Sigurnost komunikacije u kritičnoj infrastrukturi

Antunović, Josip

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

SIGURNOST KOMUNIKACIJE U KRITIČNOJ INFRASTURKTURI

COMMUNICATION SECURITY IN CRITICAL INFRASTRUCTURE

Mentor: doc. dr. sc. Ivan Cvitić

Student: Josip Antunović
JMBAG: 0135257709

Zagreb, kolovoz 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Informacije i komunikacije**

ZAVRŠNI ZADATAK br. 6906

Pristupnik: **Josip Antunović (0135257709)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnost komunikacije u kritičnoj infrastrukturi**

Opis zadatka:

U okviru završnog rada potrebno je istražiti značenje pojma kritične infrastrukture te karakteristike takvog okruženja. Uz navedeno, potrebno je analizirati i prikazati sigurnosne izazove komunikacije u okruženju kritične infrastrukture kroz pregled trendova sigurnosti, postojećih ranjivosti i do sada zabilježenih sigurnosnih incidenata. Konačno, potrebno je pružiti i sustavni pregled postojećih metoda zaštite primjenjivih u kritičnoj infrastrukturi.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

SIGURNOST KOMUNIKACIJE U KRITIČNOJ INFRASTRUKTURI

SAŽETAK

Sigurnost je jedna od glavnih briga modernih komunikacijskih sustava. Podatak koji pridonosi tome je činjenica da će troškovi kibernetičkog kriminala do 2025. dosegnuti 10,5 milijardi dolara. Stoga se svakodnevno ulažu ogromne količine resursa kako bi se povećala razina sigurnosti svih vrsta sustava. Određeni sustavi su posebno osjetljivi na sigurnosne probleme, a to su sustavi kritične infrastrukture. Kritičnu infrastrukturu predstavljaju sustavi, mreže i objekti koji pružaju osnovne usluge društvu te predstavljaju okosnicu gospodarstva, sigurnosti i zdravlja nacije, a sigurnost i dobrobit društva ovisna je o njihovoj sigurnosti i otpornosti. Zaštita kritične infrastrukture ključna je za ispravno funkcioniranje društva i oslanja se na nju za održavanje javne sigurnosti, nacionalne sigurnosti i ekonomske stabilnosti. Kibernetički napadi na kritičnu infrastrukturu kao što su transportna, energetska, komunikacijska industrija i ostale mogu uzrokovati značajnu štetu infrastrukturi i društvu koje podržava. Ovaj završni rad daje pregled značajki kritične infrastrukture, opisuje sigurnosne izazove s kojima se kritična infrastruktura susreće, te raspravlja o važnosti razvoja sigurnosnih pristupa i tehnologija za rješavanje rastućih kibernetičkih prijetnji.

KLJUČNE RIJEČI: kritična infrastruktura; kibernetička prijetnja; komunikacijski sustavi; sigurnost

COMMUNICATION SECURITY IN CRITICAL INFRASTRUCTURE

SUMMARY

Security is one of the main concerns of modern communication systems. A contributing figure is the fact that cybercrime costs will reach $10.5 billion by 2025. Therefore, enormous amounts of resources are used every day to increase the level of security of all types of systems. Certain systems are particularly vulnerable to security issues, namely critical infrastructure systems. Critical infrastructure is represented by systems, networks and facilities that provide basic services to society and represent the backbone of the nation's economy, security and health, and the security and well-being of society depends on their security and resilience. Protecting critical infrastructure is critical to the proper functioning of society and relies on it to maintain public safety, national security, and economic stability. Cyber-attacks on critical infrastructure such as the transportation, energy, communications industry and others can cause severe damage to the infrastructure and the society it supports. This bachelor thesis provides an overview of the characteristics of critical infrastructure, describes the security challenges facing critical infrastructure, and discusses the importance of developing security approaches and technology to address evolving cyber threats.

KEY WORDS: critical infrastructure; cyber threat; communication systems; security

SADRŽAJ

1. UVOD

U posljednjih 20 godina komunikacijski sustavi su prošli kroz značajnu evoluciju zahvaljujući tehnološkom napretku. Razvoj pametnih telefona, bežične tehnologije, računarstva u oblaku potpuno je promijenio način komunikacije, pohrane podataka te njihove sigurnosti. Sa sve većim prijenosom informacija putem digitalnih kanala presretanje i praćenje komunikacije učinilo je tvrtke i vladine institucije ranjivima na povrede podataka, dovodeći u opasnost povjerljive i osjetljive informacije. Jedni od najosjetljivijih sustava su sustavi kritične infrastrukture, upravo iz razloga jer je njihovo funkcioniranje nužno za svakodnevni život. Kritični infrastrukturni sustavi su sve češće meta kibernetičkih napadača, što može dovesti do katastrofalnih kvarova poput kvarova u proizvodnji električne energije, kvarova u sustavima internetskog bankarstva te kvarovima u prometu. Cilj završnog rada je definirati značajke kritične infrastrukture te opisati sigurnosne izazove s kojima se ti sustavi susreću. Također u radu se navode ranjivosti sustava kritične infrastrukture, najnoviji trendovi sigurnosti te rješenja za osiguravanje sigurnosti kritične infrastrukture. Razumijevanjem ranjivosti kritične infrastrukture i razvojem učinkovitih politika i pravila možemo osigurati javnu sigurnost, ekonomsku dobrobit i nacionalnu sigurnost. S obzirom na navedeno završni rad sastoji se od 6 poglavlja:

1. Uvod

2. Analiza značajki kritične infrastrukture

3. Sigurnosni izazovi komunikacije u kritičnoj infrastrukturi

4. Pregled trendova sigurnosti kritične infrastrukture

5. Metode zaštite komunikacija u kritičnoj infrastrukturi

6. Zaključak.

Nakon uvodnog dijela u drugom poglavlju pod nazivom Analiza značajki kritične infrastrukture definiran je pojam kritična infrastruktura te su navedene međuovisnosti među njihovim sektorima. Analizirane su pojedine značajke kritične infrastrukture ovisno o sektoru te njihova važnost za zajednicu.

U trećem poglavlju pod nazivom Sigurnosni izazovi komunikacije u kritičnoj infrastrukturi navedene su vrste prijetnji koje mogu onesposobiti kritičnu infrastrukturu, te su opisane ranjivosti koje se trebaju nadvladati tijekom komunikacije u kritičnoj infrastrukturi.

U četvrtom poglavlju pod nazivom Pregled trendova sigurnosti kritične infrastrukture istaknut je utjecaj novih tehnologija na sigurnost kritične infrastrukture naglašavajući prednosti i ranjivosti povezane s njihovom implementacijom.

U petom poglavlju pod nazivom Metode zaštite komunikacija u kritičnoj infrastrukturi opisane su metode zaštite, te su navedene mjere koje je potrebno poduzeti za smanjenje potencijalnih napada na kritičnu infrastrukturu.

U završnom šestome poglavlju nalazi se Zaključak koji povezuje sva prethodna poglavlja i daje opći uvid u završni rad.

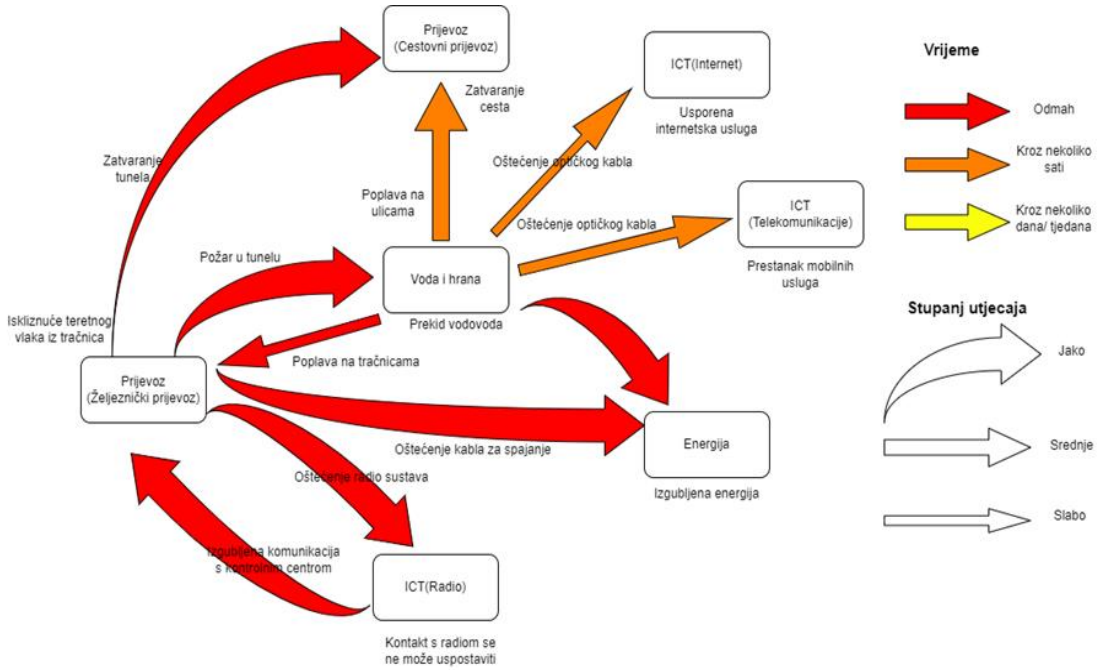
2. ANALIZA ZNAČAJKI KRITIČNE INFRASTRUKTURE

Kritična infrastruktura je vitalni dio modernih društava, budući da uključuje sredstva, sustave, objekte, mreže i druge elemente na koje se društvo oslanja kako bi održalo nacionalnu sigurnost, ekonomsku stabilnost te javno zdravlje i sigurnost [1]. Kritična infrastruktura odnosi se na temeljne sustave, objekte i mreže koji su bitni za funkcioniranje modernog društva. To uključuje stvari poput električnih mreža, javnih institucija, telekomunikacijskih sustava, vodoopskrbnih sustava, financijskih institucija i hitnih službi. Važnost kritične infrastrukture leži u činjenici da su ti sustavi okosnica modernog društva i bez njih bi svakodnevica stala [2].

2.1 Međuovisnosti sektora kritične infrastrukture

Rast i razvoj kritične infrastrukture pratio je i razvoj međuovisnosti njihovih sektora, kako na nacionalnoj tako i na međunarodnoj razini, a time i njihov pozitivan utjecaj na različite aspekte života, uključujući ekonomske, političke, kulturne i sigurnosne aspekte. Kada je riječ o poboljšanju zaštite kritične infrastrukture, jedan od najčešćih problema je nepotpuno poznavanje međuovisnosti infrastruktura. Kritične infrastrukture međusobno su ovisne, što znači da su potrebne jedna drugoj da bi uspješno funkcionirale. Naprimjer, transportni sustav ovisi o energetskom sektoru zbog izvora energije, dok se transportni sustav koristi za isporuku goriva energetskom sektoru. Kvar jedne kritične infrastrukture može imati kaskadni učinak na druge bitne infrastrukture, uzrokujući ogromne posljedice i financijski gubitak.

Potencijalni kaskadni učinci koji se mogu dogoditi vidljivi su na slici 1 koja na primjeru požara u tunelu u Baltimoreu pokazuje međuovisnosti sektora kritične infrastrukture. Boja strelice označava vrijeme koje je trebalo da se posljedice očituju (odmah, kroz par sati, kroz par dana /tjedana), dok debljina strelice označava stupanj utjecaja (jako, srednje, slabo). Uzrok navedenih događaja bilo je iskakanje vlaka koji je prevozio opasne kemikalije iz tračnica. Analizom ovog incidenta postaje vidljivo da poremećaj jednog elementa u kritičnoj infrastrukturi može pokrenuti lanac nepredvidivih događaja koji mogu biti štetni za cijelu zajednicu. Posljedice se mogu očitovati u različitim sektorima, a u nastavku će biti navedene događaji i konkretne posljedice koje je uzrokovao požar [3].



Slika 1. Međuovisnost sektora kritične infrastrukture na primjeru požara u tunelu u Baltimoreu
Izvor: [4]

Požar koji se dogodio u tunelu izazvao je pucanje vodovoda iznad tunela. Poplava koja se dogodila u nekim područjima je uzrokovala dubine i do 1 metra. Vatra i pucanje vodovoda oštetili su strujne kabele što je uzrokovalo nestanak električne energije za približno 1200 objekata u Baltimoreu. Presječeni kabel optičkih vlakana u tunelu bio je glavna internetska komunikacijska veza istočne obale koja je pripadala WorldComu. Prekid je usporio internetske usluge diljem Sjedinjenih Američkih Država (SAD) na nekoliko sati, također prekid željezničke usluge imao je značajan utjecaj u kašnjenju u isporuci ugljena i vapnenca. Za pripremu izvješća Nacionalnog odbora za sigurnost prometa trebalo je tri godine, a istraga nije uspjela utvrditi uzrok nesreće. Požar koji se dogodio u tunelu Howard Street naglašava važnost identificiranja potencijalnih ranjivosti prije nego što sto se nesreća dogodi, kao i uključivanja redundantnih sustava u slučaju nesreće. Također iz primjera je vidljivo poremećaji u jednom sektoru mogu ubrzo dovesti do kaskadnih učinaka na druge sektore. Ova međuovisnost naglašava važnost cjelovitog planiranja te koordinacije među sektorima kako bi se smanjio potencijalni utjecaj nesreća [5].

2.2 Pojmovno određivanje i podjela kritičnih infrastruktura

Izraz kritična infrastruktura odnosi se na fizičke i logičke sustave koji su neophodni za rad ekonomije i vlade. To uključuje, ali nije ograničeno na, telekomunikacije, energiju, bankarstvo i financije, prijevoz, sustave vodoopskrbe i hitne službe. S velikim potencijalnim rizicima u slučaju kašnjenja informacija ili gubitka podataka važno je uspostaviti sustave kritične komunikacije koji omogućuju brzo širenje ključnih informacija, te koordinirane odgovore hitnih službi i odgovarajućih tijela [6].

Kritična komunikacija može se definirati kao razmjena informacija koje su vitalne, hitne i često spašavaju život ili u situacijama u kojima je potrebno hitno djelovanje ili odgovor. Ova vrsta komunikacije događa se u okruženjima gdje bi svako kašnjenje ili pogrešno tumačenje moglo imati ozbiljne posljedice. Učinkovita kritična komunikacija ključna je za upravljanje katastrofama, nacionalnu sigurnost, zdravstvene usluge i prometnu sigurnost. Bez pouzdane kritične komunikacije, sposobnost brzog reagiranja na krizne situacije i zaštitu zajednice bila bi ozbiljno ugrožena.

Definiranje kritične infrastrukture često je vrlo individualno tako naprimjer ono što je kritična infrastruktura za jednu zajednicu možda neće biti kritična infrastruktura za drugu. Zato kao primjer navodi se nekoliko različitih definicija kritične infrastrukture prema određenim područjima ili zajednicama.

Definiranje pojma kritične infrastrukture u Europskoj Uniji: Kritičnu infrastrukturu čine djelatnosti, mreže, usluge i dobra materijalne informacijske tehnologije čiji bi kvar ili uništenje značajno utjecalo na zdravlje, sigurnost ili ekonomski prosperitet građana ili na učinkovito djelovanje vlada država članica [7].

Definiranje pojma kritične infrastrukture u SAD-u: Kritična infrastruktura je pojam koji se odnosi na širok opseg različitih sredstva i imovine koji su neophodni za svakodnevno funkcioniranje društvenih, ekonomskih, političkih i kulturnih sustava u SAD-u Bilo kakav prekid u elementima kritične infrastrukture predstavlja ozbiljnu prijetnju za pravilno funkcioniranje ovih sustava i može dovesti do oštećenja imovine, ljudskih žrtava i značajnih ekonomskih gubitaka [8].

Definiranje pojma kritične infrastrukture u Australiji: Kritična infrastruktura predstavlja fizičke objekte, opskrbne lance, informacijske tehnologije i komunikacijske mreže, koje bi mogle biti uništene ili onesposobljene na duže vrijeme, te značajno utjecati na društveno ili ekonomsko blagostanje nacije, ili bi utjecalo na sposobnost Australije da održi nacionalnu obranu i osigura nacionalnu sigurnost [9].

Važnost kritične infrastrukture također naglašava njezinu ranjivost na različite prijetnje i opasnosti, koje bi mogle značajno utjecati na njezin rad i otpornost. Stoga su države započele procese utvrđivanja sektora u kojima se može nalaziti kritična infrastruktura. Kriteriji za određivanje što jest, a što nije kritična infrastruktura, međusobne ovisnosti, potencijalni negativni učinci ovisnosti jednog sektora o drugome , analiza rizika i ranjivosti, sve to ulazi u selekciju za utvrđivanje sektora kritične infrastrukture.

U prosincu 2013. Ministarstvo domovinske sigurnosti SAD-a objavilo je ažurirani nacionalni infrastrukturni plan zaštite. Na primjeru Sjedinjenih Američkih Država postoji 16 kritičnih infrastrukturnih sektora čija su imovina, sustavi i mreže, bilo fizičke ili virtualne, smatrane toliko vitalnima za SAD da bi njihovo onesposobljavanje ili uništenje imalo devastirajući učinak na sigurnost, nacionalnu gospodarsku sigurnost, nacionalno javno zdravlje ili sigurnost, ili bilo koju kombinaciju njih [10].

