OTPORNOST ŽELJEZNIČKOG SEKTORA NA KIBERNETIČKE PRIJETNJE

dr. sc. **Bernard Vukelić**

Veleučilište u Rijeci

bvukelic@veleri.hr

dr. sc. **Nikola Protrka**

Veleučilište kriminalistike i javne sigurnosti

nprotrka@fkz.hr

UDK: 004.056+625.1

Digitalizacija željezničkog sektora donosi brojne prednosti, ali istodobno povećava ranjivost na kibernetičke napade koji mogu ozbiljno ugroziti sigurnost i operativnost sustava. Stručni rad analizira ključne prijetnje i izazove te opisom stvarnih primjera napada ističe važnost jačanja kibernetičke otpornosti u željezničkome sektoru.

1. Uvod

Željeznički sektor, kao jedna od najvažnijih grana kritične infrastrukture, igra ključnu ulogu u povezivanju zajednica, ekonomiji i održivome razvoju. Digitalizacija željezničkih sustava donosi znatne prednosti poput veće operativne učinkovitosti, smanjenja troškova održavanja i unapređenja sigurnosti putnika i tereta. Međutim, s uvođenjem novih tehnologija sektor se suočava s novim izazovima, posebno u području kibernetičke sigurnosti. Sve veća upotreba informacijsko-komunikacijskih tehnologija (ICT) u željezničkoj infrastrukturi povećava izloženost kibernetičkim prijetnjama. Kibernetički napadi na željezničke sustave mogu uzrokovati ozbiljne poremećaje, ugroziti sigurnost putnika te izazvati znatne ekonomske štete. Zbog toga su sigurnost mrežnih i informacijskih sustava postali prioriteti za željezničke operatere i zakonodavce.

U Europskoj uniji Direktiva NIS2 postavlja nove standarde za zaštitu kritične infrastrukture, ističući potrebu za unapređenjem sigurnosnih praksi i jačanjem otpornosti na kibernetičke napade. Ta Direktiva obuhvaća i željeznički sektor, postavljajući strože zahtjeve za operatere ključnih usluga. Slično tome Hrvatska je usvojila novi Zakon o kibernetičkoj sigurnosti koji prati smjernice Direktive NIS2, čime se dodatno osnažuje zaštita nacionalne kritične infrastrukture.

U skladu s navedenim u nastavku je dan sustavni pregled dosadašnjih istraživanja o kibernetičkoj sigurnosti u željezničkome sektoru te su analizirani stvarni primjeri incidenata. Također, istaknute su ključne prijetnje i izazovi s kojima se sektor suočava. Svrha je ovog stručnog rada istražiti ranjivosti i prijetnje u željezničkome sektoru uzrokovane sve većom digitalizacijom te skrenuti pozornost na važnost jačanja otpornosti na kibernetičke prijetnje analizom incidenata i postojećih istraživanja. Cilj je upozoriti na važnost kibernetičke otpornosti i razviti bolje razumijevanje koraka neophodnih za unaprjeđenje sigurnosti željezničkih sustava.

2. Dosadašnja istraživanja

Istraživanja u području kibernetičke sigurnosti željezničkih sustava fokusirana su na identificiranje ranjivosti u sustavima upravljanja vlakovima, signalizaciji i komunikacijskim protokolima. Glavni fokus istraživanja jesu teme povezane s definiranjem sigurnosnih svojstava željezničkih sustava, simulacije napada na željezničke sustave, razvoj i implementacija okvira i arhitekture za kibernetičku sigurnost, upravljanje rizicima, slabost ljudskog čimbenika te primjena umjetne inteligencije u kibernetičkoj sigurnosti. Istraživanja su pokazala da su mnogi željeznički sustavi dizajnirani prije pojave modernih kibernetičkih prijetnji, što ih čini posebno ranjivima.

Pregled dosadašnjih istraživanja ključan je za razumijevanje trenutačnog stanja kibernetičke sigurnosti u željezničkome sektoru, prepoznavanje postojećih praznina u znanju te usmjeravanje prema mjerama za jačanje otpornosti sustava, što je osnovni cilj ovog rada. U ovoj sekciji razrađena su dosadašnja istraživanja kroz tematske cjeline koje obuhvaćaju ključne aspekte kibernetičke sigurnosti željezničkih sustava.

