Analiza isplativosti uvođenja koncepta mreže nultog povjerenja u tvrtku operatora energetske kritične infrastrukture

Kapić, Goran

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:954314

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Goran Kapić

ANALIZA ISPLATIVOSTI UVOĐENJA KONCEPTA MREŽE NULTOG POVJERENJA U TVRTKU OPERATORA ENERGETSKE KRITIČNE INFRASTRUKTURE

SPECIJALISTIČKI RAD

Zagreb, 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Goran Kapić

ANALIZA ISPLATIVOSTI UVOĐENJA KONCEPTA MREŽE NULTOG POVJERENJA U TVRTKU OPERATORA ENERGETSKE KRITIČNE INFRASTRUKTURE

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Goran Kapić

COST-BENEFIT ANALYSIS OF INTRODUCING THE ZERO-TRUST NETWORK CONCEPT IN CRITICAL ENERGY INFRASTRUCTURE OPERATOR COMPANY

ANALIZA ISPLATIVOSTI UVOĐENJA KONCEPTA MREŽE NULTOG POVJERENJA U TVRTKU OPERATORA ENERGETSKE KRITIČNE INFRASTRUKTURE

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija „Informacijska sigurnost“, na Zavodu za primijenjeno računarstvo.

Mentor: prof. dr. sc. Krešimir Fertalj, Zavod za primijenjeno računarstvo

Specijalistički rad ima: 90 stranica

Specijalistički rad br.:

Povjerenstvo za ocjenu u sastavu:

1. prof. dr. sc. Boris Vrdoljak – predsjednik
2. prof. dr. sc. Krešimir Fertalj – mentor
3. prof. dr. sc. Neven Vrček, Sveučilište u Zagrebu Fakultet organizacije i informatike – član

Povjerenstvo za obranu u sastavu:

1. prof. dr. sc. Boris Vrdoljak – predsjednik
2. prof. dr. sc. Krešimir Fertalj – mentor
3. prof. dr. sc. Neven Vrček, Sveučilište u Zagrebu Fakultet organizacije i informatike – član

Datum obrane: 27. ožujka 2023.

POSVETA

Zahvalio bih se mojem mentoru profesoru Fertalju, na pomoći i strpljenju sa mnom kroz proces izrade ovog rada.

Hvala mojoj supruzi Nadiri koja mi je uzor da uopće pokušavam ovakve stvari i što me čini boljim čovjekom.

Hvala mojoj kćeri Nini što postoji i čini mi svaki dan sunčanim.

PREDGOVOR

Autor rada je sklopu svoje profesionalne karijere 2017. godine došao u situaciju osmisliti i upravljati uvođenjem višegodišnje sigurnosne inicijative u složeno okruženje informacijske tehnologije/operativne tehnologije (engl. *information technology/operational technology* - IT/OT) visoko reguliranog operatora nacionalne energetske kritične infrastrukture. Iako je taj projektni program uz podršku tadašnje upravljačke strukture pokrenut i potpuno implementiran tijekom zadnjih pet godina (2018.-2022.), činjenica je da je odluka o pokretanju tako značajne i financijski intenzivne sigurnosne inicijative donesena u velikoj mjeri intuitivno, bez odgovarajuće studije izvodljivosti i u nedostatku alternativne sigurne arhitekture koja bi na odgovarajući način dala odgovore na sva pitanja koja je organizacija u tom trenutku htjela riješiti. Ovaj je rad nastao kao potreba autora da sam sebi, ali i potencijalno zainteresiranim čitateljima koji se nalaze u sličnoj situaciji, pruži analitički, promišljeni i strukturirani odgovor na pitanje da li je uvođenje arhitekture nultog povjerenja (engl. *zero trust architecture* - ZTA) u tvrtki operatora kritične infrastrukture isplativo i u kojim okolnostima

SAŽETAK

Naslov: ANALIZA ISPLATIVOSTI UVOĐENJA KONCEPTA MREŽE NULTOG POVJERENJA U TVRTKU OPERATORA ENERGETSKE KRITIČNE INFRASTRUKTURE

