SWOT analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske

Hrvoje Belani[1], Josipa Kern[2], Nikola Protrka[3], Kristina Fišter[2], Mira Hercigonja-Szekeres[4]

[1]*Ministarstvo zdravstva, Uprava za e-zdravstvo, Zagreb, Hrvatska*

[2]*Sveučilište u Zagrebu, Medicinski fakultet, Zagreb, Hrvatska*

[3]*Ministarstvo unutarnjih poslova, Policijska akademija – Visoka policijska škola u Zagrebu, Zagreb, Hrvatska*

[4]*Veleučilište Hrvatsko zagorje Krapina, Zavod za informatiku, Krapina, Hrvatska*

e-pošta: hrvoje.belani@miz.hr

Sažetak: SWOT analiza je tehnika strateškog planiranja koja se može koristiti za definiranje snage, slabosti, prilika i prijetnji pri zdravstvenim ustanovama kako bi pružila jasan pregled kritičnih pokazatelja ključnih za učinak i ukupni uspjeh njihovog djelovanja i poslovanja. Cilj ovog rada je 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. SWOT analiza se provodi bez navođenja pojedinačnih zdravstvenih ustanova, već transparentno prikazuje snage, slabosti, prilike i prijetnje koje obuhvaćaju informacijsku i kibernetičku sigurnost različitih zdravstvenih ustanova Hrvatske, uvažavajući činjenicu da su mnogim ustanovama pojedine SWOT stavke zajedničke. Ovim se radom želi dati stručni doprinos koji će predstavljati temelj za daljnju razradu strategije podizanja razine informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske. Rezultati pokazuju podjednaku prisutnost svih elemenata, s potencijalom umanjivanja svih slabosti i prijetnji.

Ključne riječi: informacijska sigurnost; kibernetička sigurnost; SWOT analiza; zdravstvo; NIS direktiva

Uvod

Sigurnosne ranjivosti inherentno su prisutne u računalnim sustavima, koji postaju posebno izloženi ako djeluju u kibernetičkom prostoru, dakle spojeni na internet i s njim povezane sustave. Dok je ranjivosti računalnog sklopovlja (hardvera) donekle složenije prepoznati i iskoristiti, programska podrška (softver) redovito je meta najrazličitijih oblika kibernetičkih napada i ostvarivanja sigurnosnih prijetnji bilo vanjskih ili unutarnjih zlonamjernika ili pak nepažljivih korisnika koji uzrokuju računalno-sigurnosne incidente. Pri tome ni sustavi u zdravstvu nisu iznimka.

Štoviše, prvi dokumentirani *ransomware* napad dogodio se još u prosincu 1989. godine, poznat pod nazivima *AIDS Trojan* i *PC Cyborg*, kad je harvardski znanstvenik i evolucijski biolog dr. Joseph L. Popp povodom konferencije Svjetske zdravstvene organizacije (SZO) o AIDS-u polaznicima poštom distribuirao dvadeset tisuća 5,25-inčnih disketa s upitnikom o ovoj opasnoj virusnoj bolesti (1). Korištenjem diskete *ransomware* bi se učitao u računalo i aktivirao tek nakon 90 podizanja operacijskog sustava, šifrirao nazive datoteka i sakrio ih na drugo mjesto te ispisao obavijest da je sustav zaražen, podaci korisnika nedostupni te je

potrebno uplatiti 189 odnosno 378 USD otkupnine korporaciji *PC Cyborg* u Panami. Iako zlonamjernik nije primio mnogo uplata, ubrzo je uhapšen, osuđen i proveo neko vrijeme u zatvoru zbog počinjene značajne štete, a mnogi su korisnici u panici prebrisali memorije svojih računala pa su neke istraživačke i medicinske ustanove izgubile rezultate višegodišnjeg rada.

Kako bi se uklonili ili u najvećoj mogućoj mjeri umanjili rizici od kibernetičkog napada, nužno je biti svjestan njihova postojanja, znati kakva postupanja ili nepostupanja rizike povećavaju te prilagoditi načine korištenja računalnih sustava. Drugim riječima, neophodno je sustavno podizati i održavati prikladnu razinu kibernetičke sigurnosti računalnih sustava, kao i informacijske sigurnosti u odnosu na organizacije i procese koje ti računalni sustavi podržavaju.

Prema Nacionalnoj taksonomiji računalno-sigurnosnih incidenata (2) kibernetička sigurnost obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru, a slična definicija iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (3) navodi da je riječ o sustavu organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru. Informacijska sigurnost (4) je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. Stoga, informacijska sigurnost treba postojati bez obzira koriste li se ili ne koriste informacijsko-komunikacijske tehnologije (5). Ako se koriste, tada su neophodne i konkretne mjere kibernetičke sigurnosti. S obzirom da su informacijsko-komunikacijske tehnologije (IKT) nezaobilazne za današnje funkcioniranje zdravstvenih ustanova, u ovom se radu promatra sinergijski učinak informacijske i kibernetičke sigurnosti (IKS).