2.2.1 Kemijski sektor

Kemijski sektor SAD-a pretvara više od 70.000 različitih proizvoda bitnih za moderni život te distribuira te proizvode do više od 750.000 krajnjih korisnika diljem zemlje. Nekoliko stotina tisuća kemijskih postrojenja u SAD-u koriste, proizvode, skladište, transportiraju ili isporučuju kemikalije putem složenog lanca opskrbe. Opasne tvari koriste se za različite svrhe, od korištenja za jednostavne operacije čišćenja do korištenja pri složenim kemijskim procesima. Mogu dolaziti u čvrstom, tekućem ili plinovitom obliku, mogu biti prirodni, proizvedeni kao jedna tvar ili smjesa te kao nusproizvod industrijskog procesa [10].

2.2.2 Sektor komercijalnih objekata

Sektor komercijalnih objekata uključuje raznolik niz mjesta koja privlače veliki broj ljudi na jednom mjestu (kupovina, posao, zabava ili smještaj). Objekti unutar sektora rade na principu otvorenog javnog pristupa, što znači da se javnost može slobodno kretati bez odvraćanja od vrlo vidljivih sigurnosnih barijera. Sektor komercijalnih objekata sastoji se od osam podsektora: zabava i mediji (npr. televizijski mediji), igre (npr. kockarnice), smještaj (npr. hoteli), događaji na otvorenom (npr. tematski i zabavni parkovi), javna okupljanja (npr. arene, stadioni, nekretnine (npr. poslovne i stambene zgrade), maloprodaja (npr. trgovački centri), sportske lige (npr. profesionalne sportske lige i savezi) [10].

2.2.3 Komunikacijski sektor

Komunikacijski sektor sastavni je dio gospodarstva SAD-a. Nalazi se u pozadini poslovanja svih poduzeća, organizacija za javnu sigurnost i vlade. Komunikacijski sektor se podrazumijeva kao kritičan jer pruža "funkciju omogućavanja" svim sektorima kritične infrastrukture. Tijekom posljednjih 25 godina, sektor se razvio od pretežno pružatelja govornih usluga u raznoliku, konkurentnu i međusobno povezanu industriju koja koristi zemaljske, satelitske i bežične prijenosne sustave. Prijenos ovih usluga postao je međusobno povezan; satelitski, bežični i žični pružatelji usluga ovise jedni o drugima u prijenosu, a tvrtke rutinski dijele objekte i tehnologiju kako bi osigurale interoperabilnost. Privatni sektor, kao vlasnici i operateri većine komunikacijske infrastrukture, primarni je subjekt odgovoran za zaštitu infrastrukture i imovine sektora. Radeći sa saveznom vladom, privatni sektor može predvidjeti i odgovoriti na prekide rada u sektoru te razumjeti kako oni mogu utjecati na sposobnost nacionalnog vodstva da komunicira tijekom razdoblja krize [10].

2.2.4 Kritični proizvodni sektor

Kritični proizvodni sektor ključan je za ekonomski razvoj SAD-a. Izravan napad ili prekid određenih elemenata proizvodne industrije mogao bi poremetiti bitne funkcije na nacionalnoj razini ili na više kritičnih infrastrukturnih sektora. Kritični proizvodni sektor identificirao je

nekoliko industrija koje će služiti kao jezgra sektora. Proizvodnja primarnih metala, tvornice željeza i čelika i proizvodnja fero legura, glinica, proizvodnja i prerada aluminija, proizvodnja i prerada obojenih metala, proizvodnja strojeva, proizvodnja motora i turbina, proizvodnja opreme za prijenos snage ,zemljani radovi, proizvodnja rudarske, poljoprivredne i građevinske opreme, proizvodnja električne opreme, uređaja i komponenti, itd. Proizvodi koje proizvode ove proizvodne industrije ključni su za mnoge druge kritične infrastrukturne sektore [10].

2.2.5 Sektor brana

Sektor brana pruža kritične usluge zadržavanja i kontrole vode u SAD-u, uključujući proizvodnju hidroelektrične energije, opskrbu komunalnom i industrijskom vodom, poljoprivredno navodnjavanje, kontrolu sedimenta i poplava, riječnu plovidbu za prijevoz rasutog tereta unutarnjim vodama, upravljanje industrijskim otpadom i rekreaciju. Sektor brana ima ovisnosti s mnogim drugim sektorima uključujući komunikacijski sektor koji omogućuju daljinsko upravljanje i kontrolu sektora brana dok energetski sektor osigurava kritične izvore električne energije i mogućnost pokretanja sustava. Sektor brana osigurava vodu za navodnjavanje i štiti poljoprivredno zemljište od poplava sektoru hrane i poljoprivrede [10].

2.2.6 Bazni sektor obrambene industrije

Sektor obrambene industrijske baze svjetski je industrijski kompleks koji omogućuje istraživanje i razvoj, kao i dizajn, proizvodnju, isporuku i održavanje vojnih sustava naoružanja, podsustava i komponenti ili dijelova, kako bi se ispunili zahtjevi američke vojske. Sektor pruža proizvode i usluge koji su ključni za mobilizaciju, raspoređivanje i održavanje vojnih operacija [10].

2.2.7 Sektor hitnih službi

Sektor hitnih službi sastoji se od velikog broja obučenog osoblja, te zajedno s fizičkim i kibernetičkim resursima, pruža širok raspon usluga prevencije, pripravnosti, odgovora i oporavka tijekom svakodnevnih operacija i odgovora na incidente. Ovaj sektor uključuje geografski raspoređene objekte i opremu u plaćenim i volonterskim kapacitetima, organiziranim prvenstveno na saveznoj, državnoj, lokalnoj, plemenskoj i teritorijalnoj razini vlasti, kao što su hitne službe, gradske policijske uprave i vatrogasne postaje, uredi okružnog šerifa te Ministarstvo obrane. Misija sektora hitnih službi je spašavanje života, zaštita imovine i okoliša, pomoć zajednicama pogođenim katastrofama i pomoć u oporavku tijekom hitnih situacija [10].

2.2.8 Energetski sektor

Energetska infrastruktura SAD-a pokreće gospodarstvo 21. stoljeća. Bez stabilne opskrbe energijom zdravlje i dobrobit su ugroženi, a gospodarstvo SAD-a ne može funkcionirati. Energetski sektor je jedinstveno kritičan jer pruža "funkciju omogućavanja" u svim sektorima kritične infrastrukture. Ljudska svakodnevnica ovisi o dostupnosti i cijeni energije (putovanja, hrana, mjesto boravišta, mjesto rada). Pristupačna energija čini ljudske živote boljima i jednostavnijima. Energetski sektor je itekako svjestan svoje ranjivosti te sa suradnjom kroz industrijske grupe radi na razmjeni informacija o najboljim praksama u cijelom sektoru [10].

2.2.9 Financijski sektor

Financijski sektor predstavlja jednu od vodećih meta kibernetičkih napada. Banke su mjesto gdje je novac, a kibernetičkim kriminalcima napad na banke nudi više načina za profit kroz iznudu, krađu i prijevaru. Zbog toga financijski sektor predstavlja vitalnu komponentu kritične infrastrukture SAD-a. Sektor financijskih usluga uključuje tisuće depozitnih institucija, pružatelja investicijskih proizvoda, osiguravajućih društava, drugih kreditnih i financijskih organizacija te pružatelja kritičnih financijskih uslužnih programa. Omogućuju korisnicima polaganje sredstva i izvršavanje plaćanja drugim stranama, osiguravanje kredita i likvidnosti kupcima, ulaganje sredstva na duga i kratka razdoblja te prijenos financijskih rizika između kupaca [10].

2.2.10 Sektor hrane i poljoprivrede

Sektor hrane i poljoprivrede smatra se kritičnom infrastrukturom jer je neophodan za proizvodnju, preradu i distribuciju hrane. Poremećaj u sektoru hrane i poljoprivrede mogao bi imati značajan utjecaj na gospodarstvo i javno zdravlje. cijelog društva Sektor hrane i poljoprivrede ima kritične ovisnosti o mnogim sektorima, ali posebno o sljedećim [10]:

- sektor za vodu: za čistu vodu i za navodnjavanje i prerađenu vodu
- transportni sektor: za kretanje proizvoda i stoke
- energetski sektor: kao napajanje za poljoprivrednu proizvodnju i preradu hrane
- kemijski sektor: u kontekstu gnojiva i pesticida koji se koriste u proizvodnji usjeva.

2.2.11 Sektor državnih ustanova

Sektor državnih ustanova uključuje objekte, na teritoriju SAD-a, koji su u vlasništvu ili u najmu saveznih, državnih, lokalnih i plemenskih vlasti. Velik broj državnih objekata otvoreni su javnosti za poslovne aktivnosti, komercijalne transakcije ili rekreacijske aktivnosti, dok drugi koji nisu otvoreni za javnost sadrže vrlo osjetljive informacije, materijale, procese i opremu. Ti objekti uključuju uredske zgrade opće namjene i vojne instalacije posebne namjene, veleposlanstva, sudnice, nacionalne laboratorije i strukture u kojima se može nalaziti kritična oprema, sustavi, mreže i funkcije. Osim fizičkih struktura, sektor uključuje kibernetičke elemente koji pridonose zaštiti imovine sektora (npr. sustavi kontrole pristupa i televizijski sustavi zatvorenog kruga), kao i pojedince koji obavljaju bitne funkcije ili posjeduju taktičko, operativno ili strateško znanje [10].

2.2.12 Sektor za zdravstvo i javno zdravstvo

Sektor zdravstva i javnog zdravstva štiti sve sektore gospodarstva od opasnosti poput bio-terorizma, izbijanja zaraznih bolesti i prirodnih katastrofa. Budući da je velika većina imovine sektora u privatnom vlasništvu i pod upravom nje, suradnja i razmjena informacija između javnog i privatnog sektora ključna je za povećanje otpornosti nacionalnog zdravstva i kritične infrastrukture javnog zdravstva. Sektor zdravstva i javnog zdravstva uvelike ovisi o drugim sektorima u pogledu kontinuiteta rada i pružanja usluga, uključujući sektore komunikacija, hitne službe, hrane i poljoprivrede te transportne i energetske sektore [10].

2.2.13 IT sektor

Sektor informacijske tehnologije ključan je za nacionalnu sigurnost, gospodarstvo te javno zdravlje i sigurnost budući da poduzeća, vlade, akademska zajednica i građani sve više ovise o funkcijama sektora informacijske tehnologije. Ovi proizvodi i usluge sastavni su dio usluge koje pružaju ostali sektori kritične infrastrukture. Dok IT sektor povećava učinkovitost, djelotvornost i otpornost ostalih sektora, on se svakodnevno suočava s brojnim višestranim globalnim prijetnjama od prirodnih i umjetnih događaja [10].

2.2.14 Nuklearni reaktori, materijali i sektor otpada

Od energetskih reaktora koji opskrbljuju električnu energiju milijunima ljudi do medicinskih izotopa koji se koriste za liječenje pacijenata oboljelih od raka. SAD ima opsežnu civilnu nuklearnu infrastrukturu s čak više od 3 milijuna isporuka radioaktivnih materijala godišnje. Stoga se posebne sigurnosne mjere poduzimaju kada se radioaktivni materijali otpremaju kako bi se osigurala sigurnost prijevoznika i spriječila krađa ili sabotaža samog radioaktivnog materijala. Sektor je međuovisan s drugim sektorima kritične infrastrukture, na primjer sektor hitnih službi je obučen za djelovanje ukoliko dođe do nezgode s nuklearnim materijalima. Energetski sektor nuklearna postrojenja opskrbljuju električnom energijom i uvelike ovise o neprekinutom opskrbi električnom energijom za kontinuirani siguran rad [10].

2.2.15 Transportni sektor

Premještajući milijune ljudi i robe diljem zemlje svaki dan, sektor transportnih sustava se svakodnevno suočava s velikim brojem prijetnji i rizika. Sigurnost predstavlja primarnu važnost za svaki transportni sustav jer velik broj ljudi ovisi o njemu [10].

2.2.16 Vodovodni i kanalizacijski sustavi

Zdrava pitka voda preduvjet je zaštite javnog zdravlja i svih ljudskih aktivnosti. Stoga je osiguranje opskrbe pitkom vodom i pročišćavanje otpadnih voda ključno za suvremeni život i nacionalno gospodarstvo. Sektor vodoopskrbe i sustava odvodnje ranjiv je na razne napade, uključujući kontaminaciju smrtonosnim agensima kao što je ispuštanje otrovnih plinovitih kemikalija te kibernetičke napade. Rezultat bilo koje vrste napada mogao bi biti velik broj bolesti ili žrtava ili bi rezultat napada mogao biti uskraćivanje usluge što bi također utjecalo na javno zdravlje i ekonomsku vitalnost. Kritične usluge, kao što su vatrogastvo i zdravstvena skrb (bolnice), te drugi ovisni i međuovisni sektori, kao što su energetika, hrana, poljoprivreda te transportni sustavi, pretrpjeli bi negativne učinke uskraćivanjem pitke vode [10].

2.3 Kritična infrastruktura RH

Republika Hrvatska integrirala je niz zakonodavnih i regulatornih mjera za zaštitu svoje kritične infrastrukture. Mjere služe za identifikaciju, procjenu i ublažavanje rizika za kritične infrastrukture od prirodnih katastrofa, tehnoloških nesreća i namjernih napada. Hrvatska vlada je odredila 11 sektora kritične infrastrukture [11]:

- Energija
- Komunikacije i informacijska tehnologija
- Transport
- Zdravstvo
- Vodno gospodarstvo
- Hrana
- Financije
- Proizvodnja, skladištenje i prijevoz opasnih tvari
- Javni sektor
- Nacionalni spomenici i vrijedni predmeti
- Znanost i obrazovanje.

Zemljopisni položaj Hrvatske i izloženost raznim opasnostima, kako prirodnim (poplave, potresi) tako i onima izazvanim čovjekom, naglašavaju važnost očuvanja kritične infrastrukture. Osim toga ograničeni resursi zemlje čine je posebno osjetljivom na prijetnje, budući da možda nije u potpunosti opremljena za razvoj alternativnih ili redundantnih sustava. Također s obzirom da je Republika Hrvatska članica NATO-a i Europske unije, nužno je koordiniranje rada s drugim zemljama.

Zbog svih navedenih izazova razvijen je niz planova i programa za zaštitu kritičnih infrastruktura, uključujući:

- Nacionalni plan zaštite i spašavanja
- Nacionalna strategija za sprječavanje i suzbijanje terorizma
- Nacionalna strategija kibersigurnosti.

Ovi planovi i programi dizajnirani su kako bi osigurali da Hrvatska ima potrebne sposobnosti za sprječavanje, odgovor i oporavak od incidenata koji ugrožavaju sustave kritične infrastrukture. Stoga je nužno nastaviti ulagati napore za zaštitu kritične infrastrukture kako bi se ublažili rizici od potencijalnih prijetnji [12].

3. SIGURNOSNI IZAZOVI KOMUNIKACIJE U KRITIČNOJ INFRASTRUKTURI

Eksponencijalan tehnološki razvoj u gotovo svim sektorima doveo je do pojave sve složenijih sustava koji mogu biti meta potencijalnih napada, zbog toga briga o sigurnosti kritične infrastrukture postaje sve važnija. Međutim, ovisnost o složenim tehnološkim sustavima i velik napredak u kibernetičkim sposobnostima pojedinaca donose velik broja sigurnosnih izazova koji je potrebno riješiti kako bi kritična infrastruktura bila što sigurnija. Također velik spektar potencijalnih kibernetičkih napada i stalna prisutnost rizika od fizičkih upada, zahtijeva dobro razumijevanje prijetnji u nastajanju, snažne zaštitne mjere te zajednički napor državnog i privatnog sektora.

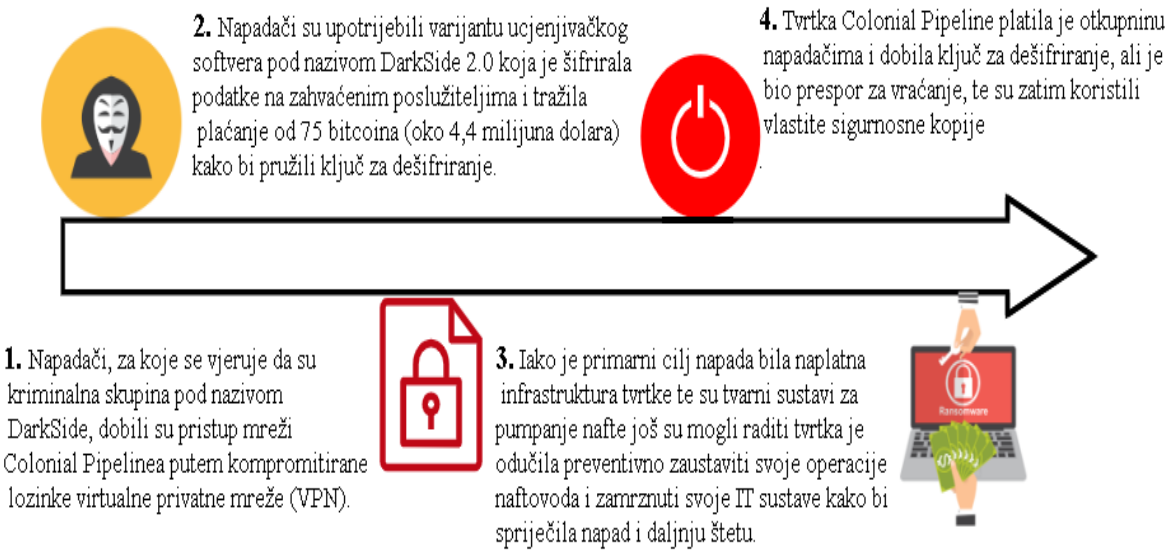
3.1 Pregled vrsta kibernetičkih prijetnji

Zadnjih nekoliko godina napadi na kritičnu infrastrukturu postali su sve češći i napredniji. Kritična infrastruktura je sve više povezana i međusobno ovisna, a ta povezanost donosi veći rizik potencijalne štete. Naime to znači da sabotiranje jednog kritičnog infrastrukturnog sustava može imati domino efekt na druge kritično infrastrukturne sustave. U sljedećim pod poglavljima bit će navedene vrste prijetnje koje mogu oštetiti komunikacije u kritičnoj infrastrukturi [13].