Rad obrađuje problematiku promjenjivih i rastućih prijetnji na Internetu u postpandemijskom svijetu i potrebu za novom paradigmom mrežne sigurnosti. Definiraju se osnovni pojmovi organizacije rada, deklariraju korišteni alati, metodologije procjene rizika i korištene metrike, te navode ograničenja i pretpostavke provedenih istraživanja. Pojašnjava se pojam arhitekture nultog povjerenja, utvrđuju njezini osnovni principi i tehnologije, te se projektno definira sigurnosna inicijativa uvođenja ove arhitekture u poslovanje. Dokumentiraju se analize rizika tvrtke prije (početak 2018. godine) i poslije (kraj 2022. godine) uvođenja sigurnosne inicijative, te se razrađuju i analiziraju ukupni troškovi njezinog uvođenja. Uspoređuje se dobiveni pozitivni pomak u profilu rizika tvrtke. Diskutira se opravdanost ulaganja za dobivene koristi kroz analizu troškova i koristi, te se uočavaju okolnosti koje bi takvu sigurnosnu inicijativu mogle učiniti opravdanom.

Ključne riječi: okvir mrežne sigurnosti, analiza rizika, analiza troška i koristi, mreža nultog povjerenja, ZTA, kibernetička sigurnost

ABSTRACT

Title: COST-BENEFIT ANALYSIS OF INTRODUCING THE ZERO-TRUST NETWORK CONCEPT IN CRITICAL ENERGY INFRASTRUCTURE OPERATOR COMPANY

The paper deals with the issue of evolving and escalating threats on the Internet in the postpandemic world and the need for a new paradigm of network security. The basic concepts of work organization are defined, the tools used, risk assessment methodologies and metrics used are declared, and limitations and assumptions of the conducted research are stated. The concept of zero-trust architecture is clarified, its basic principles and technologies are determined, and the security initiative of introducing this architecture into business is defined. Risk analysis of the company before (beginning of 2018.) and after (end of 2022.) the introduction of the security initiative is documented, and the total costs of its introduction are elaborated and analysed. The resulting positive shift in the company's risk profile is analysed. The justification of the investment for the obtained benefits is discussed through the cost-benefit analysis and the circumstances that could make such a security initiative justified are noted.

Keywords: network security framework, risk analysis, cost-benefit analysis, zero-trust network, ZTA, cybersecurity

SADRŽAJ

UVOD

Sve više organizacija mijenja svoju paradigmu informacijskih tehnologija tako da preispituje svoje navike širenja mreže po lokalnoj mreži (engl. local area network – LAN), spore i skupe izgradnje vlastitih aplikacija, te ulaganja u vlastiti hardver i kupovine licenci za različite aplikacije. Pandemija COVID-19 virusa cijeli je svijet preusmjerila na rad od kuće, čime se dodatno pospješilo gubljenje granica između Interneta i korporativne mreže i dovela u pitanje definicija što zapravo smatramo „sigurnim“ obzirom na fizičku lokaciju korisnika ili uređaja na kojem se radi. Nesposobnost da unaprijed znamo tko je „siguran“, a tko „napadač“, unijela je rasulo i posvemašnju neizvjesnost u IT strategije firmi koje se uglavnom u novoj situaciji nisu snašle. *Ransomware* je „vrsta zlonamjernog softvera iz kriptovirologije koji prijeti objavljivanjem osobnih podataka žrtve ili trajnom blokadom pristupa njima osim ako se ne isplati otkupnina“ [1]. Ovaj zloćudni kod u svim svojim inačicama je promijenio način na koji smo promatrali prijetnje s Interneta [2] i kreirao sasvim novu vrstu kriminala na globalnom nivou. Bilo je potrebno promijeniti sigurnosnu strategiju organizacija, redefinirati sigurnost na mreži i dobiti jasan okvir koji će organizaciji reći kako se dalje braniti i istovremeno sigurno širiti poslovanje.

Mnogi su tvrtke nastavile tretirati mrežnu sigurnost kao i dosad, što jest ostala jedna od opcija, ali se time prihvatio inherentni rizik ignoriranja nove realnosti: napadači su se mijenjali, prilagodili se i usvojili nova znanja i nove metode. Prijetnje su postale kudikamo ozbiljnije i teže za otkrivanje, oporavak dugotrajniji, posljedice teže, a pojavio se i prvi smrtni ishod napada računalnim virusima [3]. Ratovi danas rutinski uključuju kibernetičke napadačke udare na neprijateljsku kritičnu infrastrukturu energetskih, komunikacijskih i financijskih organizacija, a potom i institucije zdravstvenog sektora, institucije države, itd. [4].