Struktura ovog rada je sljedeća: naredno poglavlje daje prikaz globalnog stanja kibernetičke sigurnosti u zdravstvu, ističući važnost IKS za zdravstvene sustave i njihove korisnike. Poglavlje iza toga predstavlja strukturu zdravstvenog sustava Republike Hrvatske po kategorijama i vrstama zdravstvenih ustanova, složenosti i raznolikosti procesa pružanja zdravstvene zaštite i skrbi te daje mapiranje predvidljive informacijske imovine po vrstama zdravstvenih ustanova Hrvatske. Središnji dio rada čini provedena SWOT analiza IKS u zdravstvenim ustanovama Hrvatske, nakon čega slijedi poglavlje s raspravom o rezultatima analize. Posljednje poglavlje daje zaključak o provedenoj analizi i njenoj korisnosti za zdravstveni sustav Republike Hrvatske te daje prijedlog daljnjih koraka.

Stanje kibernetičke sigurnosti u zdravstvu

Povećanjem stupnja informatizacije zdravstvenih ustanova i digitalne transformacije procesa u zdravstvu diljem svijeta, kao i povezivanjem s drugim dionicima i resorima (npr. socijalna skrb, prilagodba klimatskim promjenama, zaštita od industrijskog onečišćenja, itd.), kibernetička sigurnost u zdravstvu sve više dobiva na značaju. Prema godišnjem izvještaju EUROPOL-a o prijetnjama internetskog organiziranog kriminala (6), postoje naznake da je upotreba tradicionalnog masovno distribuiranog *ransomwarea* u opadanju i počinitelji sve više sami usmjeravaju *ransomware* prema privatnim tvrtkama, zdravstvenom i obrazovnom sektoru, kritičnoj infrastrukturi i vladinim institucijama. Zdravstvo je redovito na meti kibernetičkih napada, kako zlonamjernih pojedinaca i skupina, tako i državno sponzoriranih APT (*Advanced Persistent Threat*) kampanja iniciranih od strane obavještajnih sustava pojedinih država.

Prema godišnjem izvještaju Instituta Ponemon u suradnji s IBM-om (7), zdravstvo je i dalje, jedanaestu godinu zaredom, najskuplja industrija (uzimajući u obzir bolničke ustanove i klinike) u kojoj je trošak povrede podataka od 2020. do 2021. godine globalno porastao za 30 %, sa 7,13 milijuna USD na 9,23 milijuna USD, dok je trošak povrede podataka u drugim industrijama prosječno porastao 10 %. Usporedbe radi, energetika je pala iz druge najskuplje industrije na peto mjesto, smanjivši troškove sa 6,39 milijuna USD u 2020. na 4,65 milijuna dolara u 2021. što čini smanjenje od 27,2 %. Priključuju se i druge industrije koje su doživjele velika povećanja troškova: uslužni sektor (porast 7,8 %), komunikacije – tisak, izdavaštvo, oglašavanje i odnosi s javnošću (porast 20,3 %), proizvodnja i distribucija robe za potrošnju (porast 42,9 %), maloprodaja (porast 62,7 %), elektronički mediji i komunikacije (porast 92,1 %), ugostiteljstvo (porast 76,2 %) te javni sektor (porast 78,7 %).

Najnovije istraživanje Juniper Researcha (8) navodi da će do 2026. godine pametne bolnice u svijetu imati 7,4 milijuna povezanih uređaja iz kategorije internetski povezivih medicinskih uređaja (*Internet of Medical Things, IoMT*), odnosno najmanje 3850 povezanih uređaja u svakoj pametnoj bolnici, što predstavlja ogroman rast od 231 % u odnosu na 2021. godinu. Pružanje zdravstvenih usluga koje koriste povezane uređaje kao što su senzori za daljinsko praćenje i kirurška robotika iziskivat će još veću pažnju i sustavan, planski pristup informacijskoj i kibernetičkoj sigurnosti, od razine nacionalnih zdravstvenih sustava preko ustanova pa sve do uređaja i samih korisnika, uključujući zdravstvene i druge djelatnike u zdravstvu te same pacijente.

Zdravstvene ustanove u Hrvatskoj

Prema Hrvatskom zdravstveno-statističkom ljetopisu za 2019. godinu (9), u Republici Hrvatskoj ima 49 domova zdravlja te 76 bolničkih ustanova i lječilišta, od kojih se 11 specijalnih bolnica i 5 lječilišta nalazi u privatnom vlasništvu. Tu je još 22 zavoda za javno zdravstvo, po jedan zavod za transfuzijsku medicinu i zavod za hitnu medicinu, 21 ustanova za hitnu pomoć, 358 poliklinika, 280 ustanova za njegu-skrb (koncesionari u domovima zdravlja i ustanovama te privatne prakse svrstani su pod privatno vlasništvo) te 648 trgovačkih društava za obavljanje zdravstvenih djelatnosti. Ukupan broj ljekarničkih ustanova, uključujući pripadne ljekarničke jedinice, prema podacima Hrvatske ljekarničke komore početkom 2022. godine, iznosi 1197, od čega je 42 u vlasništvu Grada Zagreba, 232 u vlasništvu županija (uključujući njih 27 u domovima zdravlja) te 950 privatnih ljekarničkih praksi. Broj ustanova za medicinu rada, prema podacima HZJZ-a mimo ljetopisa, iznosi 168, od čega njih 43 djeluje u domovima zdravlja, 1 u poliklinici Zagreb, a ostali su različiti oblici privatnih praksi. To čini sveukupno 2848 zdravstvenih ustanova bez obzira na vrstu vlasništva. Ako se ovdje pridodaju Hrvatski zavod za zdravstveno osiguranje (HZZO), koji provodi obvezno zdravstveno osiguranje, te Agencija za lijekove i medicinske djelatnosti (HALMED), koja obavlja poslove vezane uz lijekove, medicinske proizvode i homeopatske lijekove te veterinarsko-medicinske proizvode, ukupan broj ustanova iznosi 2850, raspoređenih po vrsti ustanove i vrsti vlasništva (Tablica 1, Prilog). Podaci su podložni i drugačijoj interpretaciji vlasništva, no ovdje prikazani daju dovoljno zoran prikaz..