3.1.1 Prijetnje uzrokovane ljudskim djelovanjem

Ovo može uključivati kibernetičke napade, neovlašteno mijenjanje proizvoda, eksploziju i bombaške napade. U ovom poglavlju bit će opisani kibernetički napadi budući da je to tematika završnog rada. Kibernetički napadi postaju sve učestaliji i napredniji osim za pojedince tako i za poduzeća, lokalne i državne vlasti, kao i kritičnu infrastrukturu. S porastom svijesti o kibernetičkoj kriminalu, organizacije ulažu više sve više resursa u kibernetičku sigurnost jer ulaganja u sigurnost su i dalje puno manja od potencijalne štete. Šteta uzrokovana kibernetičkim napadima može se očitovati oštećenjem i uništenjem podataka, financijskim gubitcima, krađom intelektualnog vlasništva, krađom osobnih i financijskih podataka, troškovima istrage, te reputacijskom štetom. Neki od najpoznatijih vrsta kibernetičkih napada koji mogu biti štetni po kritičnu komunikaciju su: napadi zlonamjernim softverom (eng. *Malware*), *Phising* napadi, *Man in The Middle* (MITM) napadi, te napadi umetanjem *SQL*(eng. *Structured Query Language*) koda (eng. *SQL injection*).

Malware je jedan je od najčešćih kibernetičkih napada. Zlonamjerni softver je najčešće tajno ubačen u sustav s ciljem ometanja ili počinjenja određene štete u vidu oštećenja programa i podataka koji se nalaze na sustavu, širenje na druga računala i krađom podataka. U zlonamjerni softver spadaju: virusi, crvi, trojanski virusi, špijunski programi, oglašivački programi, ucjenjivački softver [14]. Napadi zlonamjernim softverom na kritičnu komunikaciju uključuju uvođenje zlonamjernog softvera u komunikacijske sustave, što dovodi do neovlaštenog pristupa, krađe podataka ili poremećaja sustava. Zlonamjerni softver na taj način može ugroziti kritične komunikacijske sustave i poremetiti rad sustava koji zahtijevaju hitne reakcije. Poznati primjer zlonamjernog softvera poznat kao ucjenjivački softver je *ransomware*. *Ransomware* je *malware* koja šifrira datoteke žrtve, čineći ih nedostupnima, te zatim zahtijeva otkupninu, obično u obliku kriptovaluta, u zamjenu za pružanje ključa za dešifriranje kako bi se datoteke otključale.

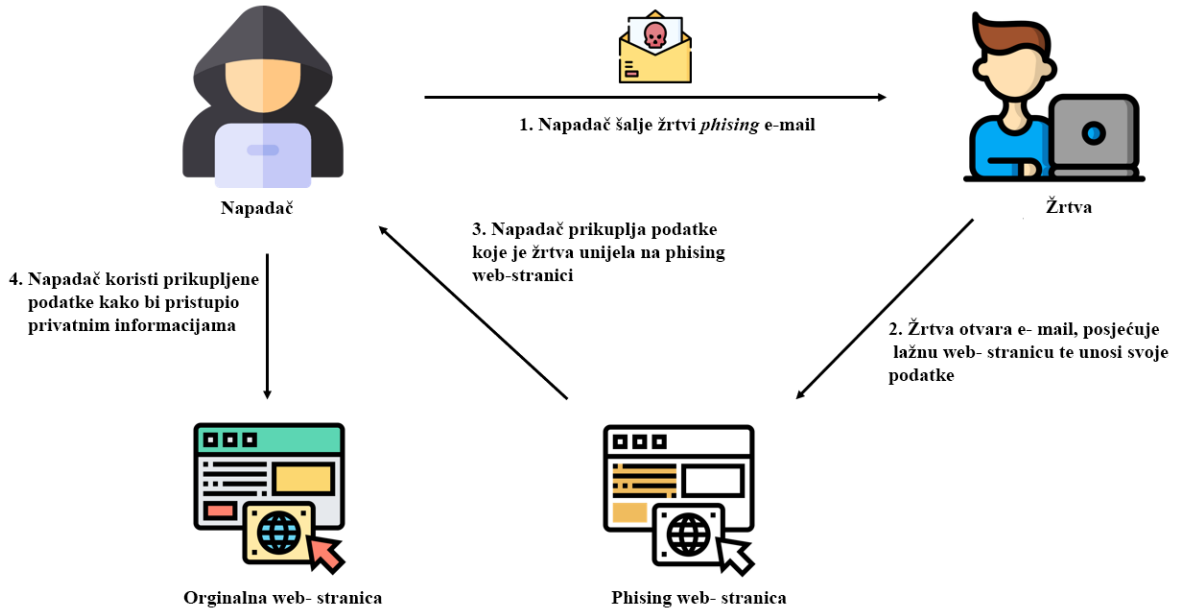


Slika 2. Odvijanje napada na naftovod Colonial Pipeline

Za jedan od najvećih *ransomware* napada a ujedno i jedan od najvećih kibernetičkih napada na kritičnu infrastrukturu smatra se napad na naftovod Colonial Pipeline. Colonial Pipeline je američki naftovod koji se proteže od Meksičkog zaljeva do istočne obale SAD-a, s gotovo 9000 kilometara cijevi. Od vitalne je važnosti jer zadovoljava potrebe za gorivom velikog dijela države te se zbog toga opravdano svrstava u kritičnu infrastrukturu. Napad započinje 6. svibnja 2021. kada hakerska grupa poznata pod nazivom DarkSide upada u sustav i vrši inicijalnu krađu podataka. DarkSide grupa je unutar dva sata ukrala više od 100 gigabajta povjerljivih podataka. Sljedeći dan napadači dobivaju kontrolu nad funkcijama sustava kao što su sustavi naplate, te u tom trenutku Colonial Pipeline postaje svjestan napada. Iako su stvarni sustavi za pumpanje nafte još su mogli raditi Colonial Pipeline je izvijestio da je zatvorio naftovod iz predostrožnosti zbog zabrinutosti da su hakeri mogli doći do informacija koje bi im omogućile izvođenje daljnjih napada na ranjive dijelove naftovoda. Napadači su zatim zatražili plaćanje otkupnine u iznosu od 75 bitcoina (4,4 milijuna dolara) za pristup alatu za dešifriranje ili će u protivnom ukradene podatke objaviti javno. Nekoliko sati kasnije tvrtka je platila otkupninu od gotovo 75 bitcoina (4,4 milijuna USD) u zamjenu za alat za dešifriranje, koji se

pokazao toliko sporim da su sigurnosne kopije tvrtke bile učinkovitije u vraćanju podataka. Na slici 2 nalazi se prikaz odvijanja napada na Colonial Pipeline. Temeljitim uviđajem utvrđeno je da su kriminalci pristup sustavu dobili lozinkom koja je dio serije procurjelih lozinki pronađenih na *dark webu*. Također prijava u sustav je imala autentifikaciju samo s jednim faktorom. Posljedice koje je opisani incident ostavio su značajne toliko da ga je američki predsjednik proglasio izvanrednim stanjem. Tijekom nedostupnosti usluga naftovoda došlo je do nedostatka zrakoplovnog goriva što je rezultiralo otkazivanjem mnogih letova u istočnom dijelu SAD-a. Također informacija o zatvaranju naftovoda prouzročila je paniku te uzrokovala ogromne gužve i na benzinskim crpkama. Panično kupovanje goriva postalo je toliko intenzivno da je ubrzo dovelo do znatnog poskupljenja cijena goriva na tom dijelu tržišta [15].

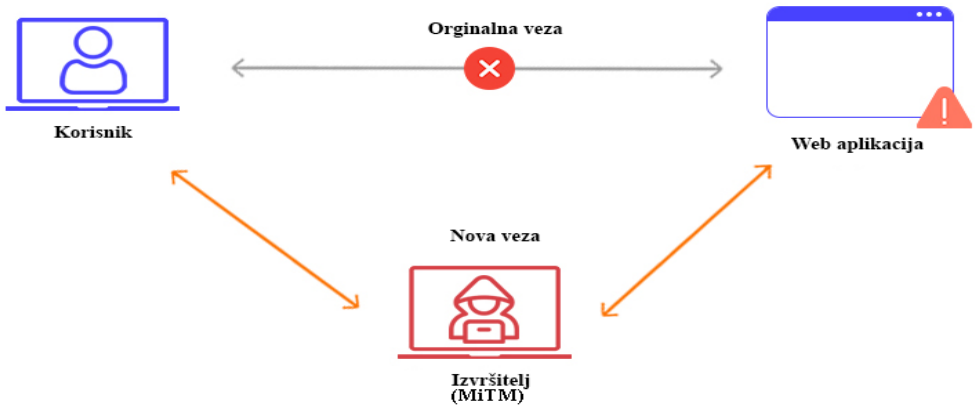
Phishing napadi predstavljaju napade u kojima se šalje lažna e-pošta, tekstualne poruke, telefonski pozivi ili web-mjesta osmišljena kako bi prevarila korisnike da preuzmu zlonamjerni softver, dijele osjetljive informacije ili osobne podatke (npr. brojeve kreditne kartice, brojeve bankovnih računa). Na slici 3 nalazi se ilustrativni prikaz odvijanja *phising* napada. U kritičnoj komunikaciji, ugroženi autentifikacijski podatci mogu dovesti do neovlaštenog pristupa komunikacijskim sustavima, omogućujući napadačima da manipuliraju informacijama ili ometaju komunikacijske kanale. Kao primjer napada u kojem je kritična infrastruktura ugrožena *phising* napadom navodi se napad na električnu mrežu Ukrajine. Napad je započeo 2015.godine kada je zaposlenik otvorio excel privitak e-pošte koji je pokrenuo zlonamjerni softver BlackEnergy. Ovaj napad će detaljnije biti opisan u nastavku rada u poglavlju pod nazivom 'Napad na električnu mrežu Ukrajine'. Mjere za sprječavanje ili smanjenje utjecaja phishing napada uključuju edukaciju korisnika, podizanje javne svijesti i tehničke sigurnosne mjere [16].



Slika 3. *Phising* napad

Izvor: [17]

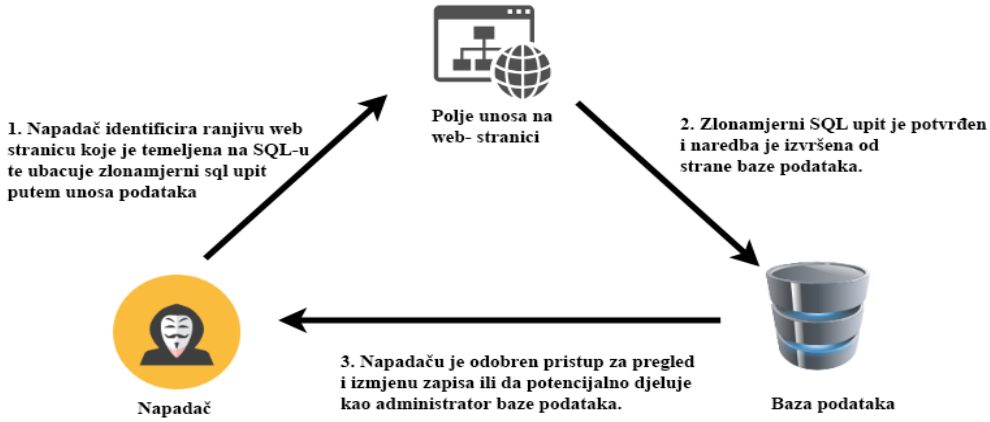
Man in the middle je vrsta napada u kojem se napadač infiltrira između pošiljatelja i primatelja te ima cilj presresti, ukrasti, modificirati podatke ili prekinuti komunikaciju i poslati zlonamjerne podatke bilo kojoj strani. Sprječavanje MITM napada najčešće se rješava nekom vrstom provjere autentičnosti na krajevima komunikacije stoga većina sigurnosnih protokola posjeduje istu. SSL (eng. *Secure Sockets Layer*) protokol koristi se upravo kako bi obje strane komunikacije mogle provjeriti autentičnost tako da obje strane budu provjerene od pouzdane treće koja ih ovjeri certifikatom [18]. MITM napadi uključuju presretanje komunikacije između dvije strane kako bi se prisluškivale, modificirale ili ubacile lažne informacije. U kritičnoj komunikaciji, MITM napadi može dovesti do širenja pogrešnih informacija drugoj strani te time ugroziti povjerljivost i integritet osjetljivih podataka. Na slici 4. nalazi se sažeti prikaz odvijanja *Man in the middle* napada.



Slika 4. MITM napad

Izvor: [19]

Napad umetanjem *SQL* koda je vrsta napada u kojoj napadač ubacuje zlonamjerni *SQL* kod u upit, koji zatim izvršava baza podataka. Ova ranjivost nastaje kada aplikacija ne uspije pravilno provjeriti valjanost i očistiti korisničke unose prije nego što ih upotrijebi u *SQL* upitima. Glavna ideja iza *SQL* ubacivanja je manipulirati strukturom *SQL* upita na način koji napadaču omogućuje izvršavanje neovlaštenih radnji ili dohvaćanje osjetljivih informacija iz baze podataka [18]. Na slici 5 nalazi se prikaz *SQL injection* napada. U sektorima kritične infrastrukture, ova povreda povjerljivih podataka može dovesti do krađe identiteta, špijunaže ili financijskih gubitaka. Također velika šteta se može dogoditi u slučaju prekida usluge. Naprimjer, u energetskom sektoru napad na bazu podataka koja kontrolira sustave distribucije električne energije mogao bi dovesti do nestanka struje ili utjecati na opskrbu električnom energijom.



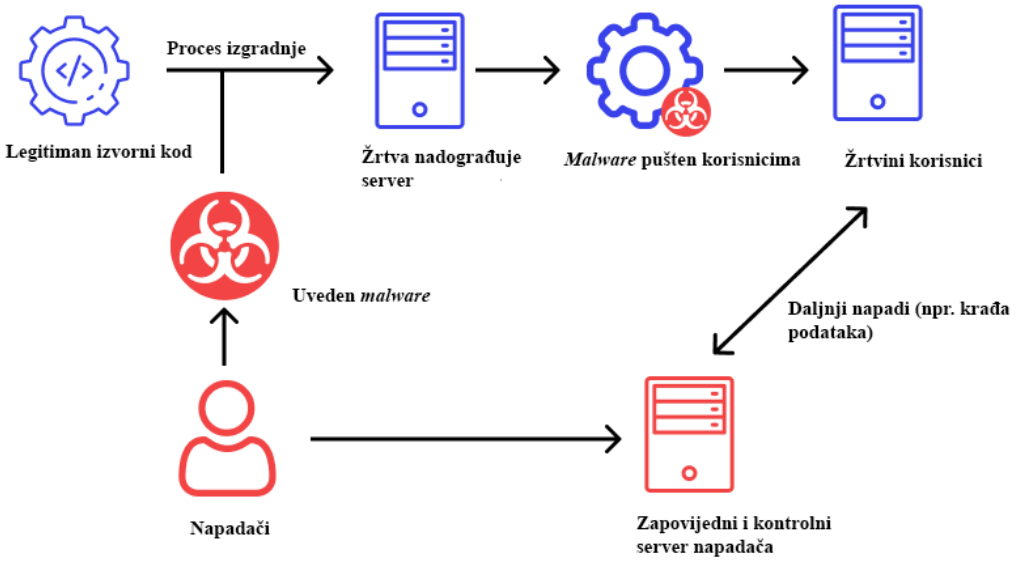
Slika 5. Napad umetanjem *SQL* koda

Izvor: [20]

Najčešći primjeri *SQL* napada javljaju se u financijskom sektoru koji spada pod kritičnu infrastrukturu a konkretni primjer je napad na Heartland Payment Systems pružatelja usluge obrade plaćanja. Napadači su prvotno dobili pristup mreži koristeći *SQL injection*, gdje su napadači iskoristili ranjivost u softveru tvrtke da ubace zlonamjerni *SQL* kod u sustav. Jednom unutar mreže, napadači su instalirali program za prisluškivanje koji je bio dizajniran da hvata i prikuplja osjetljive podatke o vlasnicima kartica dok su prolazili kroz mrežu. Ti podaci uključivali su brojeve kreditnih i debitnih kartica, datume isteka i kodove za provjeru kartica. Krađu su otkrile tvrtke za plaćanje karticama, koje su primijetile neobičan uzorak prijevarnih transakcija koje potječu od kartica obrađenih od strane Heartlanda. Utvrđeno je da je krađa izložila podatke s desetaka milijuna kreditnih i debitnih kartica. Ukradeni podaci prikupljani su nekoliko mjeseci prije nego što su otkriveni, a krađa je imala dalekosežne posljedice. Osim financijskih gubitaka koje su pretrpjeli pogođeni pojedinci i financijske institucije, Heartland se suočio s brojnim tužbama, regulatornim kaznama i štetom po ugledu [21].