Na temelju analize literature u nastavku opisani su ključni radovi koji se bave temama vezanima uz kibernetičku sigurnost željezničkih sustava. U ovoj sekciji razrađena su dosadašnja istraživanja kroz tematske cjeline koje obuhvaćaju ključne aspekte kibernetičke sigurnosti željezničkih sustava: ranjivosti sustava i infrastrukture, ljudski čimbenik, primjenu umjetne inteligencije (AI) te regulatorne okvire i sigurnosne strategije.

U radu Mikiver (1) pod naslovom „Cybersecurity in Railways: Identifying and Communicating Risks using System Dynamics Modeling“ opisani su rizici povezani s digitalizacijom željezničkog sustava i to kako oni utječu na sigurnost i kibernetičku sigurnost željeznica. Istraživanje primjenjuje sustavnu dinamičku modelaciju za prepoznavanje i komunikaciju rizika u sektoru željeznica te analizira kako povećanje razine digitalizacije može donijeti koristi, ali i povećati izloženost kibernetičkim napadima. Rad također identificira nove rizike vezane uz digitalizaciju kao što su promjene u sigurnosnoj kulturi, nejasne odgovornosti zbog deregulacije i smanjeni prioritet kibernetičke sigurnosti, što može utjecati na opću sigurnost željezničkog prometa. Opisani su različiti tipovi napada na željeznički sustav, uključujući napade poput *ransomwarea*, *DDoS* napada, curenja podataka i napada na integritet signala. Rizici povezani s tim napadima uključuju gubitak dostupnosti sustava, smanjenje razine sigurnosti, propuštanje povjerljivih podataka te ekonomske i reputacijske gubitke. Napadi mogu rezultirati

prekidom prometnih usluga, što utječe na pouzdanost i sigurnost prijevoza tereta i putnika. Osim toga rizici uključuju oštećenje infrastrukture, manipulaciju podacima i narušavanje povjerenja javnosti u sigurnost željezničkog sustava.

Primjeri uključuju radove Kour et al. (2), koji analiziraju kibernetičke prijetnje i utjecaje na željezničku infrastrukturu, te studiju Liveri et al. (3), koja ističe izazove kao što su nedostatak svijesti o kibernetičkoj sigurnosti među radnom snagom, poteškoće u povezivanju sigurnosnih i sigurnosnih sustava te izazovi digitalne transformacije željezničkog sektora. Kour i suradnici (4) provodili su istraživanja s fokusom na razvoju modela zrelosti za kibernetičku sigurnost željeznica te na identifikaciji ključnih praznina u sigurnosti sektora, uključujući nedostatak proaktivnosti i holističkog pristupa prema kibernetičkoj sigurnosti. U članku „A review on cybersecurity in railways" pregledane su glavne prijetnje, izazovi i prakse u pogledu kibernetičke sigurnosti željeznica. Članak analizira ranjivosti željezničkog sektora uslijed digitalizacije i primjene naprednih informacijskih i operativnih tehnologija. Osim toga autori ističu važnost razvoja odgovarajućih strategija i okvira kako bi se ublažili potencijalni rizici koji mogu ugroziti sigurnost sustava, putnika i infrastrukture. Rad daje sustavni pregled novih trendova i pristupa u kibernetičkoj sigurnosti te identificira moguća rješenja za budući razvoj pretraživanjem akademske i industrijske literature.

Autori su pretražili četiri popularne baze podataka (*Google Scholar*, *Scopus*, *Web of Science* i *IEEE Explore*), identificirajući 90 najrelevantnijih članaka. Analiza tih članaka pokazuje da se većina istraživanja o kibernetičkoj sigurnosti u željezničkome sektoru temelji na konceptualnim okvirima te da zaostaju u primjeni sigurnosnih rješenja koja primjenjuju umjetnu inteligenciju (AI). Članak se osvrće na dosadašnja istraživanja, identificira praznine u postojećim praksama i daje preporuke za poboljšanje kibernetičke otpornosti željeznica, uključujući naprednu obuku zaposlenika, bolju integraciju sigurnosnih tehnologija i osiguravanje odgovarajućih sigurnosnih standarda za cijelu industriju.

Masson i Gransart (5) istaknuli su manjak europskih zakona o kibernetičkoj sigurnosti za transport te nizak stupanj svijesti u tome sektoru. Izdvojili su potrebu za proaktivnijim pristupom prema kibernetičkoj sigurnosti te za edukacijom i obukom sadašnje i buduće radne snage.