Sukladno Zakonu o zdravstvenoj zaštiti (10), zdravstvena djelatnost obavlja se na primarnoj, sekundarnoj i tercijarnoj razini te na razini zdravstvenih zavoda. Zdravstvena djelatnost na primarnoj razini provodi se i organizira kao timski rad, a obuhvaća djelatnost domova zdravlja. Zdravstvena djelatnost na sekundarnoj razini provodi se i organizira kao specijalističko-konzilijarna i bolnička djelatnost, a obuhvaća djelatnost domova zdravlja i bolničkih ustanova. Zdravstvena djelatnost na tercijarnoj razini provodi se i organizira kao pružanje najsloženijih oblika zdravstvene zaštite iz specijalističko-konzilijarnih i bolničkih djelatnosti. Obuhvaća djelatnost klinika, kliničkih bolnica i kliničkih bolničkih centara.

U kontekstu ovog rada predmet SWOT analize su sve kategorije i vrste zdravstvenih ustanova Hrvatske, bez obzira na vrstu vlasništva, uvažavajući raznolikost u svrsi, opremljenosti i razini zdravstvene zaštite i skrbi koju zdravstvene ustanove pružaju. Kao podloga za provedbu SWOT analize pripremljeno je osnovno mapiranje predvidljive informacijske imovine po vrstama zdravstvenih ustanova Hrvatske (Tablica 2, Prilog), navođenjem najvažnijih informacijskih sustava, aplikacija, programskih rješenja, informacijsko-komunikacijske infrastrukture i sklopovlja kakvu pojedina vrsta zdravstvene ustanove predvidljivo ima, a sastavni su dio Zdravstvene informacijske infrastrukture RH, u smislu Zakona o podacima i informacijama u zdravstvu (11).

Priprema i provedba SWOT analize

SWOT (*Strengths, Weaknesses, Opportunities, and Threats*) analiza je tehnika strateškog planiranja, koja se koristi za definiranje snage (ili prednosti), slabosti, prilika (ili mogućnosti) i prijetnji organizacije, ustanove ili prakse u poslovnom okruženju (12). U kontekstu zdravstvenih ustanova, SWOT analiza pruža jasan pregled kritičnih pokazatelja koji su ključni za učinak i ukupni uspjeh njihovog poslovanja. Namjena SWOT analize u ovom radu jest procijeniti stanje informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske, kako je prikazano u Tablicama 3 i 4 (Prilog), uključujući i domove zdravlja i bolničke ustanove, na temelju javno dostupnih informacija i saznanja autora. SWOT analiza se provodi bez navođenja pojedinačnih zdravstvenih ustanova, već transparentno prikazuje snage, slabosti, prilike i prijetnje koje se odnose na informacijsku i kibernetičku sigurnost različitih vrsta zdravstvenih ustanova Hrvatske, uvažavajući činjenicu da su mnogim ustanovama pojedine SWOT stavke zajedničke. Rezultat ovog rada stručni je doprinos za daljnju razradu strategije podizanja razine informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske.

Rasprava o rezultatima analize

Procesi u zdravstvenim sustavima doživljavaju digitalnu transformaciju i sve se više oslanjaju na IKT, što ujedno širi polje mogućih vektora napada kibernetičkih kriminalaca. Zdravstveni djelatnici, s jedne strane, trebaju imati na raspolaganju brze, točne i pouzdane IKT alate s ciljem poboljšanja kvalitete zdravstvene zaštite i skrbi, dok s druge strane stručnjaci za kibernetičku sigurnost kontinuirano razvijaju nove strategije i najbolje prakse s ciljem zaštite zdravstvenih podataka i informacija od napada i ugroza (20). Hrvatska se suočava s velikim nedostatkom liječnika pa će se daljnje širenje jaza između potreba i ponude barem dijelom pokušati nadoknaditi uvođenjem tehnoloških rješenja koja će pomoći u poboljšanju kvalitete zdravstvenih usluga (21). No, za to je neophodna kontinuirana edukacija svih interesnih dionika o IKT i IKS.

Provedena SWOT analiza daje pregled snaga, slabosti, prilika i prijetnji koje su karakteristične za zdravstvene ustanove Hrvatske s obzirom na informacijsku i kibernetičku sigurnost. Među snage je uvršten postojeći pravni okvir koji omogućava uređenije postupanje sa zdravstvenim podacima i informacijama, a ujedno i podizanje razine kibernetičke sigurnosti barem u dijelu ključnih usluga koje pružaju one zdravstvene ustanove koje su identificirane kao operatori ključnih usluga, koristeći kritičnu IKT infrastrukturu. Slabosti su u nedorečenosti donesenih zakona, nedostatak pravilnika i posljedično neravnomjerno postupanje u zdravstvenim ustanovama u državnom i javnom vlasništvu u odnosu na privatne ustanove, što je potrebno preciznije operacionalizirati. Prilike u tom smislu su dodatna regulativa u područjima sekundarne upotrebe zdravstvenih podataka, koja je najavljena na razini Europske unije, kao i čitavog zajedničkog europskog zdravstvenopodatkovnog prostora (22).