Ovo su samo neki primjeri brojnih kibernetičkih prijetnji s kojima se suočavaju pojedinci i organizacije a kao primjer za jedan od najvećih kibernetičkih napada u povijesti navodi se napad na SolarWinds koji se dogodio 2020. godine. SolarWinds je američka tvrtka koja razvija softver za tvrtke koji im pomaže u upravljanju njihovim mrežama, sustavima i infrastrukturom. SolarWinds bio je idealna meta hakera s obzirom da njihove alate koristi velik broj visoko profiliranih tvrtki i organizacija, uključujući sve ogranke američke vojske, agenciju središnje američke savezne vlade i velik broj američkih *Fortune* 500 tvrtki. Takve organizacije visokog profila popularne su mete hakerskih skupina. Najprije je tvrtka za kibernetičku sigurnost FireEye objavila je da je žrtva sofisticiranog hakerskog napada, a već nekoliko dana kasnije pokazalo se da FireEye nije jedina žrtva, nego i tisuće drugih organizacija koje su također bile ugrožene. Napad je izveden na način da je skupina hakera zlonamjerni kod implementirala na SolarWinds-ovom alatu za upravljanje mrežom poznat kao Orion. A SolarWinds ne znajući da je zlonamjerni kod implementiran na Orion, počeo je slati ažuriranja softvera za Orion koji je u sebi imao zlonamjerni kod. Sve je izvedeno u tajnosti, a način na koji je proveden se zove napad lanca opskrbe (eng. *Supply chain attack*) [22].

Napad na lanac opskrbe je kibernetički napad koji nastoji oštetiti organizaciju ciljajući manje sigurne elemente u lancu opskrbe. Može se dogoditi u softveru ili hardveru. Kibernetički kriminalci obično ciljaju proizvodnju ili distribuciju proizvoda instaliranjem zlonamjernog softvera ili komponenti za špijuniranje temeljenih na hardveru. Na slici 6 nalaze se koraci odvijanja napada na lanac opskrbe [23].



Slika 6. Napad na lanac opskrbe

Izvor: [24]

3.1.2 Prirodne prijetnje

Prirodne prijetnje imaju mogućnost ometati, oštetiti ili čak uništiti sustave kritične infrastrukture što dovodi do značajnih štetnih učinaka na cijelo stanje jedne nacije. Odnos prirodnih katastrofa i zaštite kritične infrastrukture složen je i zahtijeva veliku pozornost stvaralaca zakona, operatera infrastrukture i agencija za upravljanje u hitnim slučajevima. Razumijevanje rizika i ranjivosti povezanih s različitim vrstama prirodnih katastrofa ključno je za razvoj učinkovitih strategija za očuvanje otpornosti kritične infrastrukture. Raznolik raspon prijetnji koji uključuje potrese, poplave, šumske požare, tornada, klizišta, a svaki od njih može imati potencijalne posljedice na ključne infrastrukturne sektore kao što su energija, transport, komunikacije i upravljanje vodom, itd. Posljedice se mogu pojaviti u obliku nestanka struje, prekida vodoopskrbe, prekida komunikacije, ugroženja opskrbnih lanaca, kao i ugroženih kapaciteta za hitne reakcije. Domino rezultat pojedinačne katastrofe može razviti ogromne posljedice na druge sektore [25]. U sljedećem primjeru navest će se prirodna katastrofa koja je imala veliki utjecaj na kritičnu infrastrukturu telekomunikacijskog sektora dvije nacije.

Potres koji se dogodio 6. veljače 2023. godine imao je značajan utjecaj na telekomunikacijski sektor Turske i Sirije. Nedugo nakon katastrofe komunikacijske usluge za milijune ljudi koji su trebali kontaktirati svoje obitelji, prijatelje ili vlasti bile su nedostupne. Mnogi ljudi su izvijestili da nisu mogli telefonirati, slati poruke ili pristupati internetu satima ili danima nakon potresa. Zbog urušavanja zgrada i problema sa izvorom energije, bazne stanice, koja su najekstremnija točka mreže bile su onemogućene zbog nedostatka radio pristupnih mreža. Neki od gubitaka veze nastali su i zbog oštećenja dalekovoda koji povezuje radio pristupnu mrežu s osnovnom mrežom. Također potres je otkrio slabosti telekomunikacijske infrastrukture u Turskoj, koja uvelike ovisi o mreži Türk Telekoma, državne tvrtke koja ima monopol nad fiksnim i širokopojasnim uslugama. Osim utjecaja na telekomunikacijski sektor Turske posljedice su utjecale i na susjednu zemlju Siriju, koja se oslanja na Tursku za svoju internetsku povezanost. Potres je prekinuo pristup internetu za većinu Sirije, koja je već patila od građanskog rata i humanitarne krize. Prekid interneta otežao je komunikaciju i koordinaciju humanitarnih radnika i aktivista civilnog društva u Siriji [26].

3.1.3 Slučajne ili tehničke prijetnje

Nazivaju se prijetnje koje nastaju zbog nenamjernih događaja ili kvarova povezanih s radom, održavanjem ili dizajnom infrastrukturnih sustava. Ti incidenti obično nisu uzrokovani namjernim ili zlonamjernim akcijama, već ljudskom pogreškom, kvarovima opreme, dizajnerskim greškama ili kvarovima sustava. Slučajno ili tehničke događaji mogu imati značajne posljedice za rad, funkcionalnost i sigurnost kritične infrastrukture. Neki od primjera slučajnih ili tehničkih prijetnji u kritičnoj infrastrukturi su kvarovi opreme, ljudske greške, dizajnerske greške i kvarovi softvera ili sustava.

Oprema koja se koristi u kritičnoj infrastrukturi, kao što su naprimjer generatori struje mogu doživjeti kvarove zbog mehaničkih, električnih ili softverskih kvarova. Posljedično ti kvarovi mogu dovesti do prekida usluga, nestanka struje i sigurnosnih rizika.

Pogreške koje su napravili operateri, osoblje za održavanje ili druge osobe uključene u rad i održavanje kritične infrastrukture mogu rezultirati slučajnim incidentima. Na primjer, nepravilno rukovanje opasnim materijalima ili operativne pogreške u elektranama mogu uzrokovati prekide ili nesreće.

Greška pri dizajniranju i izgradnji može dovesti do ranjivosti ili neočekivanih kvarova. Na primjer, strukturne slabosti u mostovima, nedovoljne mjere zaštite od požara u zgradama mogu pridonijeti nesrećama ili prekidima usluga.

Kritični infrastrukturni sustavi često se oslanjaju na složene softverske i računalne sustave. Tehnički problemi, softverski greške ili kibernetički incidenti mogu ugroziti funkcionalnost i sigurnost tih sustava, što dovodi do prekida usluga.

Rješavanje slučajnih ili tehničkih incidenata u kritičnoj infrastrukturi zahtijeva proaktivne mjere. To uključuje implementaciju robusnih postupaka održavanja, redovito provođenje inspekcije opreme, osiguravanje pravilnog osposobljavanja osoblja, korištenje redundantnih sustava, provođenje procjena rizika i kontinuirano praćenje i ažuriranja kritičnih infrastrukturnih sustava [27].

3.2 RANJIVOSTI U SUSTAVIMA KRITIČNE INFRASTRUKTURE

U današnjem povezanom svijetu, sustavi kritične infrastrukture osiguravaju normalan život, pružajući osnovne usluge i podržavajući gospodarski rast. Sustavi se oslanjanju na komunikacijske mreže kako bi se omogućile nesmetane operacije i osigurala učinkovita koordinacija. Međutim, uz brojne prednosti koje donose napredne komunikacijske tehnologije, sustavi kritične infrastrukture su suočeni s rastućim brojem ranjivosti koje predstavljaju značajne rizike za njihovu sigurnost, pouzdanost i otpornost. Kako tehnologija nastavlja napredovati velikom brzinom, konvergencija informacijske tehnologije *(Information technology*- IT) i operativne tehnologije (*Operational technology*- OT) postala je sve prisutnija. IT se odnosi na računalne i komunikacijske tehnologije koje se koriste za upravljanje i obradu informacija unutar tradicionalnih mreža, dok OT obuhvaća hardverske i softverske sustave odgovorne za kontrolu i nadzor fizičkih uređaja i procesa u operativnim okruženjima, kao što su industrijski kontrolni sustavi(*Industrial control system-ICS*).Integracija IT-a i OT-a revolucionirala je industriju povećanjem učinkovitosti, automatizacije i povezanosti. Međutim, također je uvela nove sigurnosne izazove osim za industrijske kontrolne sustave tako i za nove tehnologije, poput Interneta stvari (*Internet of Things*-IoT) i računarstva u oblaku (eng. *Cloud computing*). Razumijevanje i rješavanje ovih ranjivosti u kritičnim infrastrukturnim komunikacijskim sustavima od najveće je važnosti za zaštitu kritične infrastrukture.

3.2.1 Operativna tehnologija i njihova ranjivost

Operativnu tehnologiju predstavljaju ICS, računalni sustavi za nadzor, mjerenje i upravljanje industrijskim sustavima (*Supervisory control and data acquisition system*-SCADA), distribuirani upravljački sustavi (*Distributed control system*-DCS) i druge konfiguracije kao što su programibilni logički kontroleri (*Programmable logic controller*-PLC). Ovi se sustavi obično nalaze u sustavima kritične infrastrukture kao što su energija, voda i otpadne vode, nafta i plin, kemikalije, transport, proizvodnja hrane i diskretna proizvodnja. U početku su ICS bili analogni sustavi koji su radili izolirano od drugih sustava, dajući prednost sigurnosti, stabilnosti i pouzdanosti. Analogna priroda ovih sustava bila je prikladna za pružanje podataka i kontrolu. Međutim, s napretkom digitalnih tehnologija, moderni ICS su se razvili kako bi uključili digitalne elemente i povezanost, omogućujući poboljšane mogućnosti nadzora, kontrole i automatizacije. Ova digitalna transformacija donijela je nove izazove i ranjivosti koje zahtijevaju snažne sigurnosne mjere kako bi se osigurao integritet i otpornost kritičnih infrastrukturnih sustava. Nedostatak sigurnosti u ovim sustavima javlja se jer kontrolni sustavi rade na standardima, protokolima i softveru dizajniranim i implementiranim u vrijeme kada je površina napada bila mala, te zbog ograničene međusobne povezanosti uređaja i mreža. Upravo zbog svoje važnosti u kritičnoj infrastrukturi, industrijski upravljački sustavi postaju meta raznih napada. U tablici 1 nalazi se niz napada na kritičnu infrastrukturu koji su se dogodili u posljednjih 20 godina. Tablicom su opisani napadi te je navedena industrija u kojoj se napad dogodio kao i posljedice koje je prouzrokovao [28].

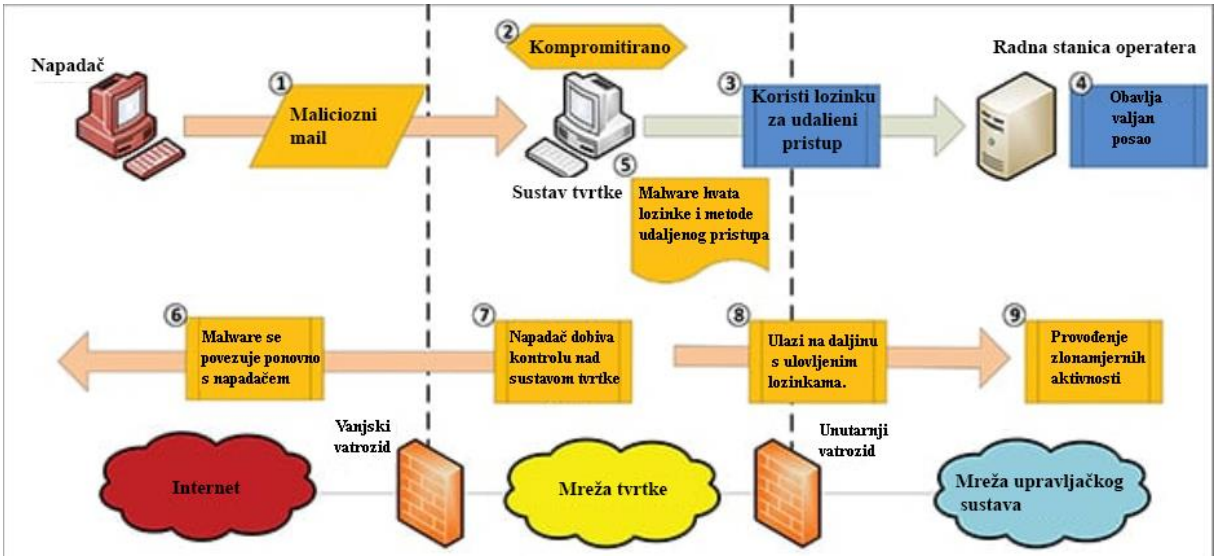
Tablica 1. Primjeri OT napada i posljedice koje je napad prouzročio u različitim industrijama

Napad	Industrija	Opis	Posljedice
Napad na električnu mrežu Ukrajine	Energija	Haker su dobili daljinski pristup te isključili struju na 30 trafostanica kroz instalaciju *firmware-a*.	Bez struje je ostalo 225.000 korisnika te je ugašen sustav telekomunikacija .Izbrisane su datoteke iz glavnog pokretačkog zapisa.
Napad na Njemačku čeličanu	Proizvodnja čelika	Hakeri su putem *phising* napada na osoblje dobili pristup mreži nakon čega su uspjeli reprogramirati PLC kontrolore te sabotirali funkciju peći.	Napad je uzrokovao fizičko oštećenje infrastrukture te gubitak kontrole nad infrastrukturom.
Napad na vodovod putem SCADA sustava	Voda	Daljinsko uništenje pumpe dobivanjem pristupa SCADA mreži. Pristup dobiven od korisničkih imena i lozinke koje je proizvođač održavao za korisnike.	Stalno paljenje i gašenje pumpe uzrokovalo je prekid rada same pumpe.
Stuxnet napad	Nuklearna postrojenja	Računalni crv dizajniran od strane SAD-a i izraelske obavještajne službe da onesposobe ključni dio iranskog nuklearnog programa.	Uništenje brojnih centrifuga u iranskom postrojenju za obogaćivanje urana izazvavši njihovo samozapaljivanje.

Izvor:[28]

3.2.1.1 Napad na električnu mrežu Ukrajine

2015. godine u Ukrajini dogodio se niz kibernetičkih napada koji je imao u cilju onesposobiti ukrajinsku elektroenergetsku mrežu. Napadi su započeli *phishing* napadima, u kojoj su se e-mailovi s malicioznim prilozima slali zaposlenicima ukrajinskih energetskih kompanija. Čim su se prilozi otvorili, *malware* bi zarazio računala i omogućio napadačima da dobiju pristup mrežama. Nakon što su napadači dobili pristup mrežama, koristili su razne metode za narušavanje elektroenergetske mreže poput slanja lažnih naredbi kontrolnim sustavima, što bi dovelo do gašenja ili nepravilnog rada sustava. *DDoS* (eng. *Denial-of-service attack*) napad web stranica i poslužitelja uzrokovao je otežani pristup kritičnim informacijama i sustavima. Na slici 7 nalazi se tijek odvijanja napada u koracima od 1 do 9. Napadi su prouzročili opsežne prekide, koji su utjecali na milijune ljudi u Ukrajini, u nekim slučajevima prekidi su trajali nekoliko sati i imali su značajan utjecaj na ekonomiju i javnu sigurnost. Ovaj kibernetički napad na energetsku infrastrukturu s korištenim znanjem i resursima ukazuje na razinu sofisticiranosti napada na kritičnu infrastrukturu. Kibernetički napadi na ukrajinsku elektroenergetsku mrežu bili su veliki alarm za svijet. Oni su pokazali ranjivost kritične infrastrukture na kibernetičke napade i potencijal takvih napada da uzrokuju opsežne poremećaje i štetu. Nakon napada, Ukrajina je poduzela korake za poboljšanje sigurnosti svoje elektroenergetske mreže [28].