Tvrtke koje imaju puno za izgubiti, a tu ubrajamo npr. operatore kritične infrastrukture i u državnom i u privatnom vlasništvu, moraju mijenjati strategiju mrežne sigurnosti. Usvajanje strategije nultog povjerenja sve se glasnije spominje kao tehnički pouzdano rješenje [5] s dobrom očekivanom otpornošću na buduće promjene u tehnologiji i širenje poslovne mreže, no postavlja se pitanje je li to izbor koji svaka organizacija kojoj je stalo do sigurnosti njezinih operacije može jednostavno odabrati i potom efikasno implementirati i održavati.

Svrha ovog specijalističkog rada je unapređenje kibernetičke sigurnosti i osiguranje kontinuiteta poslovnih procesa tvrtke Energent d.o.o. kroz uvođenje arhitekture nultog povjerenja u periodu 2018.-2022. godine, pri čemu se istražuju okolnosti i uvjeti u kojima se traženo podizanje kibernetičke sigurnosti uvođenjem ZTA moći smatrati isplativim i nekoj drugoj za takav potez zainteresiranoj tvrtki. Obzirom da je u predmetnoj inicijativi tijekom svih pet godina osobno sudjelovao u značajnoj upravljačkoj i izvršnoj ulozi, autor je motiviran retroaktivno otkriti je li se upravo implementirana petogodišnja sigurnosna inicijativa u tvrtki Energent d.o.o. pokazala isplativom ili ne. Korištena je metodologija u kojoj je uspoređen profil rizika tvrtke prije i poslije provedbe sigurnosne inicijative, te je smanjenje rizika tvrtke kroz analizu troškova i koristi uspoređeno sa vremenskim, ljudskim i financijskim resursima koje je tvrtke uložila u provedbu sigurnosne inicijative.

Nakon uvoda, u drugom poglavlju uvode se temeljni pojmovi, odabire metodologija, definiraju metrike i navode korišteni alati. Treće poglavlje navodi definiciju, svrhu, građevne elemente mreže nultog povjerenja, te se diskutiraju ključni principi, prednosti i mene ovog koncepta. Četvrto poglavlje daje unutrašnji i vanjski kontekst tvrtke Energent d.o.o. i smješta ju na svjetsku mapu energetskog sektora. Peto poglavlje analizira profil rizika tvrtke prije, a šesto poglavlje analizira profil rizika tvrtke nakon provedbe sigurnosne inicijative. Efekti provedbe sigurnosne inicijative analizirani su u sedmom poglavlju, a utrošeni resursi raščlanjeni su u osmom poglavlju. Deveto poglavlje daje konačnu analizu troškova i koristi, nakon čega slijedi kratki zaključak.

1. TEMELJNI POJMOVI I KONTEKST RADA

1.1 Definicije temeljnih pojmova

Kibernetička sigurnost definira se kao „skup alata, pravilnika, sigurnosnih mjera, pristupa, smjernica, aktivnosti, akcija, obučavanja, najboljih praksi i tehnologije koja može zaštititi kibernetičko okruženje, organizaciju i imovinu korisnika“ [13].

Sustav upravljanja informacijskom sigurnošću tvrtke (engl. *Information Security Management Systems* – ISMS) definira se kao skup politika i postupaka za sustavno upravljanje osjetljivim podacima organizacije, a cilj ISMS-a je minimizirati rizik i osigurati kontinuitet poslovanja proaktivnim ograničavanjem utjecaja proboja sigurnosti [14].

Operatori ključnih usluga pojam je definiran u sklopu NIS Direktive [15], konkretizira i lokalno transponira u sklopu hrvatske „Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga“ [12], a obuhvaća državne i privatne tvrtke koje upravljaju nacionalnom kritičnom infrastrukturom u jednom o devet prepoznatih područja djelovanja (energetika, prijevoz, bankarstvo i infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura, poslovne usluge za državna tijela). Operatori su zakonskim tekstom obvezni „provoditi mjere za postizanje visoke razine kibernetičke sigurnosti za mrežni i informacijski sustav ili njegov dio o kojem ovisi pružanje ključne usluge subjekta“ [13]. Uvođenje ZTA u Energent d.o.o. je inicijativa primarno usmjerena na uspostavu upravo navedenih „mjere za postizanje visoke razine kibernetičke sigurnosti“ u Energent d.o.o.

Rizik se definira kao „vjerojatnost da se dogodi nesretni događaj pomnožena s mogućim utjecajem ili štetom nastalom događajem“ [16].