Zdravstvena informacijska infrastruktura RH s postojećim informacijskim sustavima i pratećim sigurnosnim i zaštitnim mehanizmima predstavlja solidan temelj i dobru pretpostavku za daljnji razvoj, koji treba ići ukorak s novim tehnologijama otvarajući mogućnosti implementacije novih aplikacijskih programskih sučelja (*Application Programming Interface, API*) i uspostave veće razine interoperabilnosti, ujedno podižući razinu informacijske i kibernetičke sigurnosti već od faza planiranja i dizajna novih rješenja. Fragmentiranost medicinske dokumentacije još uvijek predstavlja izrazitu slabost sustava jer zahtijeva da zdravstveno osoblje ponovno traži informacije od pacijenta ili prepisuje iz papirnate dokumentacije, što povećava rizik za nepouzdanost informacija, narušava kvalitetu zdravstvene zaštite te dovodi do gubljenja vremena zbog neadekvatne ergonomije koja nije u skladu s normom HRN EN ISO 9241-210:2019 (23), a posljedično otvara mjesta sigurnosnim propustima zbog povećane birokracije.

Snaga je i u uvođenju edukacijskih sadržaja u obrazovanje zdravstvenih struka, gdje npr. većina medicinskih fakulteta te studija sestrinstva imaju u kurikulu sadržaje iz medicinske informatike pri čemu se posebno ističe zaštita podataka i sustava (24), a uvele su ih i srednje medicinske škole u obvezni program edukacije medicinskih sestara (25). Slabosti predstavlja trenutna situacija gdje podučavaju u obrazovnom sustavu te rade u zdravstvenom sustavu priučeni stručnjaci, odnosno nema sustavnog obrazovanja medicinskih informatičara (26). Pokazana je velika potreba za ciljanim kadrom medicinskih informatičara (27), pa je prilika uspostaviti novo zanimanje medicinskog informatičara u nacionalnom kvalifikacijskom okviru.

Kako bi se odnos prema IKS u zdravstvenim ustanovama održavao na zadovoljavajućoj razini, potrebna je kontinuirana podrška uprave svake ustanove, koja treba shvatiti važnost ulaganja u ova područja i biti svjesna neželjenih posljedica ako se ova područja zanemare radi uobičajenog izgovora – manjka financijskih sredstava. Potrebno je osvijestiti i medicinsku struku da zaštita podataka i informacijska sigurnost nisu teme kojima se bavi isključivo IT osoblje u ustanovama, već mora biti svakodnevni dio poslovne higijene svakog djelatnika.

Zaključak

Zahtjevi koji se stavljaju pred zdravstvene sustave u stalnom su porastu, dijelom zbog novih i nadolazećih pristupa i tehnologija, o čemu svjedoče i nastojanja za uvođenjem personaliziranog pristupa medicini i pružanju zdravstvene zaštite (28). Podizanje digitalnih vještina zdravstvenih djelatnika uopće, a posebno u područjima informacijske i kibernetičke sigurnosti, neophodno je kako bi se oni što spremniji uhvatili u koštac s izazovima koje donosi primjena novih i složenih tehnologija u medicini te zdravstvenoj zaštiti i skrbi (kao što su npr. kirurška robotika, primjena strojnog učenja u analizi medicinskih snimaka, analiza i zaključivanje nad velikim skupovima podataka, udaljeni nadzor sigurnosti i zdravlja pacijenata, itd.). Moraju se osnažiti u korištenju digitalnih alata i rješenja u e-zdravstvu.

Potrebno je dalje unaprjeđivati zdravstvenu informacijsku infrastrukturu, njene kapacitete i omogućiti sustavnu sekundarnu upotrebu podataka za poboljšanje znanstvenih i stručnih dostignuća te upravljanje zdravstvenim ustanovama i sustavom u cjelini, za što je nužno osigurati kvalitetu i sigurnost podataka (29). Učenje iz podataka jednako je važan aspekt informatizacije zdravstva kao što su to poboljšanje učinkovitosti procesa, pojednostavljenje administracije i smanjenje troškova, no zainteresirani istraživači i dalje se susreću s velikim preprekama u pristupu rutinski prikupljanim podacima, čak i u svojim matičnim ustanovama.

Jedna od nadolazećih tehnologija koje će naći svoju primjenu u zdravstvenom sustavu je zasigurno kvantno računarstvo (30), koje bi moglo transformirati medicinu te zdravstvenu

zaštitu i skrb nabolje u narednim godinama (31). No, samo je pitanje vremena kada će kvantna tehnologija ugroziti internetsku enkripciju na kojoj počiva informacijska i kibernetička sigurnost današnjih informacijskih sustava, stoga razvoj post-kvantnih kriptosustava mora biti jedan od prioriteta u srednjoročnom i dugoročnom razdoblju (32).