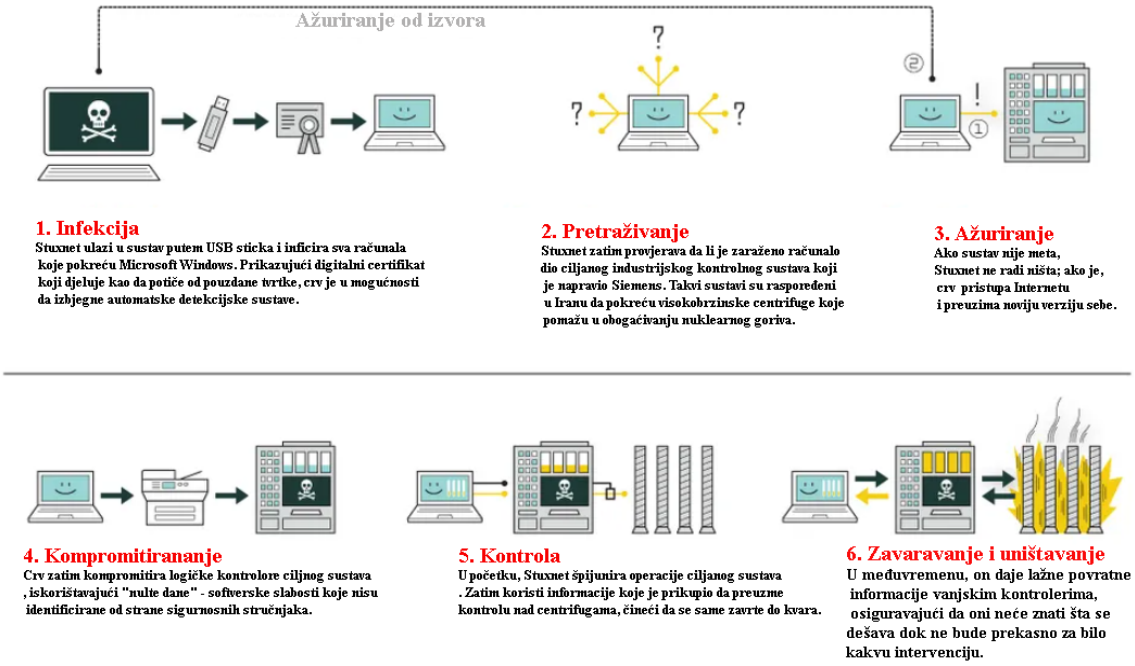
Slika 7. Tijek napada na elektroenergetsku mrežu Ukrajine

Izvor: [29]

3.2.1.2 Stuxnet napad

Stuxnet je zlonamjerni računalni crv koji je prvi put otkriven 2010.godine. Izrađen je s namjerom da bude kibernetičko ofenzivno oružje na način da onesposobi centrifuge za obogaćivanje urana te u konačnici Iranski nuklearni program. Iako nijedna država nije otvoreno priznala odgovornost, Stuxnet se smatra kibernetičkim oružjem koje su zajednički izradile SAD i Izrael u zajedničkoj operaciji poznatoj pod nazivom Olimpijske igre. Operacija je trajala nekoliko godina a odvijala se u nekoliko faza, Najprije je zlonamjerni kod ubačen u postrojenje na način da je putovao na memorijskom štapiću (eng. *Universal Serial Bus*) i širio se Microsoft Windows računalima. Virus je pretraživao svako zaraženo računalo tražeći znakove softvera

Siemens Step 7.Step 7 je softver, koji industrijska računala koja služe kao PLC-ovi, koriste za automatizaciju i nadzor elektro-mehaničke opreme. Nakon što je pronašao PLC računalo zlonamjerni softver ažurirao je svoj kod preko interneta i počeo slati upute koje uzrokuju štetu elektro-mehaničkoj opremi kojom je računalo upravljalo. U isto vrijeme, virus šalje lažne povratne informacije glavnom kontroleru. Svatko tko je promatrao opremu ne bi imao naznake problema sve dok se oprema ne bi počela samo uništavati. Na slici 8 nalazi se vizualni prikaz prethodno opisanog napada. Iako je operacija Olimpijske igre u konačnici završila vrlo uspješno, Stuxnet se uspio proširio internetom te na taj način došao do mogućnosti da može ugroziti mnoga industrijska postrojenja širom svijeta. U kibernetičkom svijetu Stuxnet je definitivno najsloženije i najopasnije digitalno oružje ikad izrađeno. Prije otkrivanja Stuxneta, zlonamjerni programi su se koristili u svrhu ostvarivanja nelegalne zarade, dolaska do povjerljivih informacija i slične manje opasnije operacije. Međutim operacija Olimpijske igre je otvorila skroz novo poglavlje u pogledu mogućih kibernetičkih napada na SCADA ili slične sustave [30].



Slika 8. Tijek Stuxnet napada

Izvor: [31]

Većina OT sustava radi odvojeno od IT sustava i infrastrukture, što se obično naziva "zračnim razmakom. Takav pristup pri dizajniranju ovakvih sustava doveo je do toga da su performanse stavljene u prvi plan dok da se o sigurnosnom aspektu nije razmišljalo. Ovakav stav uzrokovao je značajnu ranjivost tijekom razdoblja održavanja, gdje izvođači koriste multimedijske uređaje kao što su laptopi, prijenosni tvrdi diskovi i memorijski štapići kao pomoć za održavanje unutar industrijske infrastrukture. Napad Stuxnet bio je primjer zlonamjernog softvera koji je prenesen putem zaraženog memorijskog štapića, čime se virus mogao širiti.

Napad na Ukrajinsku elektroenergetsku mrežu i Stuxnet napad primjeri su u kojima je ljudska intervencija, bilo zlonamjerne namjere ili običnim neoprezom, pružila priliku kibernetičkim kriminalcima da iskoriste slabosti OT okruženja. Uzimajući u obzir širok raspon ranjivih protokola koji se koriste u OT-u te ogromni potencijal štete. potrebna su daljnja istraživanja kako bi se smanjio rizik od potencijalne štete.

3.2.2 Informacijska tehnologija i njihova ranjivost

Informacijska tehnologija, s druge strane, fokusira se na upravljanje, obradu i komunikaciju digitalnih informacija unutar organizacije. Osim toga obuhvaća područje pohrane podataka, umrežavanja, softverskih aplikacija, računalstva u oblaku koje podržavaju poslovne operacije, uključujući one povezane s kritičnom infrastrukturom. Dok se OT fokusira na kontrolu i automatizaciju fizičkih procesa u stvarnom vremenu, IT pruža potrebnu infrastrukturu i alate za upravljanje podacima, analizu, komunikaciju i sigurnost u kritičnim infrastrukturnim sustavima. IT sigurnost u informacijskoj tehnologiji često uključuje mjere poput vatrozida, enkripcije, kontrole pristupa i sigurnosnih revizija. Tijekom 2020. i 2021. godine odnosno tijekom trajanja globalne pandemije poduzeća su se morala prilagoditi situaciji isporuke digitalnih usluga. To razdoblje dovelo je do eksponencijalnog razvoja računarstva u oblaku [32].

Računarstvo u oblaku odnosi se na praksu korištenja mreže udaljenih poslužitelja, smještenih na internetu, za pohranu, upravljanje i obradu podataka. U računarstvu u oblaku riječ oblak koristi se kao metafora za "internet“ gdje se različite usluge kao što su poslužitelji, pohrana i aplikacije isporučuju na računala i uređaje organizacije putem interneta. Računarstvo u oblaku se smatra jednim od obećavajuća rješenja za potrebe za pristupom i korištenjem resursa osiguranih putem interneta. Može se podijeliti na tri razine ovisno o uslugama koje pružatelji nude [33]: Softver kao usluga (*Softver as a Service*-SaaS), Platforma kao usluga (*Platform as a Service*-PaaS) i Infrastruktura kao usluga (*Infrastructure as a Service*-IaaS).

SaaS je model usluge u kojem pružatelj upravlja svim slojevima sustava od hardvera do aplikacija, tako da sve što korisnik treba učiniti je prijaviti se i koristiti aplikaciju. Neki od najpoznatijih SaaS softvera uključuju Microsoft Office 365, Google Apps (npr. Gmail), Dropbox.

PaaS korisnicima pruža platformu za razvoj, pokretanje i upravljanje aplikacijama bez potrebe da brinu o temeljnoj infrastrukturi. U PaaS modelu, pružatelj usluga u oblaku nudi kompletno okruženje za razvoj i implementaciju, uključujući hardver, operativne sustave, programske jezike i okruženja za izvođenje. Primjeri PaaS pružatelja usluga uključuju AWS Elastic Beanstalk, Windows Azure, Google App Engine.

IaaS je model usluge pomoću kojeg računalne resurse opskrbljuje pružatelj usluga u oblaku. Glavna prednost IaaS-a je ta što korisnik ima puno slobode u načinu na koji želi koristiti infrastrukturu. Na primjer, mogu stvarati virtualne strojeve (*Virtual Machine*-VM) instalirati operativne sustave u VM, graditi baze podataka i stvarati spremnike za pohranu**.** Primjeri IaaS pružatelja usluga uključuju Amazon Web Services (AWS), Microsoft Azure.

Tablica 2. Sigurnosni zahtjevi i moguće prijetnje za svaku od razina usluga u računarstvu u oblaku

Razina usluge	**Sigurnosni zahtjevi**	**Moguće prijetnje**
SaaS	Kontrola pristupa Zaštita komunikacije Zaštita podataka od izlaganja Dostupnost usluge Sigurnost softvera Kontrola pristupa	Prekid podataka Izloženost u mreži Presretanje Promjena podataka Kršenje privatnosti Otmica sesije
PaaS	Kontrola pristupa Sigurnost aplikacije	Poplava veze DDoS napad
IaaS	Upravljanje oblakom Kontrola sigurnosti Komunikacija sigurnosti Sigurnost podataka Zaštitite slike	Ometanje komunikacije Izloženost u mreži Lažno predstavljanje Modifikacija softvera Prekid softvera Otmica sesije

Izvor: [33]

Kao što se vidi na tablici 2 IaaS, PaaS i SaaS zahtijevaju različite razine sigurnosnih mjera. Upravo iz razloga jer razine imaju različite odgovornosti ovisno o vrsti. Naprimjer u slučaju IaaS i PaaS usluge, korisnik je odgovoran za upravljanje i osiguravanje vlastite baze podataka, umjesto korištenja javne baze podataka, zbog čega se oni također nazivaju privatnim oblacima. Pod SaaS okruženjem, pružatelj usluga oblaka odgovoran je za osiguranje svih slojeva sustava.

Usluge u oblaku nude niz prednosti kao što su skalabilnost, visoka dostupnost i smanjeni troškovi održavanja. Sve ove značajke doveli su do prijelaza mnogih poduzeća, vladinih organizacija na upotrebu ove tehnologije. Međutim, uz sve ove obećavajuće značajke, još uvijek postoji niz tehničkih barijera koje ometaju korištenje clouda, poput sigurnosti i kvalitete usluge. Ranjivosti koje treba uzeti u obzir kada organizacija premješta svoje kritične aplikacije i podatke u cloud computing okruženje su: povreda podataka, uskraćivanje resursa, zlouporaba usluga u oblaku.

Povreda podataka je kršenje sigurnosti u kojem se osjetljivi, zaštićeni ili povjerljivi podaci kopiraju, prenose, pregledavaju, mijenjaju ili koriste od stane neovlaštenih osoba. Za primjer napada gdje su ukradeni podatci navodi se Hafnium napad na Microsoft Exchange server 2021. godine. Napadači su prvo dobili pristup ranjivim Exchange poslužiteljima iskorištavanjem ranjivosti *ProxyLogon*. Kad su ušli unutra, uspostavili su alat za daljinski pristup kako bi mogli trajno pristupiti kompromitiranom poslužitelju. To im je omogućilo krađu osjetljivih podataka, instaliranje dodatnog zlonamjernog softvera i daljnje provođenje zlonamjernih aktivnosti. Utjecaj napada bio je značajan i utjecao je na tisuće organizacija širom svijeta, uključujući vladine agencije, tvrtke i obrazovne ustanove [34].

DDoS napadi rade na principu da se ogromna količina prometa pošalje na mrežu ili poslužitelj kako bi se taj sustav preopteretio te u konačni onesposobio za pružanje tražene usluge. Cilj *DDoS* napada je iscrpiti resurse aplikacije. U 2018. platforma za razvoj softvera GitHub pretrpjela je masivni *DDoS* napad koji je dosegao brzinu od 1,3 Tbps, šaljući pakete brzinom od 126,9 milijuna u sekundi. Iako su bili spremni na takve napade, njihovi sustavi su bili preplavljeni ovim velikim prometom što je rezultirao prekidom usluge[34].

Zlouporaba usluga u oblaku odnosi se na činjenicu iskorištavanja usluga u oblaku za obavljanje neetičkih ili zlonamjernih aktivnosti korisnika oblaka u cilju stjecanja koristi ili financijske dobiti. Neki od primjera zloupotreba usluga u oblaku su [34]: *cryptojacking*, kampanje za neželjenu poštu, *hosting* ilegalnog sadržaja.

Cryptojacking je postupak u kojem napadači koriste resurse oblaka kako bi rudarili kripto valute bez znanja ili dopuštenja vlasnika. Oni iskorištavaju računalnu snagu i skalabilnost usluga u oblaku za rudarenje kripto valuta, potencijalno uzrokujući financijske gubitke legitimnom korisniku.

Kampanje za neželjenu poštu i krađu identiteta. Usluge u oblaku mogu se iskoristiti za slanje velikih količina neželjene e-pošte ili za *hostiranje* web stranica za krađu identiteta. Napadači mogu koristiti resurse oblaka za distribuciju zlonamjernih poruka e-pošte ili postavljanje lažnih web stranica kako bi prevarili korisnike da otkriju osjetljive informacije.

Hosting ilegalnog sadržaja. Usluge pohrane u oblaku mogu se zloupotrijebiti za *hostiranje* i distribuciju ilegalnog sadržaja, poput materijala zaštićenog autorskim pravima, piratskog softvera ili eksplicitnog materijala, čime se krše zakoni o intelektualnom vlasništvu ili pravila sadržaju.

Kao primjer za zloupotrebu usluga u oblaku navodi se incident koji se dogodio u Rusiji 2018. godine. Nekoliko znanstvenika koji rade u strogo tajnom ruskom nuklearnom postrojenju uhićeno je zbog rudarenja bitcoina (kriptovaluta) dok su bili na poslu. Znanstvenici su optuženi da su koristili jedno od najmoćnijih superračunala u zemlji za rudarenje kriptovaluta. Računala unutar nuklearnih postrojenja rijetko su povezana na internet kao preventivna mjera protiv kibernetičkih napada. Međutim, neposredno nakon pokušaja zloupotrebe superračunala, sigurnosni odjel nuklearnog centra je upozoren [35].

4. PREGLED TRENDOVA SIGURNOSTI KRITIČNE INFRASTRUKTURE

Brzo razvijanje i širenje novih tehnologija, zahtjeva od svih sudionika zaštite kritične infrastrukture da budu u toku s najnovijim trendovima. Širenje Internet stvari uređaja i usvajanje računarstva u oblaku predstavlja nove ranjivosti koje se moraju riješiti kako bi se učinkovito zaštitila mreža kritične infrastrukture. Nadalje sigurnost lanca opskrbe postala je ranjiva točka velikog broj sustava zbog velikog broj mogućih napada na svaku točku lanca opskrbe. Iako nove tehnologije poput umjetne inteligencije (*Artificial intelligence*- AI), strojnog učenja (eng. *Machine Learning*), 5G-a imaju veliku mogućnost poboljšanja sigurnosti kritične infrastrukture, postoji također velika mogućnost potencijalnog rizika od zloupotrebe tih tehnologija. Suradnja između javnih i privatnih entiteta postala je sve važnija za sigurnost kritične infrastrukture stoga vlade i privatne tvrtke dijele obavještajne podatke o prijetnjama i najboljim praksama zaštite kako bi ostali korak ispred napadača. U nastavku ovog poglavlja navesti će se važnost zaštite lanca opskrbe te rizike koje sabotaža lanca opskrbe donosi. Opisat će utjecaj novih tehnologija kao što je umjetna inteligencija na sigurnost kritične infrastrukture, naglašavajući prednosti i ranjivosti povezane s njihovom implementacijom [36].

4.1 Važnost zaštite lanca opskrbe

Napad u lancu opskrbe događa se kada se izvođač kibernetičkog napada infiltrira u mrežu dobavljača softvera i koristi zlonamjerni kod za kompromitiranje softvera prije nego što softver dođe do svojih korisnika. Ugroženi softver tada ugrožava podatke ili sustav korisnika. Novi softver može biti ugrožen od samog početka ili do ugrožavanja može drugim putem, naprimjer nadogradnjom ili popravkom. Opskrbni lanac softvera ima veliku ranjivost jer u njemu sudjeluje velik broj sudionika, od distributera i dobavljača u prodaji, do onih koji sudjeluju u isporuci i proizvodnji softvera. Na slici 9 nalazi se prikaz životnog ciklusa lanca opskrbe softvera koji se sastoji od 6 faza: dizajn, razvoj i proizvodnja, distribucija, raspoređivanje i nabava, održavanje i uništenje. A u svakoj fazi lanca opskrbe, softver je u riziku od zlonamjernog ili nenamjernog unošenja ranjivosti [37].

Slika 9. Faze životnog ciklusa lanca opskrbe softvera

Izvor: [37]

Najčešće tehnike za izvođenje napada na lanac opskrbe softvera su [37]:preuzimanje ažuriranja, potkopavanje potpisa koda, kompromitiranje otvorenog izvornog koda.