Procjena rizika se definira kao „identifikacija opasnosti koje bi mogle negativno utjecati na sposobnost organizacije da provodi svoje poslovne operacije“ [17]. Procjena rizika služi za identifikaciju raznih tipova rizika i „pružaju mjere, procese i kontrole za smanjenje utjecaja tih rizika na poslovne operacije“ [17].

Prihvatljivi rizik je „razina preostalog rizika za koju je utvrđeno da predstavlja razumnu razinu potencijalnog gubitka/prekida za određeni IT sustav“ [18].

Preostali rizik ili rezidualni rizik je definiran kao „rizik koji ostaje nakon što se kontrole uzmu u obzir“ [16].

Operativni IT rizik je definiran kao „poslovni rizik povezan s korištenjem, vlasništvom, radom, uključenošću, utjecajem i usvajanjem IT-a unutar tvrtke“ [19].

Utjecaj rizika je definiran kao „procjena štete koju bi rizični događaj mogao prouzročiti“ [16].

Vjerojatnost rizika je definirana kao „vjerojatnost da će se neki rizik ostvariti“ [16].

„**Katalog servisa**“ ili katalog usluga referentni je izvor točnih informacija o svim IT/OT uslugama koje nudi IT/OT odjel neke tvrtke. ITIL [20] definira katalog servisa kao „centraliziranu bazu podataka točnih informacija o aktivnim ponudama IT usluga i podskup portfelja usluga pružatelja IT usluga“. U Energentu d.o.o. ova definicija se standardno odnosi i na IT i na OT servise koji se koriste u organizaciji.

Servis je definiran kao „sredstvo za omogućavanje zajedničkog stvaranja vrijednosti olakšavanjem ishoda koje kupci žele postići“ [20]. U praktičnom smislu, riječ je o nekom IT/OT sustavu za koji poslovni korisnik s opravdanom poslovnom svrhom može dobiti licenci uz odgovarajući pristup, pri čemu servis ne uključuje samo aplikativno rješenje, nego i sve ostale komponente imovine nužne da bi taj servis prema poslovnom korisniku bio potpuno funkcionalan (hardver, softver, inženjeri, električna energija, fizički prostor za smještaj opreme, licence, ugovori o održavanju, poslovni podaci i slično).

Imovina je „svaka stavka od vrijednosti za dionike“ [18], odnosno sve ono što je potrebno da bi neki servis imao uredan produkcijski rad. Imovina može biti „materijalna (npr. fizička stavka kao što je hardver, računalna platforma, mrežni uređaj ili druga tehnološka komponenta) ili nematerijalna (npr. ljudi, podaci, informacije, softver, sposobnost, funkcija, usluga, zaštitni znak, autorska prava , patent, intelektualno vlasništvo, imidž ili ugled)“ [18].

Evidencija imovine se vode u IT/OT okruženjima kako bi se osiguralo „da organizaciji na učinkovit i isplativ način pružaju pogled na resurse koji su joj potrebni“ [21]. Podaci o imovini uključuju „lokaciju, korisnike, održavanje i podršku, dokumentaciju, izvedbu, licence, usklađenost, cijenu, fazu životnog ciklusa i drugo“.

Vlasnik rizika je „pojedinac koji je u konačnici odgovoran za osiguranje da se rizikom upravlja na odgovarajući način“ [22]. U Energentu d.o.o. ovo nije pojedinac, nego organizacijska jedinica na čelu s direktorom.

Vlasnik imovine u ISO 27001 odgovoran je za upravljanje svakodnevnom imovinom, kao što su elektronički podaci i tiskane kopije, kao i hardver, softver, usluge, ljudi i objekti. Vlasnik rizika odgovoran je za upravljanje prijetnjama i ranjivostima koje bi mogle biti iskorištene. U

slučaju tvrtke Energent d.o.o., svaki vlasnik imovine uvijek je organizacijska jedinica načelu s direktorom, a ta ista organizacijska jedinica uvijek je i vlasnik svih rizika vezanih uz predmetnu imovinu.

„Crveni" rizici je termin standardno u upotrebi unutar ISMS-a tvrtke, a odnosi se na „visoke" rizike, odnosno one rizike za koje je procjena rizika pokazala da imaju vrijednost između 6 i 9 sukladno korištenoj metodologiji procjene rizika Ministarstva financija [8]. Ovakve je rizike nužno tretirati jer im je visina neprihvatljivo visoka, a visoki broj „crvenih" rizika sugerira visokorizični profil organizacije ili njezinog dijela. U svim tablicama i grafičkim prikazima označeni su redovito crvenom bojom.