U članku Thadurija, A., Aljumailija, M., Koura, R., i Karima, R. (6) pod naslovom „Cybersecurity for eMaintenance in railway infrastructure: risks and consequences" istraženi su rizici i posljedice uvođenja kibernetičke sigurnosti u e-održavanje željezničke infrastrukture. Glavni fokus je na analizi potencijalnih rizika i ranjivosti koje digitalizacija donosi, posebno u održavanju željezničkih sustava koji primjenjuju informacijsku i operativnu tehnologiju. Autori istražuju prijetnje koje proizlaze iz digitalizacije te strategije za prevenciju i upravljanje rizicima koji mogu utjecati na sigurnost željezničkog prometa.

Autori poput Lva i Lia (7), Hatzivasilisa (8), Pizzija (9), Pawlika (10) i Heinricha (11) istraživali su teme sigurnosne autentifikacije, analize rizika, sigurnosne modele za CBTC sustave te zamjenu zastarjelih algoritama novim sigurnosnim rješenjima za željezničke komunikacije.

Autori Neema i Potteiger (12) istraživali su otpornost željezničkih sustava upotrebljavajući simulacije i modeliranje, uključujući evaluaciju otpornosti infrastrukture na kibernetičke napade te metamodeliranje otpornosti na temelju simuliranih podataka. Simulacije napada na željezničke sustave pokazale su kako napadači mogu iskoristiti ranjivosti za uzrokovanje poremećaja u operacijama, pa čak i ugroziti sigurnost putnika.

Ponsard (13) i Priscoli (14) predložili su različite okvire za sigurnost kao što su okvir KAOS za automatizirane operacije i okvir SHIELD za jačanje sigurnosti i privatnosti u željezničkim sustavima nadzora.

Autori Lopez i Agouado (15) obradili su metode za procjenu sigurnosnih rizika, fokusirajući se na europske željezničke kontrolne sustave i prijetnje koje se pojavljuju zbog povećane digitalizacije infrastrukture. Metode su uključivale primjenu robusnih kriptografskih mehanizama, uvođenje naprednog sustava distribucije ključeva, razvoj sigurnog modula za pohranu ključeva i integritet sustava te implementaciju mjera za sprječavanje ometanja radijskih signala. Autori Frangie i suradnici (16) istraživali su ulogu ljudskog čimbenika u kibernetičkoj sigurnosti željeznica, s težištem na razvoju preporuka i kontrole za sigurnosne procese unutar sustava.

Wang i suradnici (17) analizirali su primjenu umjetne inteligencije u kibernetičkoj sigurnosti željezničkih sustava, uključujući sigurnosne procjene i analizu rizika za sustave velikih brzina.

Istraživači su također istaknuli potrebu za kontinuiranom edukacijom zaposlenika.

3. Primjeri stvarnih incidenata

Željeznički sektor suočava se s nizom kibernetičkih prijetnji koje mogu ozbiljno utjecati na sigurnost i operativnost sustava. Posljednjih godina željeznički sektor postao je znatna meta kibernetičkih napada zbog povećanog opsega digitalizacije i uvođenja naprednih tehnologija. Prema članku objavljenom u ožujku 2023. u *International Railway Journalu* (18), Europska agencija za kibernetičku sigurnost (ENISA) objavila je svoj prvi izvještaj o kibernetičkim prijetnjama u transportnome sektoru, s posebnim težištem na željezničkome sektoru. Izvještaj obuhvaća razdoblje od siječnja 2021. do listopada 2022. i identificira glavne prijetnje, uključujući napade ucjenjivačkim softverom (engl. *ransomware*), koji čine 45 posto svih kibernetičkih napada na željeznice. Većina napada ciljala je IT sustave željeznica, uključujući sustave za prodaju karata, mobilne aplikacije i sustave za informiranje putnika, uzrokujući prekide u dostupnosti tih usluga.

Prema članku objavljenome na *SecureWorldu* (19), kibernetički napadi na željezničke sustave porasli su za 220 posto u posljednjih pet godina, a incidenti su zabilježeni diljem svijeta.

U nastavku opisano je nekoliko poznatih napada i sigurnosnih izazova s kojima se sektor suočavao posljednjih godina.

San Francisco Municipal Transportation Agency (SFMTA) ransomware napad (2016.)

U studenome 2016. *San Francisco Municipal Transportation Agency* (SFMTA) pretrpjela je napad ucjenjivačkim softverom (engl. *ransomware*) (20) koji je onemogućio sustave naplate karata, omogućujući putnicima besplatan prijevoz. Napadači su tražili otkupninu od 100 bitcoina za dešifriranje podataka. SFMTA je uspjela obnoviti sustave bez plaćanja otkupnine.