Preuzimanje ažuriranja odnosi se na redovita ažuriranja koja moderni softver dobiva kako bi se otklonile pogreške i sigurnosne propusti. Softverski pružatelji usluga obično distribuiraju ažuriranja sa centraliziranih poslužitelja kao rutinski dio održavanja proizvoda. Napadači mogu preuzeti ažuriranje infiltrirajući se u mrežu pružatelja usluga i umetnuti zlonamjerni kod u izlazno ažuriranje ili izmijeniti ažuriranje kako bi napadač dobio pristup nad normalnom funkcionalnošću softvera.

Potpisivanje koda koristi se za provjeru identiteta autora koda i integriteta koda. Napadači potkopavaju potpisivanje koda samo potpisujući certifikate, razbijajući sustave za potpisivanje ili iskorištavajući pogrešno konfigurirane kontrole pristupa računu. Potkopavanjem potpisivanja koda, hakeri mogu uspješno preuzeti softverska ažuriranja predstavljajući se kao pouzdan pružatelj usluga i umetnuti zlonamjerni kod u ažuriranje.

Sabotiranje otvorenog izvornog koda događaju se kada napadači umetnu zlonamjerni kod u javno dostupne biblioteke koda, koje neiskusni programeri, koji traže besplatne blokove koda za izvršavanje specifičnih funkcija, dodaju u svoj vlastiti kod treće strane. 2018. godine istraživači su otkrili 12 zlonamjernih Python biblioteka učitane na službenom Python Package Index (PyPI). Napadač je koristio taktike *typosquattinga* tako što je stvorio biblioteke pod nazivom "diango", "djago", "dajngo", itd., kako bi namamio programere koji traže popularnu Python biblioteku "django". Biblioteke su sadržavali su dodatnu funkcionalnost koja je omogućivala dobivanje udaljenog pristupa na korisničkoj strani.

4.2 Umjetna inteligencija u sigurnosti kritične infrastrukture

Napredak u analitici podataka, strojnom učenju i ostalim srodnim tehnologijama doveo je do velikog razvoja same umjetne inteligencije. Neki od najsloženijih sustava umjetne inteligencije koriste se upravo u sustavima kritične infrastrukture. Umjetna inteligencija u kritičnim sustavima može uključivati tehnike poput uzoraka podudaranja, donošenje odluka, prediktivne analitike, otkrivanje anomalija i još mnogo toga. Jednostavniji scenarij primjene umjetne inteligencije je automatiziranje mnogih rutinskih zadataka koji su u prošlosti zahtijevali ljude (npr. analitičare) da prebiru kroz ogromne količine podataka kako bi iz njih izvadili informacije na temelju kojih bi se trebale donositi odluke, a u mnogim slučajevima AI može donijeti mnoge od tih odluka ako je pravilno treniran. Iako se AI može implementirati u hardveru ili softveru, dizajn, implementacija i testiranje moraju se obaviti na vrlo visokim marginama sigurnosti, zaštite i pouzdanosti. Kada AI u kritičnim sustavima ne bi radio kako je namjeravano, mogu se pojaviti ozbiljne posljedice. Posljedice mogu varirati od manjih anomalija u radu do katastrofalnih grešaka koje dovode do značajnog gubitka novca i imovine, ozljeda i gubitka ljudskog života, možda na velikoj skali. Međutim sa pravilnim implementacijom umjetna inteligencija u kritičnoj infrastrukturi nudi brojne prednosti i mogućnosti za poboljšanje operativne učinkovitosti, optimizaciju raspodjele resursa, poboljšanje sigurnosti i omogućavanje naprednog donošenja odluka. Neki od ključnih područja u kojima se AI primjenjuje u kritičnoj infrastrukturi navedeni su u narednim pod poglavljima [38].

4.2.1 Telekomunikacijski i elektroenergetski sektor

U telekomunikacijskom i elektroenergetskom sektoru AI će donijeti nove razine sigurnosti, uključujući predviđanje i ublažavanje prijetnji. Mreže će biti potpuno samorekonfigurabilne kako bi se prilagodile prekidima i uzorcima opterećenja tijekom vrhunca. Robotsko ispitivanje potpomognuto utjecajem umjetne inteligencije, omogućit će bolje programe održavanja za udaljene i teško dostupne resurse.

4.2.2 Sektor vodoopskrbe

U sektoru vodoopskrbe očekuje se da će AI poboljšati kvalitetu vode unapređenjem algoritama za nadzor. Ruralna i slabo pokrivena područja vidjet će povećanje dostupnosti svježe vode. AI nudi poboljšanje filtracije, pročišćavanja i pumpanja. Ovi sustavi mogu također promicati bolje upravljanje i održivost prirodnih resursa kroz naprednu analitiku podataka.

4.2.3 Sektor proizvodnje električne energije, plina i nafte

Već se mogu vidjeti značajna poboljšanja u stavkama poput uravnoteženja opterećenja električne energije i dijagnostici kvarova. Ali čak i u naprednim zemljama poput SAD-a, komponente u elektroenergetskom sustavu i u distribuciji plina mogu biti stare više od 100 godina. Ovi stari infrastrukturni sustavi mogu imati veliku korist od preventivnog održavanja- a kako bi se spriječili kritični kvarovi i omogućilo pravovremeno preuređenje.

4.2.4 Sektor autonomne vožnje

Očekuje se brzi porast broja povezanih vozila i sukladno tome, mogućnost aplikacija za inteligentne ceste i autoceste. Inteligentni transportni sustavi pružaju napredne usluge kroz analitiku, kao što je praćenje prometa i identifikacija prekoračitelja brzine. Pametne autoceste, koje surađuju s drugim sustavima kao što su dronovi, mogu poboljšati protok prometa, spriječiti prometne nesreće, zaštititi sigurnost biciklista, pješaka koje prelaze cestu te pomoći vozačima pronaći parkirna mjesta. Dodavanje 5G tehnologije i drugih mehanizama s velikom širinom pojasa omogućit će autonomnim vozilima da međusobno komuniciraju i dijele informacije o prometu.

4.2.5 Sektor željezničkog prometa

Umjetna inteligencija može značajno unaprijediti frekvenciju prediktivnog održavanja koristeći napredne analize podataka za otkrivanje grešaka i planiranje proaktivnih aktivnosti održavanja. AI također optimizira upravljanje prometom, prilagođavajući raspored vlakova na temelju kapaciteta, potražnje i uvjeta pruge. Automatizirani sustavi rada vlakova koriste AI za kontrolu ubrzanja, kočenja i regulacije brzine, povećavajući sigurnost i smanjujući ljudske pogreške. Međutim važno je istaknuti da implementacija umjetne inteligencije u željezničke sustave zahtijeva pažljivo razmatranje sigurnosnih propisa, te vrlo pomnog definiranja odnosa čovjeka i stroja.

4.2.6 Financijski sektor

AI pruža pojačanu sigurnost, otkrivanje i prevenciju prijevara. Određene populacije, osobito starije osobe, vrlo su sklone prijevarama, a algoritam strojnog učenja ključan je za zaštitu njihove imovine. Očekuje se da će ove tehnologije nastaviti napredovati i povećati javno povjerenje u sve financijske sustave.

4.2.7 Sektor javne sigurnosti

U javnoj sigurnosti prednosti AI-ja već se vide u identifikaciji prijetnji kroz prepoznavanje lica i prepoznavanje obrazaca ponašanja. Sve više, algoritmi dubokog učenja koristit će se za nadzor i identifikaciju prijetnji u javnim prostorima. Zakonodavni organi sve više će koristiti AI da se nose s velikim brojem informacija uključenih u kriminalističke istrage, čineći ih učinkovitijima i sigurnijim za javnost.

4.2.8 Sektor zdravstva

U zdravstvu postoji veliki broj ugrađenih AI aplikacija u dijagnosticiranju stanja pacijenata. AI algoritmi mogu analizirati medicinske slike kao što su *X-zrake*, nalaze magnetske rezonance i CT nalaze kako bi pomogli u otkrivanju i dijagnozi različitih stanja. Sustavi koji pokreću umjetna inteligencija mogu identificirati obrasce i anomalije, pomažući radiolozima u izradi točnijih tumačenja i poboljšanju ranog otkrivanja bolesti. Provedeno je zanimljivo istraživanje koje kaže da obučenom liječniku (kardiologu) općenito je potrebno oko 13 minuta za tumačenje MRI srca. Ali s dolaskom umjetne inteligencije (AI) i algoritama strojnog učenja, nalaz se može analizirati u otprilike četiri sekunde – gotovo 186 puta brže. Također je otkriveno da nije bilo značajne razlike u točnosti kada je algoritam strojnog učenja testiran na preciznost u usporedbi sa stručnjakom. Sigurno će biti potrebno više studija i istraživanja prije nego što ova vrsta pristupa postane održiva i sigurna za zdravstveni sektor [39].

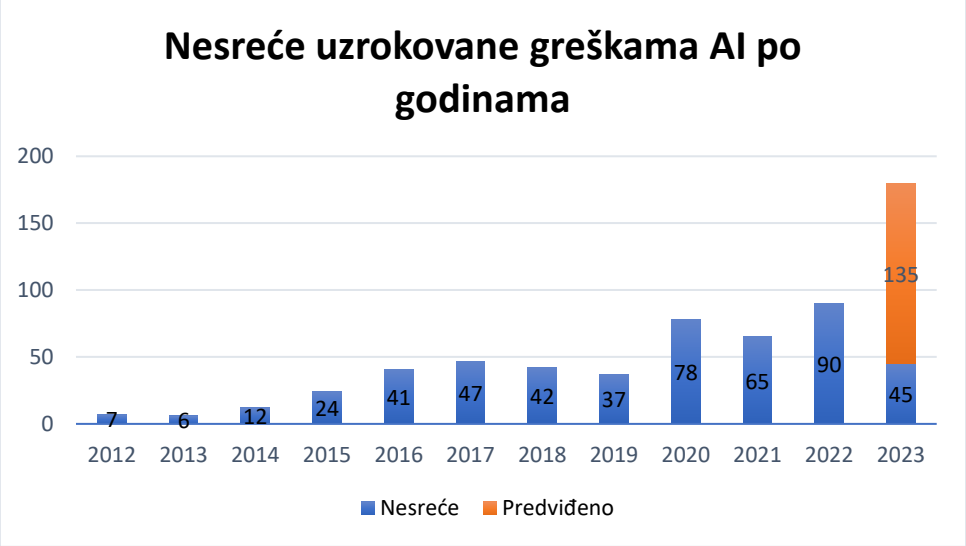
4.2.9 Sektor hrane i poljoprivrede

Umjetna inteligencija u sektoru hrane i poljoprivrede se koristi u raznim područjima, uključujući preciznu poljoprivredu, gdje umjetna inteligencija analizira podatke kako bi optimizirala poljoprivredne mehanizme i povećala prinose usjeva. Sustavi pokretani umjetnom inteligencijom mogu nadzirati usjeve, otkrivati bolesti i pružati pravovremene intervencije za bolje zdravlje usjeva. Lanac opskrbe hranom optimiziran je algoritmima umjetne inteligencije koji upravljaju zalihama, predviđaju potražnju i pojednostavljuju logistiku. Također analizom senzorskih podataka u mehanizmima kvalitete proizvoda dobivaju se visokokvalitetni proizvodi.

4.2.10 Potencijalne opasnosti umjetne inteligencije

lako su razne prednosti primjene umjetne inteligencije u kritičnoj infrastrukturi postoje razni izazovi i pitanja koja se trebaju riješiti. Kritični infrastrukturni sustavi su sami po sebi vrlo skupi za razvoj, testiranje i implementaciju. Sa implementacijom umjetne inteligencije oni postaju još su skuplji zbog kompleksnosti algoritama koji su uključeni. No, osim financijskih izazova postoje brojni drugi. Budući da umjetna inteligencija radi i donosi odluke na skupovima podataka na kojima je trenirana, to potencijalno može rezultirati diskriminirajućim ishodima ili odlukama. U kritičnoj infrastrukturi, loše trenirani algoritmi umjetne inteligencije mogli bi dovesti do donošenja pogrešnih odluka što može rezultirati katastrofalnim posljedicama.

Prema bazi podataka o incidentima s umjetnom inteligencijom postoji više od 500 incidenata u kojima je sudjelovala umjetna inteligencija, a kao što prikazuje dijagram u nastavku taj broj raste iz godine u godinu. U prvom tromjesečju 2023. godine već je bilo 45 nesreća, a sa takvom stopom rasta do kraja godine taj će se taj broj približiti iznosu od 200 [40].



Grafikon 1. Nesreće uzrokovane greškama umjetne inteligencije po godinama

Izvor: [40]

Ako korištenje umjetne inteligencije donosi brojne prednosti i napredak, ono također nosi potencijalne negativne učinke koje treba uzeti u obzir. Jedna od posljedica je premještanje radnih mjesta, budući da tehnologije umjetne inteligencije automatiziraju zadatke koje su prije obavljali ljudi. To može dovesti do nezaposlenosti i ekonomskih razlika. Još jedan problem su etičke implikacije umjetne inteligencije, posebno u područjima kao što su privatnost i sigurnost. Sustavi umjetne inteligencije mogu prikupljati i analizirati ogromne količine osobnih podataka, što izaziva zabrinutost zbog kršenja privatnosti i neovlaštenog pristupa. Osim toga, pristranosti se mogu ugraditi u algoritme umjetne inteligencije, što rezultira diskriminirajućim ishodima i jačanjem postojećih društvenih nejednakosti. Nadalje, postoji rizik od pretjeranog oslanjanja na sustave umjetne inteligencije, gdje ljudska prosudba i donošenje odluka mogu biti zanemareni, što dovodi do ogromnih nesreća kao što nam pokazuje prethodno naveden grafikon.

5. METODE ZAŠTITE KOMUNIKACIJA U KRITIČNOJ INFRASTRUKTURI

Zaštita komunikacijskih sustava u kritičnoj infrastrukturi od iznimne je važnosti jer potencijalni napad ili greška u radu sustava može imati ozbiljne posljedice, uključujući gubitak financijskih sredstava, ugrožavanje javne sigurnosti i potencijalno ugrožavanje nacionalne sigurnosti. Stoga je važno primijeniti odgovarajuće metode zaštite kako bi se stvorile komunikacijske mreže koje će biti otporne na kvarove i ranjivosti. U ovom poglavlju bit će opisane različite metode i tehnike koje se mogu koristiti za osiguravanje mreža u kritičnoj infrastrukturi. Navest će se osnovna načela i prakse koje pomažu smanjiti rizike, povećati otpornost i osigurati nesmetan protok informacija u kritičnim sektorima. Opisat će se koncepti poput segmentacije mreže, koji uključuje podjelu infrastrukturnih mreža na manje, izolirane segmente. Takav pristup ograničava utjecaj sigurnosnog proboja, sprječavajući širenje zlonamjernog softvera ili neovlaštenog pristupa kritičnim operativnim sustavima. Također će se raspravljati o potencijalu enkripcije i sustava za otkrivanje upada za provedbu kontrole pristupa, nadzora prometa i sprječavanja neovlaštene komunikacije. Dobro razumijevanje potencijalnih prijetnji i snažne sigurnosne strategije mogu znatno smanjiti vjerojatnost od uspješnih kibernetičkih napada.

5.1 Mrežna segmentacija

Segmentacijom mreže se naziva proces kojim se računalna mreža dijeli na manje dijelove. Svrha je poboljšanje performansi i sigurnosti mreže. Primjer segmentacije se može naći u industrijskim postrojenjima gdje OT i IT mreže čine dva odvojena okruženja koja imaju različite svrhe. OT mreža se koristi za upravljanje i nadzor fizičkih procesa koji čine glavnu djelatnost industrijskog objekta, dok se IT mreža koristi za komunikaciju i obradu podataka. Industrijski kontrolni sustavi, obično moraju biti izolirani od ostalih mreža naprimjer interneta jer se time smanjuje površina napada i minimizira rizik od izravnih kibernetičkih napada [41].

Primarni razlog segmentiranja OT i IT mreža je sprječavanje neovlaštenog pristupa OT mrežama s IT strane. Razdvajanjem dviju mreža smanjuje se napadni prostor jer se potencijalni napadač mora prebaciti s jedne mreže u drugu. U segmentiranoj mreži, napadač koji je dobio pristup IT mreži još uvijek bi trebao pronaći način da pristupi OT mreži kako bi uzrokovao štetu. Prednosti segmentacije mreže su sljedeći [42]: poboljšanje operativnih performansi smanjenje zagušenja mreže, onemogućavanje štetnog prometa.

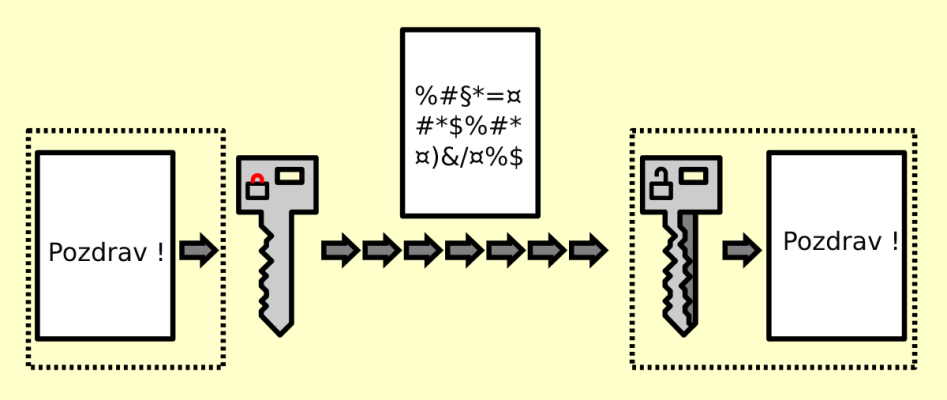
Naprimjer u medicini, medicinski uređaji mogu se segmentirati iz mreže posjetitelja tako da pregledavanje interneta ne utječe medicinske uređaje. Kao drugi primjer iz medicine navode se infuzijske pumpe koje se koriste u bolnicama. One nisu dizajnirane s naprednom sigurnosnom obranom, a segmentacija mreže može spriječiti da štetni internetski promet dođe do njih.