Zaključno, uz nužno kontinuirano obrazovanje zdravstvenih djelatnika te razvoj novih kvalifikacijskih i obrazovnih profila ciljanih stručnjaka medicinskih informatičara, jedan od prijedloga za učinkovito umanjenje rizika od kibernetičkih napada i ugroza je uspostava tzv. centra za dijeljenje i analizu informacija u zdravstvu (*Health Information Sharing and Analysis Center, H-ISAC*) na nacionalnoj razini, koji može operativno djelovati u sklopu postojeće Uprave za e-zdravstvo Ministarstva zdravstva. Funkcija centra H-ISAC u Hrvatskoj bila bi uspostaviti i sustavno provoditi skup procesa i organizacijskih postupaka s ciljem poboljšanja i unaprjeđenja informacijske i kibernetičke sigurnosti u zdravstvenom sektoru dijeljenjem informacija o kibernetičkim ranjivostima, rizicima, napadima, kao i preventivnim i korektivnim mjerama i rješenjima koja je potrebno poduzeti kako bi se izbjegle ili svele na najmanju moguću mjeru štete uzrokovane incidentima kibernetičke sigurnosti. Potrebno je zdravstvene ustanove redovito informirati i s njima razmjenjivati informacije o događajima i temama informacijske i kibernetičke sigurnosti kako bi se osigurala visoka razina kvalitetne i pouzdane zdravstvene zaštite i skrbi, omogućavanjem sigurnog i robusnog pristupa podacima pacijenata i zdravstvenih djelatnika, a H-ISAC je jedan od načina, kakav također preporučuje Agencija za kibernetičku sigurnost EU (ENISA) (33), da se to postigne.

Literatura

1. Lessing M. Case Study: AIDS Trojan Ransomware. SDxCentral; lipanj 2020. Dostupno na: https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/, pristup 25. siječnja 2022.
2. NCERT, ZSIS, HAKOM, HNB, MUP RH, MORH. Nacionalna taksonomija računalno-sigurnosnih incidenata. Verzija 2.1; prosinac 2021. Dostupno na: https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf, pristup 25. siječnja 2022.
3. NN 64/18. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Narodne novine; srpanj 2018. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_64_1305.html, pristup 25. siječnja 2022.
4. Republika Hrvatska. Ured Vijeća za nacionalnu sigurnost. Što je informacijska sigurnost? Dostupno na: https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost, pristup 25. siječnja 2022.
5. Belani H. Radna skupina za informacijsku i kibernetičku sigurnost (IKS). Bilten Hrvatskog društva za medicinsku informatiku (Online). 2021:27(2). Dostupno na: https://hrcak.srce.hr/clanak/378555, pristup 25. siječnja 2022.
6. Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. Dostupno na: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crim[e_threat_assessment_iocta_2021.pdf, pristup 25. siječnja 2022.
7. Ponemon Institute, IBM Security. Cost of a Data Breach Report 2021, IBM Corporation, New York, SAD. Dostupno na: https://www.ibm.com/security/data-breach, pristup 25. siječnja 2022.
8. Wears A. Smart Hospitals: Technologies, Global Adoption & Market Forecasts 2021-2026. Juniper Research, Basingstoke, Hampshire, Velika Britanija; October 2021. Dostupno na: https://www.juniperresearch.com/researchstore/key-vertical-markets/smart-hospitals-market-research, pristup 25. siječnja 2022.