WannaCry napad na Deutsche Bahn (2017.)

U svibnju 2017. globalni napad ucjenjivačkim softverom poznat kao *WannaCry* pogodio je mnoge organizacije diljem svijeta, uključujući njemačkoga željezničkog prijevoznika Deutsche Bahn. Iako nisu zabilježeni ozbiljni poremećaji u voznome redu, napad je uzrokovao probleme s informacijskim ekranima na stanicama, automatima za prodaju karata i drugim digitalnim sustavima korisničkog servisa. (21)

Napad na Švedsku transportnu agenciju (2017.)

U listopadu 2017. švedska transportna agencija (*Transportstyrelsen*) bila je meta *DDoS* napada koji je prouzročio znatne smetnje u komunikacijskim mrežama i rezultirao prekidima u željezničkome prometu. Taj napad utjecao je na rad kontrolnih sustava koji upravljaju prometom vlakova, uzrokujući kašnjenja i obustave u željezničkome prometu u nekoliko dijelova zemlje. Napadi su doveli i do privremenog pada njihove službene mrežne stranice. (22)

Napad na dansku željezničku tvrtku DSB (2018.)

U svibnju 2018. danska državna željeznička tvrtka DSB pretrpjela je kibernetički napad koji je uzrokovao prekid u prodaji karata i informiranju putnika, što je dovelo do znatnih poremećaja u prometu. (23)

Napad na švicarskog proizvođača vlakova Stadler Rail (2020.)

U svibnju 2020. švicarski proizvođač vlakova *Stadler Rail* bio je meta kibernetičkog napada koji je rezultirao krađom osjetljivih podataka. Napadači su prijetili objavom ukradenih podataka ako otkupnina ne bude plaćena. (24)

Kibernetički napad na Northern Rail (2021.)

Tijekom ljeta 2021. *Northern Rail* suočio se s ozbiljnim kibernetičkim napadom usmjerenim na njihove novoinstalirane samoposlužne automate za prodaju karata, poznate kao *Flowbird*. Ti automati, instalirani samo dva mjeseca prije u sklopu modernizacijskog programa vrijednog 17 milijuna funti te popularni zbog mogućnosti beskontaktnog plaćanja, postali su meta *ransomware* napada koji je onemogućio njihovu funkcionalnost i uzrokovao znatne poremećaje u željezničkome prometu. Napadači su zahtijevali otkupninu u kriptovalutama u zamjenu za dekripcijski ključ. *Northern Rail* odmah je isključio pogođene automate i obavijestio nadležne vlasti. Obnova sustava trajala je nekoliko dana, tijekom kojih su putnici morali koristiti alternativne metode kupnje karata. (25)
Godina 2022. bila je vrlo izazovna za željezničku kibernetičku sigurnost zbog poznatih napada na željezničke mreže u Bjelorusiji, Italiji i Danskoj. U veljači 2022. hakerska skupina Cyberpartisans (26) napala je bjeloruske željeznice kako bi poremetila ruske vojne aktivnosti. U ožujku iste godine napad je uzrokovao obustavu prometa talijanskoga željezničkog poduzeća, dok je u listopadu iste godine sličan napad zaustavio željeznički promet u Njemačkoj. Talijanska državna željeznička tvrtka *Ferrovie dello Stato Italiane* (FS) u ožujku 2022. bila je meta *ransomware* napada. U tome slučaju hakeri su tražili pet milijuna dolara, uz prijetnju povećanja iznosa na 10 milijuna dolara ako se ne plati u roku od tri dana. Napad je doveo do privremenoga gašenja računalnih sustava kako bi se spriječilo širenje *malwarea*. Kao mjeru opreza tvrtka je obustavila prodaju karata putem interneta i u uredima, preusmjeravajući korisnike na alternativne metode kupnje. (27)

Napad na talijanski željeznički sustav (2023.)