Segmentacija mreže pokazala se korisnom za zaštitu od napada na lanac opskrbe koji je detaljnije opisan u poglavlju 3. Segmentacija mreže dijeli mrežu na manja područja na temelju funkcija te time smanjuje potencijalnu štetu *ransomware-a* ili drugog zlonamjernog softvera koji se može proširiti od kompromitiranog dobavljača. Također ograničavanjem dostupne površine napada, utjecaj svakog napada postaje puno manji, što olakšava oporavak ili zamjenu izgubljenih podataka.

Važno je istaknuti da je segmentacija mreže samo jedan od alata za postizanje sigurnosti, ali sama po sebi neće biti dovoljna za maksimalnu zaštitu. Segmentacija usporava napad te minimizira njegov učinak, a za maksimalnu sigurnost potrebno je upotrijebiti druge metode koje će biti navedene.

5.2 Kriptografske metode

Enkripcija je proces kodiranja informacija. Odnosno izvorni prikaz informacija, poznat kao otvoreni tekst pretvara se u alternativni oblik poznat kao šifrirani tekst. U idealnom slučaju, samo ovlaštene strane mogu dešifrirati šifrirani tekst natrag u otvoreni tekst i pristupiti izvornim informacijama. Enkripcija sama po sebi ne sprječava smetnje, ali uskraćuje razumljiv sadržaj potencijalnom napadaču. Iz tehničkih razloga, shema šifriranja obično koristi pseudo-nasumični ključ šifriranja koji generira algoritam. Moguće je dešifrirati poruku bez posjedovanja ključa, ali za dobro osmišljenu shemu šifriranja potrebni su značajni računalni resursi i vještine. Ovlašteni primatelj može jednostavno dekriptirati poruku pomoću ključa koji je pošiljatelj dao primateljima, ali ne i neovlaštenim korisnicima. Rane tehnike šifriranja svoju prvu primjenu su imale kao vojne poruke u ratovima. Od tada su se pojavile nove tehnike koje su postale uobičajene u svim područjima modernog računarstva. Na slici 10 nalazi se ilustrativni prikaz kako funkcionira enkripcija [43].



Slika 10. Prikaz odvijanja procesa enkripcije

Izvor: [43]

Enkripcija je također ključna za sigurnost sustava kritične infrastrukture te komunikacijskih kanala kroz koje se šalju i primaju osjetljivi podatci. Enkripcija štiti integritet podataka tijekom komunikacije te omogućuje sigurnu instalaciju sigurnosnih ažuriranja. -

Jedan od najčešće korištenih algoritama enkripcije danas je Napredni standard šifriranja (*Advanced Encryption Standard*-AES). AES je simetrični algoritam ,odnosno isti ključ se koristi i za šifriranje i za dešifriranje podataka. Ključ se dijeli između pošiljatelja i primatelja šifriranih podataka i čuva se u tajnosti kako bi se spriječio neovlašteni pristup.

Snaga algoritma AES enkripcije leži u njegovoj sposobnosti da se odupre *brute-force* napadima. *Brute-force* napadi uključuju isprobavanje svih mogućih kombinacija ključeva dok se ne pronađe pravi ključ. Uz veličinu ključa od 128 bita do 256 bita, broj kombinacija postaje toliko velik, da ga je praktički nemoguće probiti korištenjem *brute-force* metode [44].

Još jedna prednost algoritma AES enkripcije je njegova učinkovitost. Može brzo šifrirati i dešifrirati podatke bez previše procesorske snage što ga čini prikladnim za aplikacije koje

zahtijevaju šifriranje i dešifriranje u stvarnom vremenu, kao što su online transakcije i internet bankarstvo. AES je zbog svoje sigurnosti, standardizacije, kompatibilnosti postao i standard američke savezne vlade. Koristi se od manje osjetljivih razina vlade pa sve do onih visoko povjerljivih razina koju koriste vojska i tajne službe [45].

Enkripcija primjenu u kritičnoj infrastrukturi pronalazi kao mjera predostrožnosti u raznim zajednicama. Europska unija (EU) usvojila je nekoliko mjera za poboljšanje kibernetičke sigurnosti svoje kritične energetske infrastrukture. Jedna od tih mjera je upotreba enkripcije za osiguravanje komunikacije između energetskih operatora i vlasti, kao i između različitih energetskih sustava i uređaja. Enkripcija može pomoći u sprječavanju kibernetičkih napada koji bi mogli poremetiti ili oštetiti opskrbu energijom ili ugroziti osjetljive podatke [46].

U SAD-u, North American Electric Reliability Corporation (NERC) zahtijeva od svih organizacija kritične infrastrukture, uključujući one u energetskom sektoru, da koriste enkripciju za zaštitu podataka sustava SCADA. Ovaj zahtjev je dizajniran kako bi se spriječio neovlašteni pristup ovim podacima, te spriječilo ometanje ili onemogućavanje elektroenergetskog sustava [47].

5.3 Kontrola pristupa

Kontrole pristupa imaju važnu ulogu u osiguranju sigurne komunikacije u kritičnoj infrastrukturi. One uključuju implementaciju različitih mehanizama za sprječavanje neovlaštenog pristupa i zaštitu osjetljivih informacija. Neke od najbitnijih metoda kontrola pristupa koje je potrebno implementirati su: dvofaktorska autentifikacija (*Two-factor authentication*- 2FA), pravila jakih lozinki, kontrola pristupa temeljena na ulogama, bilježenje i nadzor pristupa [48].

Dvofaktorska autentifikacija zahtijeva od korisnika pružanje dva oblika autentifikacije. Obično kombinira nešto što korisnik zna (npr. lozinku) s nečim što korisnik posjeduje (npr. jedinstveni kod s mobilnog uređaja ili maila). Ovo dodaje dodatni sloj sigurnosti u slučaju proboja same lozinke.

Implementacijom jakih lozinki smanjuje se osjetljivost na brute-force napade. To uključuje zahtjev da zaporke imaju minimalnu duljinu, složenost (kombinacija velikih i malih slova, brojeva i simbola) te njihovo redovito mijenjanje. Osim navedenih stavki vrlo je važno istaknuti i korištenje različitih zaporki za svaki od računa.

Kontrola pristupa temeljena na ulogama (eng. *Role-based access control*) je metoda kontrole pristupa koja dodjeljuje dopuštenja korisnicima na temelju njihovih uloga unutar organizacije. Svakom korisniku je dodijeljena određena uloga, a prava pristupa definirana su na temelju tih uloga. Ovo osigurava da korisnici imaju pristup samo onim resursima i informacijama koji su potrebni za njihove radne obveze, čime se smanjuje rizik od neovlaštenog pristupa [49].

Mnogi *ransomware* napadi na kritičnu infrastrukturu mogu se povezati s osnovnim sigurnosnim autentifikacijama kao što su korisničko ime i lozinka. U napadu na naftovod Colonial Pipeline koji je ranije detaljnije opisan, prijava za virtualnu privatnu mrežu (*Virtual Private Network*-VPN) pripadala je zaposleniku za kojeg se vjeruje da je neaktivan. Daljnjim istraživanjem ustanovljeno je da je zaposlenik možda upotrijebio lozinku na drugoj web stranici koja je prethodno bila ugrožena. Još jedan od propusta u istoimenome napadu je nekorištenje

2FA. Izvršni direktor Colonial Pipeline-a priznao je da VPN sustav korišten za infiltraciju u mrežu tvrtke nije imao postavljen 2FA. Ta druga sigurnosna prepreka mogla je otežati kriminalcima izvođenje napada.

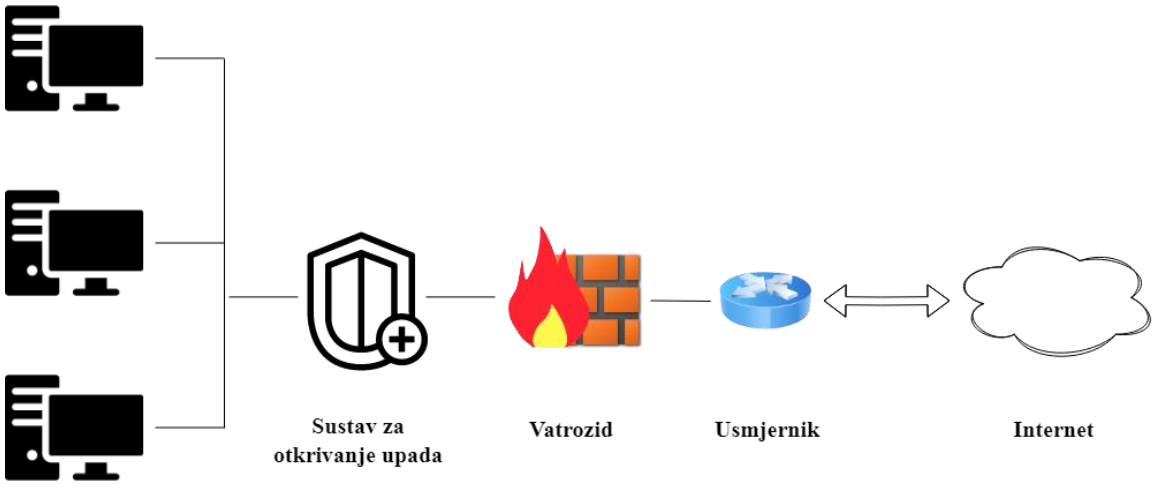
Na prethodnom primjeru jasno je vidljiva važnost implementacije mjera kontrole pristupa,. Upotrebom potrebnih mjera tvrtke mogu značajno smanjiti rizik od neovlaštenog pristupa, povrede podataka i potencijalne smetnje u svojim komunikacijskim sustavima.

5.4 Sustav za otkrivanje upada

Sustav za otkrivanje upada (*Intrusion Detection System*- IDS) je sustav koji automatizirano prati mrežne i sistemske događaje u svrhu detekcije kršenja sigurnosne politike. Takav sustav nije zadužen za sprječavanje upada na sustav. U svrhu sprječavanja upada koristi sustav za sprječavanje upada (*Intrusion Preventions System* – IPS), koji najčešće kao jedan od svojih dijelova sadrži i sustav za detekciju upada. Najčešće programska rješenja posjeduju elemente i za detekciju i za sprečavanje, stoga se radi o sustavima za detekciju i sprječavanje upada (Intrusion Prevention Detection System-IPDS). Najvažnija uloga takvih sustava jest identificiranje mogućih sigurnosnih incidenata. Tek kada je mogući sigurnosni incident identificiran, sustav pokušava spriječiti upad. IDS sustavi dijele se na sustave za detekciju neovlaštenih aktivnosti u mreži (*Network Intrusion Detection Systems* – NIDS) i sustave za detekciju neovlaštenih aktivnosti na računalu (*Host-based Detection Systems*- HIDS) [50].

NIDS sustavi prate i analiziraju mrežni promet koji može biti potencijalna prijetnja u stvarnom vremenu uz pomoć NIDS senzora. Senzori provjeravaju sadržaj i informacije zaglavlja svih paketa koji se kreću mrežom. NIDS senzori postavljeni su na ključnim točkama u mreži kako bi pregledali promet sa svih uređaja na mreži.

HIDS sustavi nadziru i analiziraju konfiguraciju sustava i aktivnosti aplikacija za uređaje koji rade na mreži poduzeća. HIDS senzori rade snimku postojećih sistemskih datoteka i uspoređuju ih s prethodnim snimkama. Oni traže neočekivane promjene, kao što su prepisivanje, brisanje i pristup određenim portovima.



Slika 11. Primjer implementacije sustava za otkrivanje upada u jednostavnoj mreži

Izvor: [51]

Na slici 11 nalazi se prikaz implementacije IDS-a u jednostavnoj mreži. Kao što se vidi na slici, kada je riječ o zaštiti mreže IDS nije sveobuhvatno sigurnosno rješenje nego su tu i ostali sigurnosni mehanizmi poput vatrozida. Iako i vatrozid i IDS imaju identičnu ulogu kada je u pitaju mrežna sigurnost, oni se značajno razlikuju. Razlike se očituju u tome IDS neprekidno osluškuje sustav tražeći znakove napada (napadi mogu dolaziti izvana ili biti u samom sustavu) te signalizira ukoliko primijeti neku sumnjivu aktivnost. S druge strane, vatrozid samo ograničava pristup između mreža. Velika većina sustava za otkrivanje upada ima sposobnost povezivanja aktivnosti primijećenih u nekom vremenu te slanja obavijesti osoblju o napadu u tijeku.

Suprotne tome vatrozid obično reagira na svaki paket pojedinačno i ne uzima u obzir prethodne događaje. Može se zaključiti da vatrozid i IDS ipak imaju drugačije uloge u zaštiti sigurnosne infrastrukture, i samim time ne isključuju jedan drugog [52]. Unatoč svim prednostima koje sustav za otkrivanje upada donosi postoje i neke negativne strane [53]:

- postoje situacije kada IDS može poslati lažnu uzbunu u vezi nekog paketa. Takvi lažni alarmi ponekad mogu stvoriti ozbiljne probleme jer tada može doći do zanemarivanja prave prijetnje
- sustavi za otkrivanje upada (IDS) pate od ozbiljnog problema. Ne uspijevaju otkriti novi sumnjivi upad jer novi zlonamjerni softver ne prikazuje obrazac prethodnog neobičnog ponašanja. Stoga IDS mora poduzeti korake kako bi otkrio takvo novo ponašanje. Tako da organizacija može odmah poduzeti mjere opreza u slučaju takve prijetnje.

Važnost implementacije sustava za otkrivanje upada vidljiv je na primjeru Njemačke koja je usvojila revidirani Zakon o IT sigurnosti (ITSA 2.0). Zakon naglašava važnost sustava za otkrivanje upada te od svih opskrbljivača energije, vodovoda, te odnedavno tvrtki za zbrinjavanje otpada zahtijeva implementaciju sustava za otkrivanje upada. Prema obrazloženjima zakona, ovaj sustav trebao bi pružiti cjelovitije zaštitu komunikacijske tehnologije operatora kritične infrastrukture, odnosno voditi računa o cjelokupnoj infrastrukturi kako bi se kontinuirano identificirale i sprječavale prijetnje [54.]

Implementacija IDS-a u kritičnoj infrastrukturi pruža mogućnosti proaktivnog nadzora i otkrivanja prijetnji. IDS sudjeluje u zaštiti kritične imovine, sprječava neovlašteni pristup i gubitak podataka, te osigurava pouzdanost kritičnih infrastrukturnih sustava. Međutim, kao što je navedeno ranije IDS bi trebao biti popraćen i raditi u suradnji drugim sigurnosnim mjerama kao što su vatrozidi, kontrole pristupa i redovite sigurnosne procjene kako bi se uspostavio siguran sustav kritične infrastrukture [52].

5.5 Mjere fizičke sigurnosti

Fizičke sigurnosne mjere igraju ključnu ulogu u zaštiti kritične infrastrukture od neovlaštenog pristupa, sabotaže, krađe i drugih fizičkih prijetnji. Ukoliko se zanemari fizički aspekt zaštite kritične infrastrukture napadač može lako oštetiti ili ukrasti kritična IT sredstva, instalirati zlonamjerni softver na sustave ili ostaviti priključak za daljinski pristup na mreži kao što je dogodilo u mnoštvo prethodno navedenih primjera.

Ovaj oblik zaštite naziva se dubokom ili slojevitom zaštitom, budući da postoji nekoliko kontrolnih točaka u fizičkim infrastrukturama. Fizička šteta jednako je štetna kao i digitalni gubitak a često jedna vrsta štete podrazumijeva drugu, stoga se ne smiju zanemariti mjere fizičke sigurnosti. sigurnosne mjere osmišljene su za sprječavanje neovlaštenog pristupa, oštećenja ili poremećaja kritičnih infrastrukturnih sustava uključuju [55]:

- fizičke barijere koje uključuju ograde, zidove, stupiće ili druge strukture dizajnirane za sprječavanje neovlaštenog pristupa ili ublažavanje utjecaja fizičkog napada
- sustave kontrole pristupa koji mogu uključivati brave, kartice s ključevima, biometrijske skenere i druge mehanizme koji osiguravaju da samo ovlaštene osobe mogu ući u određena područja
- sustave nadzora koji uključuju kamere, bespilotne letjelice i druge tehnologije nadzora mogu nadzirati infrastrukturu kako bi otkrile neobične aktivnosti ili prijetnje
- sigurnosno osoblje koje obuhvaća skup stražara, zaštitara ili policije koji mogu patrolirati infrastrukturom, reagirati na incidente osigurati prisutnost odvraćanja
- senzore za otkrivanje upada koji mogu detektirati kada netko pokuša probiti fizičku barijeru ili pristupiti ograničenom području.

