zdravstvenog osoblja, i doprinijeti osvješćivanju donositelja odluka o važnosti informacijske i kibernetičke sigurnosti.

Stoga je 24. svibnja 2021. godine pri Hrvatskom društvu za medicinsku informatiku (HDMI) osnovana Radna skupina za informacijsku i kibernetičku sigurnost u zdravstvu (skraćeno: IKS). S obzirom na žarište djelovanja, radna skupina okuplja motivirane stručnjake s komplementarnim znanjima iz različitih područja djelovanja koji imaju duboko razumijevanje i iskustvo u područjima informacijske i kibernetičke sigurnosti u zdravstvu čime se bave u stručne ili znanstvene svrhe, kao i razvojem ili upravljanjem informacijskom i kibernetičkom sigurnošću u okviru Zdravstvene informacijske infrastrukture RH. Inicijatori Radne skupine IKS su: Krunoslav Antoliš, Hrvoje Belani (voditelj), Kristina Fišter, Mira Hercigonja-Szekeres, Josipa Kern, Nikola Protrka i Krešimir Šolić.

Misija Radne skupine IKS je podizanje spremnosti ustanova i drugih dionika u zdravstvu RH u područjima informacijske i kibernetičke sigurnosti, uz osnaživanje kompetencija zdravstvenog osoblja, prenošenje znanja i iskustava te osvješćivanje donositelja odluka o važnosti informacijske i kibernetičke sigurnosti.

Ciljevi Radne skupine IKS su:

1. izrada smjernica, preporuka i prijedloga politika u područjima informacijske i kibernetičke sigurnosti za primjenu u zdravstvenim ustanovama i kod drugih dionika u zdravstvu;
2. pospješivanje edukacije stručnog osoblja u zdravstvenim ustanovama o primjeni mjera informacijske i kibernetičke sigurnosti i poslovnoj higijeni vezanoj uz rad sa zdravstvenim podacima i informacijama te informacijskim sustavima i aplikacijama e-zdravstva;
3. osvješćivanje donositelja odluka u zdravstvu o važnosti informacijske i kibernetičke sigurnosti i potrebnim financijskim ulaganjima za podizanje razine sigurnosti mrežnih i informacijskih sustava;

4. pospješivanje međusektorske suradnje u područjima informacijske i kibernetičke sigurnosti, kao i suradnje sa nadležnim i stručnim tijelima (UVNS, SOA, ZSIS, NCERT), s ciljem razmjene znanja i iskustava te poticanje kontinuirane suradnje sa dionicima u zdravstvenom sustavu.

Postavljene ciljeve Radna skupina IKS će nastojati ispuniti sljedećom strategijom djelovanja, između ostalog:

- okupljanjem stručnjaka, predstavnika različitih dionika zdravstvenog sustava koji imaju komplementarna znanja o informacijskoj i kibernetičkoj sigurnosti, od pravnih i organizacijskih do procesnih aspekata do tehničkih aspekata, kao i razmjene praktičnih znanja i iskustava u tim područjima;
- diseminacijom informacija među članovima radne skupine o aktualnim projektima u RH i EU vezanim za područja informacijske i kibernetičke sigurnosti te digitalnog zdravstva i e-zdravstva;
- poticanjem članova radne skupine na prikupljanje i međusobnu razmjenu iskustava u uspostavi i održavanju mjera informacijske i kibernetičke sigurnosti;
- jačanjem kapaciteta radne skupine radom na metodološkim izazovima informacijske i kibernetičke sigurnosti (kroz razgovor, forum ili radionice), diseminacijom kontakata i prezentacija s relevantnih konferencija na kojima je sudjelovao neki od članova radne skupine;
- lobiranjem kod donositelja odluka te u ustanovama u zdravstvu za donošenje prikladnih mjera informacijske i kibernetičke sigurnosti te osiguravanjem pravnog i financijskog okvira za podizanje razine sigurnosti mrežnih i informacijskih sustava u okviru Zdravstvene informacijske infrastrukture RH;
- aktivnim predlaganjem poboljšanih mjera informacijske i kibernetičke sigurnosti u zdravstvu, kroz smjernice, preporuke i prijedloge politika te lobiranje kod donositelja odluka;
- suradnjom s drugim radnim skupinama (unutar i izvan HDMI-a) te srodnim inicijativama i stručnim udrugama (npr. ISACA Croatia Chapter), s ciljem prepoznavanja zajedničkih izazova (npr. potreba za dodatnom edukacijom zdravstvenog osoblja o informacijskoj i kibernetičkoj sigurnosti) i predlaganja zajedničkih rješenja;
- podizanjem svijesti stručnog osoblja u zdravstvu o mogućnostima i važnosti informacijske i kibernetičke sigurnosti kroz suradnju s relevantnim društvima i komorama te kroz edukaciju studenata, uz korištenje primjera iz prakse;
- podizanjem svijesti pacijenata i građana o mogućnostima i važnosti informacijske i kibernetičke sigurnosti u zdravstvu putem web sjedišta HDMI-a i kroz suradnju s udrugama pacijenata i drugim organizacijama civilnog društva.

Plan rada Radne skupine IKS do kraja 2021. godine obuhvaća sljedeće aktivnosti:

1. situacijsku analizu informacijske i kibernetičke sigurnosti u zdravstvu RH, korištenjem prikladnih metodologija i obuhvata reprezentativnog uzorka ustanova i drugih dionika;

2. uključivanje jednog člana radne skupine u stručnu skupinu na međunarodnoj razini i u suradnji s EU tijelima (Europska komisija – DG CONNECT, EU agencija ENISA, itd.);
3. izradu dokumenta sa smjernicama i/ili preporukama o mjerama informacijske i kibernetičke sigurnosti za jednu razinu zdravstvene zaštite (npr. primarnu) i/ili jednu kategoriju ustanova u zdravstvu (npr. bolničke ustanove);
4. najmanje jedno predstavljanje radne skupine na relevantnim međunarodnim konferencijama i stručnim časopisima.

Članovi HDMI-a zainteresirani za sudjelovanje u Radnoj skupini IKS mogu se javiti voditelju Hrvoju Belaniju na adresu e-pošte hrvoje.belani{@}miz.hr, a sve javne isporuke Radne skupine, kao i druge relevantne informacije iz područja informacijske i kibernetičke sigurnosti objavljivat će se na mrežnim stranicama HDMI-a.