9. HZJZ. Hrvatski zdravstveno-statistički ljetopis za 2019. godinu. Zagreb; 2020. Dostupno na: https://www.hzjz.hr/hrvatski-zdravstveno-statisticki-ljetopis/hrvatski-zdravstveno-statisticki-ljetopis-za-2019/, pristup 25. siječnja 2022.
10. NN 100/18, 125/19, 147/20. Zakon o zdravstvenoj zaštiti. Narodne novine; 2018. Dostupno na: http://digarhiv.gov.hr/arhiva/263/184016/narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_64_1305.html, pristup 25. siječnja 2022.
11. NN 14/19. Zakon o podacima i informacijama u zdravstvu. Narodne novine; veljača 2019. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2019_02_14_269.html, pristup 25. siječnja 2022.
12. Baghouri SM. A Step-By-Step Guide To SWOT Analysis In Healthcare, Unnus 2021. Dostupno na: https://unnus.com/medical/healthcare-swot-analysis/, pristup 25. siječnja 2022.
13. NN 68/18. Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga; srpanj 2018. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html, pristup 25. siječnja 2022.
14. NN 14/19. Zakon o podacima i informacijama u zdravstvu; siječanj 2019. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2019_02_14_269.html, pristup 25. siječnja 2022.
15. Deklaracija o e-zdravlju – Prva revizija; 2021. Akademija medicinskih znanosti Hrvatske. Dostupno na: http://www.amzh.hr/wp-content/uploads/2021/05/Deklaracija-o-eZdravlju-Prva-revizija-1.pdf, pristup 25. siječnja 2022.
16. Kern J, Mađarić M. Kako ocijeniti vrijednost e-zdravlja u Hrvatskoj?. Bilten Hrvatskog društva za medicinsku informatiku) (Online) [Internet]. 2020 [pristup 25. siječnja 2022.]; 26(1):11-23. Dostupno na: https://hrcak.srce.hr/235403.
17. Republika Hrvatska Zavod za sigurnost informacijskih sustava. Dostupno na: https://www.zsis.hr/, pristup 25. siječnja 2022.
18. Republika Hrvatska Sigurnosno-obavještajna agencija. Kibernetička sigurnost. Dostupno na: https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/, pristup 25. siječnja 2022.
19. Odjel za nacionalni CERT. Hrvatska akademska i istraživačka mreža (CARNET), Dostupno na: https://www.cert.hr/, pristup 25. siječnja 2022.
20. Baretić M, Protrka N. (2021) Healthcare Information Technology: Fast and Accurate Information Access vs. Cyber-Security. International Journal of E-Services and Mobile Applications 2021;13 (4):77-87. doi:10.4018/ijesma. 2021100105.
21. Relić D, Fišter K, Božikov J. Using Simulation Modeling to Inform Policy Makers for Planning Physician Workforce in Healthcare System in Croatia. Stud Health Technol Inform. 2019 Aug 21;264:1021-1025.
22. European Health Data Space, European Commission, Public Health, eHealth:Digital health and care. Dostupno na: https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en., pristup 25. siječnja 2022.
23. Hrvatski zavod za norme. Hrvatski normativni dokument: oznaka HRN EN ISO 9241-210:2019. Dostupno na https://repozitorij.hzn.hr/norm/HRN+EN+ISO+9241-210%3A2019. pristup 25. siječnja 2022.
24. Kern J, Petrovečki M (urednici). Medicinska informatika. Zagreb: Medicinska naklada 2009.
25. Matić I, Kern J, Matić N. Prikaz knjige: Matić I, Kern J, Matić N. Načela administracije - udžbenik za četvrti razred medicinske škole . Bilten Hrvatskog društva za medicinsku informatiku (Online) [Internet]. 2020 [pristupljeno 11.02.2022.];26(1):31-33. Dostupno na: https://hrcak.srce.hr/235406
26. Fišter K, Hrabač P, Relić D, Išgum B, Erceg M. Educational Landscape of Biomedical Informatics in Croatia: Who Are the Teachers and What Are Their Attitudes. Stud Health Technol Inform. 2018;255:217-221.

27. Fišter K, Belani H, Relić D, Erceg M. Biomedical Informatics Workforce in Croatia: Qualitative Analysis of Teachers' Opinions on Needs and Employment Opportunities. Stud Health Technol Inform. 2019 Aug 21;264:1921-1922.
28. Fišter K, Polašek O, Vuletić S, Kern J. Single nucleotide polymorphisms and health behaviours related to obesity - trawling the evidence in the prospect of personalised prevention. Stud Health Technol Inform. 2009;150:762-6.
29. Fišter K, Pleše B, Pristaš I, Kurth T, Kujundžić Tiljak M. Setting up research infrastructure for secondary use of routinely collected health care data in Croatia. Croat Med J. 2017 Oct 31;58(5):327-329.
30. Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J. Quantum Computing for Healthcare: A Review. 2021. Dostupno na: https://www.techrxiv.org/articles/preprint/Quantum_Computing_for_Healthcare_A_Review/17198702, pristup 25. siječnja 2022.
31. Solenov D, Brieler J, Scherrer JF. The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine. Mo Med. 2018;115(5):463-467.
32. Castelvecchi D. Quantum-computing pioneer warns of complacency over Internet security. Nature 2020;587(7833):189.
33. Information Sharing and Analysis Centers (ISACs), ENISA European Union Agency for Cybersecurity. Dostupno na https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing, pristup 25. siječnja 2022.

Prilozi

Tablica 1. Broj zdravstvenih ustanova u RH po vrsti ustanove i vrsti vlasništva u 2019./2022.

Vrsta vlasništva / Vrsta ustanove	Državno vlasništvo	Vlasništvo županije	Vlasništvo grada ili općine	Privatno vlasništvo
klinički bolnički centar	5	0	0	0
klinička bolnica	3	0	0	0
klinika	4	0	0	1
opća bolnica	0	22	0	0
specijalna bolnica	0	23	0	11
lječilište	0	2	0	5
poliklinika	0	0	11	347
zavod za javno zdravstvo	1	21	0	0
drugi zavod ili agencija	4	0	0	0
dom zdravlja	1	45	3	0
ljekarna	0	232	42	950
ustanova za hitnu pomoć	0	21	0	0
ustanova za medicinu rada	1	39	4	124
ustanova za njegu-skrb	0	1	1	278
trgovačko društvo za zdravstvene djelatnosti	0	0	0	648

Tablica 2. Mapiranje predvidljive informacijske imovine[*] po vrsti zdravstvene ustanove