U rujnu 2023. *Trenitalia*, najveći talijanski željeznički prijevoznik, suočila se s masivnim distribuiranim napadom uskraćivanja usluga *DDoS* (engl. *Distributed Denial of Service*). Napad je trajao nekoliko sati, uzrokujući znatne smetnje u njihovim mrežnim uslugama, uključujući sustave za mrežne rezervacije karata, informacijske mrežne stranice i mobilne aplikacije. Napadači su iskoristili botnet mrežu sastavljenu od milijuna kompromitiranih uređaja diljem svijeta kako bi preopteretili poslužitelje *Trenitalije* velikim količinama lažnog prometa. Cilj je bio ometanje dostupnosti ključnih usluga koje svakodnevno koriste milijuni putnika. Takvi napadi često primjenjuju različite metode, uključujući *SYN flood*, *UDP flood* i *HTTP flood*, kako bi zaobišli zaštitne mehanizme. Incident je potaknuo *Trenitaliju* da dodatno ojača svoje sigurnosne protokole, uključujući redovite sigurnosne provjere, unapređenje *firewalla* i implementaciju naprednih sustava za detekciju prijetnji. (28)

Napad na poljski željeznički sustav (2023.)

U kolovozu 2023. poljski željeznički sustav bio je meta kibernetičkog napada koji je uzrokovao zaustavljanje više od 20 vlakova. Napadači su iskoristili ranjivost u radio-stop sustavu, koji automatski zaustavlja vlakove pri prijemu određenog signala. Neki od lažnih signala sadržavali su rusku himnu i dijelove govora Vladimira Putina. Poljske vlasti istražuju moguće veze s ruskim akterima. (29)

Napad na javnu Wi-Fi mrežu na britanskim željezničkim postajama (2024.)
U rujnu 2024. javni Wi-Fi u 19 željezničkih postaja pod upravom *Network Raila* bio je meta kibernetičkog napada. Putnici koji su se pokušali povezati na Wi-Fi mrežu bili su preusmjereni na stranicu s islamofobnim porukama. *Network Rail* odmah je isključio Wi-Fi uslugu i pokrenuo istragu u suradnji s Britanskom prometnom policijom. Istraga je otkrila da je neovlaštena promjena na početnoj stranici Wi-Fi mreže obavljena putem legitimnoga administratorskog računa tvrtke *Global Reach*, koja pruža uslugu

Wi-Fi-ja. Nakon incidenta uhićen je zaposlenik *Global Reach Technologyja* pod sumnjom za prekršaje (30)

Naravno, to nisu jedini zabilježeni napadi na željeznički sektor. Tako je autor Arun Rajagopal (31), voditelj kibernetičke sigurnosti u tvrtki *AEGIS Engineering Services*, opisao niz velikih kibernetičkih napada na željeznički sektor posljednjih godina.

U 2015. poljski željeznički sustav pretrpio je napad koji je uzrokovao kvarove signalizacije i kašnjenja vlakova. U travnju 2016. belgijska željeznička mreža bila je meta napada koji je privremeno onemogućio mrežnu prodaju karata, dok su operacije vlakova ostale neometane. Iste godine gradski prijevoz San Francisca doživio je napad ucjenjivačkim softverom (engl. *ransomware*) koji je poremetio sustave naplate karata, no agencija je uspjela obnoviti sustave bez plaćanja otkupnine. U 2017. ukrajinski željeznički sustav bio je meta napada koji je poremetio sustave voznog reda, uzrokujući zbrku među putnicima, a u 2018. željeznički sektor u sjevernoj Engleskoj pretrpio je napad koji je utjecao na informacijske sustave i doveo do poremećaja u pružanju usluga. U svibnju 2020. njemački prijevoznik *Deutsche Bahn* doživio je napad koji je utjecao na prikaz informacija o dolascima i odlascima vlakova na platformama, uzrokujući neugodnosti za putnike. Iste godine Češke željeznice bile su meta napada koji je ciljao njihove sustave e-pošte i IT infrastrukturu, bez izravnih operativnih poremećaja. U srpnju 2020. hakeri su napali infrastrukturu Indijskih željeznica, defacirali službenu mrežnu stranicu i tražili otkupninu u bitcoinima. U siječnju 2020. *ransomware* napad pogodio je nekoliko tranzitnih sustava u jugoistočnome SAD-u, uključujući Regionalnu tranzitnu upravu New Orleansa, utječući na sustave naplate karata i voznog reda. Belgija je 2021. doživjela napad koji je utjecao na dispečerske sustave vlakova, uzrokujući poremećaje u voznome redu. Iste godine švicarski proizvođač vlakova *Stadler Rail* bio je meta napada koji je rezultirao krađom osjetljivih podataka, uz prijetnje objavom ukradenih podataka ako otkupnina ne bude plaćena.