Ulaganje u sigurnost fizičke infrastrukture pruža nekoliko ključnih prednosti kao što su: smanjenje rizika, sprječavanje neovlaštenog pristupa, kontinuitet rada, javnu sigurnost, nacionalna sigurnost, osiguranje i odgovornost. Ulaganje u sigurnost fizičke infrastrukture preventivna je mjera koja bi mogla značajno uštedjeti troškove, zaštititi javnu sigurnost i dugoročno osigurati siguran rad. Ove mjere fizičke sigurnosti trebale bi biti integrirane s drugim sigurnosnim slojevima, kao što su mjere kibernetičke sigurnosti, sigurnosni protokoli osoblja, te planovi u slučaju incidenta, kako bi se pružio sveobuhvatan pristup zaštiti kritične infrastrukture.

6. ZAKLJUČAK

Važnost kritične infrastrukture leži u činjenici da su ti sustavi neizostavni dio modernog društva bez kojih bez bi svakodnevni život stao. Aspekt komunikacije jedna je od stavki koja se ne smije zanemariti kada je riječ o kritičnim sustavima, upravo zbog toga sigurnost komunikacijskih sustava kritične infrastrukture od iznimne je važnosti za svakog pojedinca. Velik broj mogućih prijetnji koje iz dana u dan postaju mnogobrojnije i složenije glavni su izazov s kojim se susreću komunikacijski sustavi kritične infrastrukture te osoblje zaduženo za njihovu zaštitu.

S velikom složenosti samih sustava kritične infrastrukture veliki je broj sigurnosnih izazova te potencijalnih točaka napada za same sustave. IT trendovi i inovacije povezane s digitalnom transformacijom doveli su do toga da se veliki broj OT sustava spaja na internet. Zbog ovog smjera povezanosti na internet te veće otvorenosti sustava, enormno se povećavaju operativni sigurnosni rizici. Prijelaz sa zatvorenih na otvorene sustave, poznat i kao IT-OT konvergencija, stvara nove sigurnosne rizike kojima treba pridati pažnju. Također rastući trendovi u zaštiti kritične infrastrukture poput umjetne inteligencije, računarstva u oblaku, 5G-a nude brojne inovacije u smislu zaštite kritične infrastrukture ali i brojne izazove koje je potrebno riješiti prije njihove kompletne implementacije.

Zaštita komunikacije u kritičnoj infrastrukturi je višestruki pothvat koji zahtijeva sveobuhvatan pristup. Implementacijom snažnih mrežnih sigurnosnih mjera, korištenjem tehnologija šifriranja, jačanjem fizičke sigurnosti, sustavi kritiče infrastrukture mogu poboljšati otpornost i sigurnost svojih komunikacijskih mreža, osiguravajući kontinuiran i pouzdan rad vitalnih usluga. Istovremeno s novim prijetnjama koje se neprestano pojavljuju potrebna su stalna istraživanja te zajednička suradnja između sudionika koji sudjeluju u zaštiti kritične infrastrukture. Rješavanjem ovih izazova i kontinuiranim poboljšavanjem kibernetičke sigurnosti, stabilnost i sigurnost sustava kritične infrastrukture dovest će se na najvišu razinu.

LITERATURA

1. Europska Unija. *Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite*. Bruxelles: Službeni list Europske Unije; 2008. Preuzeto s: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN [Pristupljeno: 4. travnja 2023.]

2. Ravnateljstvo civilne zaštite. *Kritična infrastruktura*. Preuzeto s: https://civilna-zastita.gov.hr/kriticna-infrastruktura/111 [Pristupljeno:5.travnja 2023.]

3. Pederson P, Dudenhoeffer D, Hartley S, Permann M. Idaho National Laboratory, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho Falls; 2006. Preuzeto s: http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf [Pristupljeno: 5. travnja 2023.]

4. ResearchGate. *Interdependency graph of 2001 Baltimore tunnel fire*. Preuzeto s: https://www.researchgate.net/figure/Interdependency-graph-of-2001-Baltimore-tunnel-fire-19_fig6_286328683 [Pristupljeno: 5.travnja.2023.]

5. Wikipedia. *Howard Street Tunnel fire*. Preuzeto s: https://en.wikipedia.org/wiki/Howard_Street_Tunnel_fire [Pristupljeno: 5.travnja.2023.]

6. White House. *Presidential Decision Directive/NSC-63*: Critical Infrastructure Protection; 1998. Preuzeto s: https://irp.fas.org/offdocs/pdd/pdd-63.htm [Pristupljeno: 5. travnja. 2023.]

7. Murray A, Grubesic T. Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics*. 2012;29(1): 56-65. Preuzeto s: https://www.sciencedirect.com/science/article/abs/pii/S0736585311000438 [Pristupljeno: 5. travnja 2023.]

8. A Division of The Attorney Generals Department. Emergency Management Australia, *Critical Infrastructure Emergency Risk Management and Assurance*; 2003. Preuzeto s: https://www.files.ethz.ch/isn/10231/doc_10261_290_en.pdf [Pristupljeno: 5. travnja 2023.]

9. Škero M, Ateljević V., Kancelarija za evropske integracije. *Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES*; 2015. Preuzeto s: https://scindeks-clanci.ceon.rs/data/pdf/0042-8426/2015/0042-84261503192S.pdf [Pristupljeno: 5. travnja 2023.]

10. Cybersecurity and Infrastructure Security Agency. *Critical Infrastructure Sectors*. Preuzeto s: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sector [Pristupljeno: 5. travnja 2023.]

11. Republika Hrvatska. *Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura*. Izdanje: 108. Zagreb: Narodne novine; 2019 Preuzeto s: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html [Pristupljeno: 5. travnja 2023.]

12. Ministarstvo obrane Republike Hrvatske. *The Republic of Croatia national security strategy*. Preuzeto s: https://www.morh.hr/wp content/uploads/2018/04/strategy_18012018.pdf [Pristupljeno: 5. travnja 2023.13. Rosslin John Robles,Min-kyu Choi, Eun-suk Cho1 Seok-soo Kim, Gil-cheol Park, Jang-Hee Lee. Common Threats and Vulnerabilities of Critical Infrastructures. *International Journal of Control and Automation.* 2008;1(3): 17-21. Preuzeto s: http://article.nadiapub.com/IJCA/vol1_no1/3.pdf [Pristupljeno: 5. travnja 2023.]

14. Wikipedia. *Zloćudni softver*. Preuzeto s: https://hr.wikipedia.org/wiki/Zloćudni_softver. [Pristupljeno: 5. travnja 2023.]

15.Stančin D. *Analiza kibernetičkih prijetnji povezanih s krađom identiteta u uvjetima pandemije COVID-19*. Diplomski rad. Sveučilište u Zagrebu, Ekonomski fakultet; 2022. Preuzeto s: https://repozitorij.efzg.unizg.hr/islandora/object/efzg%3A9194/datastream/PDF/view [Pristupljeno: 20. kolovoza 2023.]

16. Carnet CERT. *Phishing napadi*. CCERT-PUBDOC-2005-01-106. Preuzeto s: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2005-01-106.pdf [Pristupljeno: 5. travnja 2023.]

17. Simplilearn. *What is Phishing Attack? Definition, Types and How to Prevent it*. Preuzeto s: https://www.simplilearn.com/ice9/free_resources_article_thumb/phishing_working_2-What_Is_Phishing.PNG [Pristupljeno: 20. kolovoza 2023.]

18. Sviben T. *Analiza kibernetičkih napada na kritične infrastrukture*. Diplomski rad. Sveučilište u Zagrebu, Ekonomski fakultet; 2022. Preuzeto s: https://zir.nsk.hr/islandora/object/efzg:9022/datastream/PDF/view Pristupljeno: 6. travnja 2023.]

19.Wallarm. *What is MITM - Man in the Middle Attack*. Preuzeto s: https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack [Pristupljeno 20. kolovoza 2023.]

20. Spiceworks. *What Is an SQL Injection*. Preuzeto s: https://www.spiceworks.com/it-security/application-security/articles/what-is-sql-injection/ [Pristupljeno 20. kolovoza 2023.]

21. Computer world. *SQL injection attacks led to Heartland, Hannaforrd breaches*. Preuzeto s: https://www.computerworld.com/article/2527185/sql-injection-attacks-led-to-heartland--hannaford-breaches.html [Pristupljeno 30. kolovoza. 2023.]

22. Toplak M. *Problematika zero day napada i moguća zaštita*. Diplomski rad. Sveučilište u Zagrebu, Ekonomski fakultet; 2021. Preuzeto s: https://zir.nsk.hr/en/islandora/object/efzg%3A7134/datastream/PDF/view [Pristupljeno: 6. travnja 2023.]

23. Wikipedia. *Supply chain attack*. Preuzeto s: https://en.wikipedia.org/wiki/Supply_chain_attack [Pristupljeno: 10. travnja 2023.]

24. Wallarm. *What is a Supply Chain Attack?*. Preuzeto s: https://www.wallarm.com/what/what-is-a-supply-chain-attack [Pristupljeno 20. kolovoza 2023.]

25. lon Urlainis, Igal M. Shohet, Robert Levy, David Ornai, Oren Vilnay. Damage in critical infrastructures due to natural and man-made extreme events. *Procedia Engineering*. 2014; 85: 529-535.Preuzeto s: https://www.sciencedirect.com/science/article/pii/S1877705814019468?ref=pdf_download&fr=RR-2&rr=7d2f49b56f890618 [Pristupljeno: 18. travnja 2023.]

26. Worldbank. *Earthquake Damage in Türkiye Estimated to Exceed $34 billion: World Bank Disaster Assessment Report.* Preuzeto s http://documents1.worldbank.org/curated/en/099022723021250141/pdf/P1788430aeb62f08009b2302bd4074030fb.pdf [Pristupljeno: 20. kolovoza 2023.]

27. Public Safety Canada. *Threats to Canada's Critical Infrastructure*. Preuzeto s: https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf [Pristupljeno: 18. travnja 2023.]

28. Murray G, Johnstone M, Valli, C. The convergence of IT and OT in critical infrastructure. U:. *Proceedings of 15th Australian Information Security Management Conference*, 5-6 December 2017, Perth, Australia. Perth: Research Online;2017.pp. 149-155. Preuzeto s: https://core.ac.uk/download/pdf/159235139.pdf [Pristupljeno: 22. travnja 2023.]

29. Powermag. *Why Power Generators Can't Ignore the Ukraine Cyberattack*. Preuzeto s: https://www.powermag.com/wp-content/uploads/2016/05/PWR_050116_SR_Ukraine_Fig2.jpg [Pristupljeno: 20. kolovoza 2023.]

30. Žagar M. *Napadi zlonamjernim programima na računalno upravljanja industrijska postrojenja*. Polytechnic and design, 2016, 4(1):30-36.Preuzeto s: https://doi.org/10.19279/TVZ.PD.2016-4-1-04 [Pristupljeno 22. travnja 2023.]

31. IEEE Spectrum. *The Real Story of Stuxnet*. Preuzeto s: https://assets.rbl.ms/25571945/origin.jpg [Pristupljeno 21. kolovoza 2023.]

32. Tintor D. *OT i IT kibernetička sigurnost*. Završni rad. Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija; 2020. Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:200:716238 [Pristupljeno 26. travnja 2023.]

33. Jannati H, Bahrak B. An improved authentication protocol for distributed mobile cloud computing services. *International Journal of Critical Infrastructure Protection*, 2017; 19: 59-67. Preuzeto s: https://core.ac.uk/download/pdf/96564885.pdf [Pristupljeno 2.svibnja 2023.]

34. Pericherla, S. Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art. *The ISC International Journal of Information Security*, 2023; 15(1): 1-58. Preuzeto s: https://www.isecure-journal.com/article_154670_e5e692199d1faab97eac08d75daae657.pdf [Pristupljeno 2.svibnja 2023.]

35. BBC News. *Russian nuclear scientists arrested for 'Bitcoin mining plot*. Preuzeto s: https://www.bbc.com/news/world-europe-43003740 [Pristupljeno 2.svibnja 2023.]

36. Nozomi Networks. *Trends and Countermeasures for Critical Infrastructure Attacks* Preuzeto s: https://www.nozominetworks.com/downloads/Nozomi-Networks-OT-IoT-Security-Report-ES-2021-2H.pdf [Pristupljeno 2.svibnja 2023.]

37. Cybersecurity and Infrastructure Security Agency. *Defending Against Software Supply Chain Attacks*. Preuzeto s: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf [Pristupljeno 2.svibnja 2023.]

38. Laplante P, Milojicic D, Serebryakov S, Bennett D. *Artificial Intelligence and critical systems: from hype to reality computer*, 2020; 53(11):45-52. Preuzeto s: https://www.osti.gov/servlets/purl/1713282 [Pristupljeno 20.svibnja 2023.]

39. Bhuva A, Bai W, Lau C, Davies R, Ye Y, Bulluck H, McAlindon E, Culotta, V, Swoboda P, Captur G, Treibel T, Joao A, Knott K, Seraphim A, Cole G, Petersen S, Edwards N, Greenwood J, Bucciarelli D, Hughes A, Rueckert D, Moon J, Manisty C. *A Multicenter, Scan-Rescan, Human and Machine Learning CMR Study to Test Generalizability and Precision in Imaging Biomarker Analysis. Circ Cardiovasc Imaging*, 2019; 12(10). Preuzeto s: https://www.ahajournals.org/doi/epub/10.1161/CIRCIMAGING.119.009214 [Pristupljeno 20.svibnja 2023.]

40. AI Incident Database. Preuzeto s: https://incidentdatabase.ai/ [Pristupljeno 25.svibnja 2023.

41. Cisco. *What Is Network Segmentation*. Preuzeto s: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html#~how-segmentation-works [Pristupljeno 10. lipnja 2023.]

42. Radiflow. *The Crucial Role of IT-OT Network Segmentation in Protecting Critical Infrastructure.* Preuzeto s: https://www.radiflow.com/blog/the-crucial-role-of-it-ot-network-segmentation-in-protecting-critical-infrastructure [Pristupljeno 10.lipnja 2023.]

43. Wikipedia. *Encryption*. Preuzeto s: https://en.wikipedia.org/wiki/Encryption [Pristupljeno 10 lipnja 2023.]

44. Wikipedia. *Advanced Encryption Standard*. Preuzeto s: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard [Pristupljeno 10. lipnja 2023.]

45. Carnet CERT. *AES algoritam*. CCERT-PUBDOC-2003-08-37. Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-08-37.pdf [Pristupljeno 10. lipnja 2023.]

46. European Parliamentary Research Service. *Cybersecurity of critical energy infrastructure*. Preuzeto s s: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI%282019%29642274_EN.pdf [Pristupljeno 30. kolovoza 2023.]

47. Zafirovic-Vukotic M, Moore R, Leslie M, Midence R, Pozzuoli M. Secure SCADA network supporting NERC CIP. *IEEE Power & Energy Society General Meeting, 2009,* Calgary, Canada; 2009, pp. 1-8. Preuzeto s: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5275559 [Pristupljeno 30. kolovoza 2023.]

48. Infosec. *Access Control Implementation in ICS*. Preuzeto s: https://resources.infosecinstitute.com/topic/access-control-implementation-in-ics/ [Pristupljeno 12. lipnja 2023.]

49. National Institute of Standards and Technology. *Role Based Access Control*. Preuzeto s: https://csrc.nist.gov/projects/role-based-access-control [Pristupljeno 15. lipnja 2023.]

50. Centar informacijske sigurnosti. *IPS/IDS*. Preuzeto s: https://www.cis.hr/sigurnosni-alati/ips-ids.html [Pristupljeno 15. lipnja 2023.]

51.Comodo. *What is an intrusion detection system(IDS)*. Preuzeto s: https://www.comodo.com/images/ids-in-security.png [Pristupljeno 15. lipnja 2023.]

52. Pavković N. Sveučilište u Zagrebu, *Detekcija upada u sustav*. Zagreb: Fakultet elektrotehnike i računarstva; 2007. Preuzeto s: http://sigurnost.zemris.fer.hr/ns/2007_pavkovic/IDS.html [Pristupljeno 15. lipnja 2023.]53.

53. Aljanabi M, Ismail M, Hussein A. Intrusion Detection Systems, Issues, Challenges, and Needs. *International Journal of Computational Intelligence Systems*, 2021; 14(1): 560-571. Preuzeto s: https://www.atlantis-press.com/article/125951139.pdf [Pristupljeno 15. lipnja 2023.]

54. Rhebo. *New German IT Security Act Makes Intrusion Detection Systems Mandatory*. Preuzeto s: https://rhebo.com/en/company/news/post/new-german-it-security-act-makes-intrusion-detection-systems-mandatory/ [Pristupljeno 30. kolovoza 2023.]

55. Senstar. *Physical Infrastructure Security*. Preuzeto s: https://senstar.com/senstarpedia/physical-infrastructure-security/ [Pristupljeno 15. lipnja 2023.]

POPIS SLIKA

POPIS TABLICA

POPIS GRAFOVA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Sigurnost komunikacije u kritičnoj infrastrukturi , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 4. 9. 2023.

Josip Antunović, Antunović Josip
(ime i prezime, *potpis*)