<table>
<tr><th>Informacijska imovina
Vrsta ustanove</th><th>Programska podrška (softver)</th><th>Računalno sklopovlje (hardver)</th><th>Mrežna infrastruktura</th><th>Zdravstvena inform. infra.</th></tr>
<tr><td>klinički bolnički centar</td><td rowspan="6">- BIS (G100)
- RIS
- LIMS
- IS bolničke ljekarne
- Poslovni IS
- Centralna platforma za registraciju COVID testiranja
- G110
- G120</td><td rowspan="3">- vlastiti hardver na lokaciji ustanove
- CDU RH
- hardver u oblaku komercijalnog pružatelja usluge</td><td rowspan="6">- vlastita mrežna infrastruktura na lokaciji ustanove
- HealthNet (državne i javne ustanove)
- HITRONet (državne i javne ustanove)
- komercijalna mreža (državne, javne i privatne ustanove)</td><td rowspan="3">- CEZIH (portal, OsigInfo, eKarton, eNaručivanje, eUputnice, eNalazi, Prioritetno naručivanje, eVaccination, itd.)
- CUS (fakturiranje bolničkih računa, prijem i otpust, strukturirana otpusna pisma, DTS gruper, obavijesti korisnicima, evidencija opreme)
- eDelphyn
- eCEZDLIH</td></tr>
<tr><td>klinička bolnica</td></tr>
<tr><td>klinika</td></tr>
<tr><td>opća bolnica</td><td rowspan="3">- vlastiti hardver na lokaciji ustanove
- hardver u oblaku komercijalnog pružatelja usluge</td></tr>
<tr><td>specijalna bolnica</td></tr>
<tr><td>lječilište</td></tr>
<tr><td>poliklinika</td><td rowspan="2">- Vlastiti hardver na lokaciji ustanove
- CDU RH</td><td rowspan="2">- CEZIH (prijava zarazne bolesti, eVacc.), eCEZDLIH</td></tr>
<tr><td>zavod za javno zdravstvo</td><td>- NAJS, COVID-19 (nadzori, testiranja)</td></tr>
<tr><td>drugi zavod ili agencija</td><td>- ZOROH (HZZO)
- HALMED IS
- HZHM IS
- eDelphyn (HZTM)</td><td>- CEZIH (HZZO operator sustava)</td></tr>
<tr><td>dom zdravlja</td><td>G2, G3, G4, G5, G6, G7, G9, G13, COVID-19 (nadzori, testiranja)</td><td rowspan="2">- vlastiti hardver na lokaciji ustanove
- usluga u oblaku certificiranog proizvođača Gx</td><td rowspan="2">- CEZIH (portal, OsigInfo, eRecepti, eUputnice, eNalazi, eNaručivanje,eVacc., eKarton, ePomagala)
- eHDSI</td></tr>
<tr><td>ljekarna</td><td>- G8</td><td>- Komercijalna mreža</td></tr>
<tr><td>ustanova za hitnu pomoć</td><td>- ePCR</td><td rowspan="3">- vlastiti hardver na lokaciji ustanove
- hardver u oblaku komercijalnog pružatelja usluge</td><td rowspan="3">- vlastita mrežna infrastruktura
- HealthNet (državne i javne ustanove)
- komercijalna mreža (javne i privatne ustanove)</td><td>- CEZIH (OsigInfo, eKarton)</td></tr>
<tr><td>ustanova za medicinu rada</td><td>- IS za medicinu rada i zaštitu na radu</td><td>- CEZIH (eVacc.)
- COVID testiranja</td></tr>
<tr><td>ustanova za njegu-skrb</td><td>- G11
- G14</td><td>- COVID testiranja</td></tr>
</table>

** Kratice:*

BIS – bolnički informacijski sustav;
CEZIH – Središnji zdravstveni informacijski sustav RH;
ePCR – electronic Patient Care Record;
LIMS – laboratorijski informacijski sustav;
RIS – radiološki informacijski sustav;
CDU RH – Centar dijeljenih usluga Republike Hrvatske;
eHDSI – eHealth Digital Service Infrastructure;
IS – informacijski sustav (opći);
NAJS – Nacionalni javnozdravstveni informacijski sustav RH;
ZOROH – Zdravstveno osiguranje – Registar osiguranika Hrvatske;
Gx – programska podrška certificiranih proizvođača za različite zdravstvene djelatnosti (izvor: http://www.cezih.hr/).

Tablica 3. SW analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama

	Uglavnom pozitivno	**Uglavnom negativno**
	Snage (S)	**Slabosti (W)**
Unutarnji utjecaji	• Donesen Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kojim je dio zdravstvenih ustanova identificirano kao operatori ključnih usluga (čl. 7, prilog I.) (3) te Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (13). • Donesen Zakon o podacima i informacijama u zdravstvu (za IKS posebno važni čl. 19,26,30,31,34) (14). • Donesena Deklaracija o e-zdravlju, koja je uvrštena u strateške dokumente (15). • Sigurnosni sloj CEZIH-a kao obavezan za integraciju vanjskih informacijskih sustava i programske podrške certificiranih proizvođača. • Sigurnosna infrastruktura NAJS-a smještenog na državnoj informacijskoj infrastrukturi (DII), kao dio zdravstvene informacijske infrastrukture (ZII). • Uvedeni edukacijski sadržaji o zaštiti podataka i kibernetičkoj sigurnosti u obrazovanje zdravstvenih struka. • Predanost i opća sposobnost medicinskog, zdravstvenog, IT osoblja u ustanovama. • Interoperabilnost ZII (CEZIH i G2/G8) na EU razini (eHDSI).	• Nedostaje tijelo za nadzor pojava i upravljanja računalno-sigurnosnim incidentima (neažurnost sustava, nedozvoljeno korištenje resursa, itd.). • Nije doneseno pet podzakonskih akata – pravilnici o e-kartonu, CEZIH-u, NAJS-u, medicinskoj dokumentaciji, informacijskim standardima u zdravstvu te stručnom nadzoru. • Znatan stupanj birokracije u ustanovama uzrokuje sigurnosne propuste (arhiv po hodnicima, itd.). • Nedovoljna uređenost informacijske sigurnosti (npr. neredovite pričuvne kopije) predstavlja kontinuirani rizik. • Umor djelatnika zbog prekovremenog rada može uzrokovati pogreške u postupanju s osjetljivim podacima. • Nedostatak kontinuirane podrške uprave ustanove i neprikladno izdvajanje iz proračuna može dovesti do neželjenih posljedica IKS. • Nedovoljna interoperabilnost nekih Gx aplikacija s CEZIH-om bez zajedničkog modela za razmjenu podataka (16). • Nepostojanje automatizirane razmjene medicinskih podataka među bolničkim informacijskim sustavima.