4. Rasprava

U analizi prijetnji, izazova i stvarnih incidenata u željezničkome sektoru istaknuto je kako kibernetička sigurnost postaje prioritet za osiguranje kontinuiteta usluga i zaštitu infrastrukture. Ključni nalazi iz prethodnih sekcija upućuju na složenu prirodu prijetnji, koje obuhvaćaju tehnološke, organizacijske i ljudske čimbenike. Integracija tih nalaza u širi kontekst jasno pokazuje da uspješno suočavanje s tim izazovima zahtijeva suradnju različitih dionika, uključujući operatere, zakonodavce i istraživače.

Prikazani primjeri incidenata poput napada *ransomwareom* na *Deutsche Bahn* ili *DDoS* napada na talijansku željezničku mrežu upućuju na potrebu za jačanjem operativne otpornosti sustava. Direktive i zakoni nude temeljne smjernice, ali njihova primjena u praksi zahtijeva proaktivniji pristup. To uključuje redovitu procjenu ranjivosti, simulacije napada i integraciju suvremenih sigurnosnih tehnologija poput umjetne inteligencije i kriptografskih rješenja. Za zakonodavce osobito je važno osigurati odgovarajuće regulatorne mehanizme koji potiču suradnju među operaterima ključnih usluga i vlastima, ali i osigurati financijsku i tehničku podršku za implementaciju sigurnosnih mjera.

Dosadašnja istraživanja otkrivaju ključne praznine poput nedostatka integracije umjetne inteligencije u sigurnosne prakse i manjka koordinacije između sigurnosnih i operativnih sustava. Buduće istraživanje treba usmjeriti na razvoj okvira koji povezuju tehničke inovacije sa sustavnim pristupom upravljanju rizicima. Poseban je izazov edukacija zaposlenika i podizanje razine svijesti o kibernetičkim prijetnjama, što je identificirano kao jedan od glavnih čimbenika rizika.

Rezultati istraživanja ovog stručnog rada jasno pokazuju kako ranjivosti u željezničkome sektoru nisu samo tehničko pitanje, već i strateški izazov koji zahtijeva integrirani pristup. Jačanjem otpornosti sektora ne samo da se povećava razina sigurnosti, već se gradi povjerenje putnika i osigurava održivost sustava. Ovo istraživanje pruža smjernice za sustavno unaprjeđenje sigurnosnih praksi i ističe važnost ulaganja u kibernetičku sigurnost kao ključni element suvremenoga željezničkog sektora.

5. Zaključak

Kibernetička sigurnost u željezničkome sektoru sve je veći izazov koji zahtijeva proaktivan i koordiniran pristup svih dionika uključenih u upravljanje i zaštitu kritične infrastrukture. S obzirom na rastuću digitalizaciju sustava i složenost informacijsko-komunikacijskih tehnologija sektor se suočava s povećanom izloženošću sofisticiranim kibernetičkim prijetnjama. Primjeri iz prakse jasno pokazuju da posljedice kibernetičkih incidenata mogu biti ozbiljne, uključujući prekide u radu, ugrožavanje sigurnosti putnika i tereta te znatne ekonomske gubitke.

Europska unija kroz Direktivu NIS2 postavlja visoke standarde zaštite kritične infrastrukture, a Republika Hrvatska usklađuje se s tim smjernicama donošenjem Zakona o kibernetičkoj sigurnosti. Ipak, samo zakonski okvir nije dovoljan. Neophodno je omogućiti integraciju sigurnosnih mjera u sve faze razvoja i rada željezničkih sustava, od dizajna do svakodnevnih operacija.

Ključne komponente unaprjeđenja kibernetičke sigurnosti uključuju kontinuiranu edukaciju i obuku zaposlenika kako bi se smanjio rizik povezan s ljudskim čimbenikom, implementaciju suvremenih tehnoloških rješenja poput umjetne inteligencije za detekciju i prevenciju prijetnji, proaktivno upravljanje rizicima, što uključuje redovite procjene ranjivosti, simulacije napada i ažuriranje sigurnosnih protokola te suradnju na nacionalnoj i međunarodnoj razini radi razmjene znanja i resursa te usklađenog odgovora na prijetnje.

Sve veći broj incidenata ističe potrebu za ulaganjima u kibernetičku sigurnost kao temeljni prioritet željezničkih operatera. Ulaganje u zaštitu nije samo pitanje sigurnosti, već i povjerenja putnika i održivosti sektora. Izgradnja otpornog sustava koji može predvidjeti, spriječiti i brzo reagirati na kibernetičke prijetnje ključna je za osiguranje kontinuiranog i sigurnog prijevoza putnika i tereta.

Zaključno, željeznički sektor mora kontinuirano unapređivati svoju otpornost na kibernetičke prijetnje kako bi osigurao sigurne, pouzdane i učinkovite usluge u sve složenijemu digitalnom okružju.

LITERATURA

[1] Mikiver, C. (2022) - "Cybersecurity in Railways: Identifying and Communicating Risks using System Dynamics Modeling". KTH Industrial Engineering and Management.

[2] Kour, R., Thaduri, A., & Karim, R. (2019) - "Cybersecurity for railways–A maturity model". Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 234(10), str. 1129-1148.

[3] Liveri, D., Kour, R., & Karim, R. (2020) - "Cybersecurity in railway: A framework for improvement of digital asset security" (doktorska disertacija, Luleå University of Technology).

[4] Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2022) - "A review on cybersecurity in railways". Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit.

[5] Masson, É., & Gransart, C. (2017) - "Cyber security for railways-a huge challenge-Shift2Rail perspective". International workshop on communication technologies for vehicles, str. 97-104.

[6] Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019) - "Cybersecurity for eMaintenance in railway infrastructure: risks and consequences".

[7] Lv C and Li Y. (2019.) A security vehicle network organization method for railway freight train based on lightweight authentication and property verification. In: International Conference on Big Data and Security, Singapore, 20 December, 2019, pp. 178–189. Springer.

[8] Hatzivasilis G, Fysarakis K, Ioannidis S, et al. (2021): SPD-safe: secure administration of railway intelligent transportation systems. Electronics 2021; 10(1): 92.

[9] Pizzi G.(2020.): Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment. Transp Res Proc 2020; 45: 250–257.

[10] Pawlik M. (2019.): Railway safety and security versus groing cy bercrime challenges. In: International Conference on Transport Systems Telematics, Poland, 2019, pp. 57–68. Springer

[11] Heinrich M, Vieten J, Arul T, et al. (2018): 'Security analysis of the RaSTA safety protocol' In: 2018 IEEE International Conference on ISI, Miami, FL, USA, 9, pp. 199–204. IEEE.

[12] Neema H, Koutsoukos X, Potteiger B, et al. (2020) Simulation testbed for railway infrastructure security and resilience evaluation. In Proceedings of the 7th Symposium on Hot Topics in the Science of Security, New York, NY, 21 Sep tember, 2020, pp. 1–8.

[13] Ponsard C, Grandclaudon J, Massonet P, et al. Assessment of emerging standards for safety and security co-design on a 18 Proc IMechE Part F: J Rail and Rapid Transit 237(1) railway case study. In: International Conference on Model and Data Engineering, Marrakesh, Morocco, 24 October, 2018, pp. 130–145. Springer

[14] Priscoli FD, Giorgio AD, Esposito M, et al. Ensuring cyber security in smart railway surveillance with SHIELD. IJCCBS 2017; 7(2): 138–170.

[15] Lopez I and Aguado M. Cyber security analysis of the European train control system. IEEE Communications Magazine 2015.

[16] Frangie RC, Chehab T, Kan J, et al. Smart railways… or not so smart: a cyber security perspective. In: Rail: Smart, Automated, Sustainable: Proceedings of the 2018 Conference on Railway Excellence (CORE 2018), Sydney, Australia, pp.230–239.

[17] Wang, Y., & Xu Wei, J. (2018) - "Applications of artificial intelligence in cybersecurity for railway systems".

[18] International Railway Journal. (2023.): 'EU cybersecurity agency reports on threat to rail'. Preuzeto s https://www.railjournal.com/technology/eu-cybersecurity-agency-reports-on-threat-to-rail/ (Pristupljeno: 24. studenoga 2024.).

[19] Sivesind, C. (2024). 'Cyber Attacks on Railway Systems Increase by 220%', SecureWorld, 20 August. Dostupno na: https://www.secureworld.io/industry-news/railway-cyber-attacks (Pristupljeno: 24. studenoga 2024.).

[20] Greenberg, A. (2016) - 'San Francisco Municipal Transportation Agency ransomware attack'. Wired.

[21] Railway-News. (2017.): 'Global Cyber Attack Hits Deutsche Bahn'. Dostupno na: https://railway-news.com/global-cyber-attack-hits-deutsche-bahn/ (Pristupljeno: 20. studenoga 2024.).

[22] IT Security Guru. (2017.): 'Swedish Transport Agency hit by DDoS attack'. Dostupno na: https://www.itsecurityguru.org/2017/10/13/swedish-transport-agency-hit-ddos-attack/ (Pristupljeno: 18. studenoga 2024.).