Tablica 4. OT analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama

	Uglavnom pozitivno	**Uglavnom negativno**
	Prilike (O)	**Prijetnje (T)**
Vanjski utjecaji	• Nacionalni i EU propisi kao poluga za povećanje proračuna ustanova za IKS. • Interes medija i javnosti za zdravstveni sustav treba iskoristiti za proaktivnu i pozitivnu komunikaciju te promicanje potreba u područjima IKS u zdravstvu. • Redovitije obnavljanje računalne opreme i sklopovlja i financiranje novih modernih medicinskih uređaja. • Centraliziranost sustava za obradu podataka u pojedinim dijelovima zdravstvenog sustava: CEZIH za zdravstvenu zaštitu, NAJS za javno zdravstvo, CUS za upravljanje bolnicama, eDelphyn za transfuziju, itd. • Intenzivnija suradnja s tehničkim tijelima izvan resora zdravstva (npr. Zavod za sigurnost informacijskih sustava (17), Centar za kibernetičku sigurnost Sigurnosno-obavještajne agencije (18), Nacionalni CERT (19), itd.). • Sustavan rad na edukaciji i informiranju svih dionika u sustavu (zdravstvenih radnika, informatičara koji rade u zdravstvu, drugih zaposlenika u zdravstvu, ali i korisnika) o IKS. • Reguliranje sekundarne upotrebe podataka na razini EU te zajedničkog europskog zdravstvenopodatkovnog prostora. • Učenje na iskustvima digitalizacije tijekom epidemije bolesti COVID-19.	• Sve veći rizici od računalno-sigurnosnih incidenata i hakerskih napada u zdravstvenom sustavu. • Svaki, i najmanji nedostatak informiranosti i edukacije može dovesti do nemarnih radnji i računalno-sigurnosnih incidenata s posljedicama izvan sustava zdravstva. • Manjak stručnog osoblja u zdravstvenom sustavu i izvan njega povećava rizike od pojave propusta IKS. • Veća izloženost komercijalnih pružatelja usluga u oblaku napadima i povredi zdravstvenih podataka. • Složenost implementiranih informacijskih sustava zahtijeva veću pažnju i posvećenost međuresornih stručnih timova. • Manjak vizije uprava zdravstvenih ustanova o važnosti ulaganja u IKS. • Nerazumijevanje medicinske struke o važnosti edukacije i provedbe mjera IKS. • Nedovoljna educiranost i informiranost zdravstvenog osoblja o IKS postojećih informacijskih sustava može dovesti do propusta i štete (financije, sigurnost pacijenata, itd.). • Neizvjesnost obzirom na dolazak kvantnih tehnologija i njihovu primjenu u zdravstvenom sustavu. • Prijetnje koje donosi primjena nadola-zećih tehnologija (npr. 3D ispisivanje)

SWOT Analysis of Information Security and Cybersecurity in Croatian Healthcare Institutions

Hrvoje Belani[1], Josipa Kern[2], Nikola Protrka[3], Kristina Fišter[2], Mira Hercigonja-Szekeres[4]

[1]*Ministry of Health, Directorate for e-Health, Zagreb, Croatia*

[2]*University of Zagreb, School of Medicine, Zagreb, Croatia*

[3]*Ministry of Interior, Police Academy – Zagreb Police College, Zagreb, Croatia*

[4]*University of Applied Sciences Hrvatsko Zagorje Krapina, Department for Informatics. Krapina, Croatia*

e-mail: hrvoje.belani@miz.hr

Abstract: SWOT analysis is a strategic planning technique that can be used to define the strengths, weaknesses, opportunities and threats at health facilities to provide a clear overview of critical indicators crucial to the performance and overall success of their operations and business activities. The aim of this paper is to assess the state of information security and cybersecurity in Croatian healthcare institutions, including health centres and hospitals, based on publicly available information and awareness of the authors. The SWOT analysis is conducted without mentioning individual healthcare institutions, but transparently shows the strengths, weaknesses, opportunities and threats that include information security and cybersecurity of various healthcare institutions in Croatia, taking into account the fact that many SWOT items are common to many institutions. This paper aims to provide an expert contribution that will be the basis for further elaboration of the strategy for raising the level of information security and cybersecurity in Croatian healthcare institutions. The results show equal presence of all elements, with the potential to reduce all weaknesses and threats.

Keywords: information security; cybersecurity; SWOT analysis; healthcare; NIS directive