[23] Reuters. (2018.): 'Danish train operator DSB hit by cyber attack'. Dostupno na: https://www.reuters.com/article/us-cyber-attack-danish-railways-idUSKCN1IP2M4 (Pristupljeno: 7. studenoga 2024.).

[24] BleepingComputer. (2020.): 'Ransomware attack hits train manufacturer Stadler Rail'. Dostupno na: https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-train-manufacturer-stadler-rail/ (Pristupljeno: 24. studenoga 2024.).

[25] Townsend, K. (2021). Ransomware Attack on UK Rail System – Spray and Pray or Targeted? SecurityWeek. Preuzeto s https://www.securityweek.com/ransomware-attack-uk-rail-system-spray-and-pray-or-targeted/ (Pristupljeno: 7. studenoga 2024.).

[26] Andrew Roth, "Cyberpartisans hack Belarusian railway to disrupt Russian buildup," The Guardian, 25 January 2022. https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup (Pristupljeno: 7. studenoga 2024.)

[27] Cybersecurity Trends. (2022). Ransomware: il riscatto per l'attacco hacker alle Ferrovie dello Stato sale a 10 milioni di euro. Rivista Cybersecurity Trends. Dostupno na: https://www.cybertrends.it/ransomware-il-riscatto-per-lattacco-hacker-alle-ferrovie-dello-stato-sale-a-10-milioni-di-euro/

[28] Briginshaw, D. (2022, March 29). Italian railway IT system suffers major cyber-attack. International Railway Journal. Dostupno na: https://www.railjournal.com/infrastructure/italian-railway-it-system-suffers-major-cyber-attack/ (Pristupljeno: 14. studenoga 2024.).

[29] Morris, L. (2023). 'Poland investigates train mishaps for possible Russian connection'. The Washington Post, 28. kolovoza. Dostupno na: https://www.washingtonpost.com/world/2023/08/28/poland-hacking-trains-russia/ (Pristupljeno: 24. studenoga 2024.).

[30] Stedman, H. (2024, 26. rujna). 'Cyber vandalism' shuts down wifi at 19 Network Rail stations. Evening Standard. Dostupno na https://www.standard.co.uk/news/tech/network-rail-british-transport-police-manchester-evening-news-europe-london-b1184337.html. (Pristupljeno: 29. studenoga 2024.)

[31] Rajagopal, A. (2024.): 'A Timeline of Cyber Attacks on the Rail Sector'. AEGIS Engineering Services,

SAŽETAK

OTPORNOST ŽELJEZNIČKOG SEKTORA NA KIBERNETIČKE PRIJETNJE

Željeznički sektor ključna je infrastruktura mnogih zemalja koja omogućuje prijevoz milijuna putnika i tereta svakoga dana. Digitalizacija sustava donosi poboljšanja u učinkovitosti i sigurnosti, no također povećava ranjivost na kibernetičke prijetnje. U Europskoj uniji Direktiva NIS2 postavlja strože zahtjeve za kibernetičku sigurnost, uključujući željeznički sektor, kako bi se zaštitila kritična infrastruktura. U Republici Hrvatskoj novi Zakon o kibernetičkoj sigurnosti prati tu Direktivu, ističući važnost upravljanja kibernetičkim rizicima i prijavljivanja incidenata. Ovaj stručni rad nudi pregled dosadašnjih istraživanja, analizira incidente i opisuje glavne prijetnje željezničkome sektoru.

Ključne riječi: *kibernetička sigurnost, željeznički sektor, kibernetički incidenti, prijetnje, incidenti*

Kategorizacija: *stručni rad*

SUMMARY

RESISTANCE OF THE RAILWAY SECTOR TO CYBER THREATS

The railway sector is the main infrastructure of many countries, enabling every day a millions passenger and freight transportation. Digitalization of systems brings improvements in efficiency and security, but also increases vulnerability to cyber threats. In the European Union, the NIS2 Directive provides measures for a high common level of cybersecurity to protect critical infrastructure, including in the railway sector. In the Republic of Croatia, the new Law on cybersecurity follows that Directive measures, emphasizing the importance of managing cyber risks and reporting incidents. This professional paper provides an overview of research, analyzes incidents and describes the main threats to the railway sector.

Key words: *cybersecurity, railway sector, cyber incidents, threats, incidents*

Categorization: *professional paper*