„Žuti" rizici je termin standardno u upotrebi unutar ISMS-a tvrtke, a odnosi se na „srednje" rizike, odnosno one rizike za koje je procjena rizika pokazala da imaju vrijednost 4 ili 5 sukladno korištenoj metodologiji procjene rizika Ministarstva financija [8]. Ovakve je rizike moguće, ali nije obvezno tretirati jer im je visina srednje visoka, a visoki broj „žutih" rizika sugerira srednje rizični profil organizacije ili njezinog dijela. U svim tablicama i grafičkim prikazima označeni su redovito žutom bojom.

„Zeleni" rizici je termin standardno u upotrebi unutar ISMS-a tvrtke, a odnosi se na „niske" rizike, odnosno one rizike za koje je procjena rizika pokazala da imaju vrijednost između 1 i 3 sukladno korištenoj metodologiji procjene rizika Ministarstva financija [8]. Ovakve rizike nije potrebno tretirati jer im je visina prihvatljivo niska, a visoki broj „zelenih" rizika sugerira niskorizični profil organizacije ili njezinog dijela. U svim tablicama i grafičkim prikazima označeni su redovito zelenom bojom.

Profil rizika je „kvantitativna analiza vrsta prijetnji s kojima se suočava organizacija, imovina, projekt ili pojedinac", a cilj mu je „pružiti nesubjektivno razumijevanje rizika dodjeljivanjem numeričkih vrijednosti varijablama koje predstavljaju različite vrste prijetnji i opasnosti koje predstavljaju" [23]. Svaka tvrtka ima u nekom trenutku svoj jedinstveni profil rizika „temeljen na imovini koju želi zaštititi, ciljevima koje želi postići, svojoj sposobnosti da se nosi s rizicima i svojoj spremnosti da to učini" [23].

Analiza troškova i koristi (engl. *cost-benefit analysis*) je „sustavni pristup procjeni snaga i slabosti alternativa", a koristi se za „određivanje opcija koje pružaju najbolji pristup postizanju koristi uz očuvanje ušteda u transakcijama, aktivnostima i funkcionalnim poslovnim zahtjevima" [26].

Troškovi implementacije IT/OT servisa uključuju izravne i neizravne troškove ulaganja u nabavu i implementaciju nekog servisa u poslovno okruženje tvrtke, od definicije ciljeva servisa, tehničkih i funkcionalnih zahtjeva do puštanja u produkcijski rad. Za potrebe ovog rada, u neizravne troškove uključeni su troškovi satnice vlastitih radnika koji su sudjelovali u procesu implementacije, dok su u izravne troškove uključeni ugovorni troškovi vanjskih partnera koji su angažirani za nabavu opreme i implementacijske i integracijske troškove uvođenja predmetnog servisa.

Troškovi održavanja IT/OT servisa uključuju izravne i neizravne troškove održavanja nekog servisa u produkcijskom radu unutar poslovnog okruženja tvrtke, od puštanja u produkcijski rad do gašenja servisa. Za potrebe ovog rada, u neizravne troškove uključeni su troškovi satnice vlastitih radnika koji su sudjelovali u procesu održavanja, dok su u izravne troškove uključeni ugovorni troškovi vanjskih partnera koji su angažirani za održavanje predmetnog servisa.

Koristi implementacije IT/OT servisa je vrlo teško izravno kvantificirati jer većina servisa, odnosno u užem smislu tehničkih kontrola povezanih sa sigurnošću nema izravnu vezu sa novčanim vrijednostima realizacije rizika, odnosno teško je napraviti konzistentnu procjenu što u novčanim vrijednostima znači ako se neki sigurnosni sustav (servis) uvede ili ne za tvrtku. Za potrebe ovog rada promatran je sigurnosni profil tvrtke prije i poslije uvođenja pojedinog servisa u sklopu implementacije ZTA, te je usporedbom brojčanih vrijednosti sigurnosnog profila tvrtke prije i poslije uvođenja ZTA dobiven „pomak“, odnosno smanjenje vrijednosti rizika cijele tvrtke. Taj „pomak“ predstavlja ključnu korist implementacije cijele ZTA inicijative, a kumulativni „pomak“ nakon implementacije svih deset projekata predstavlja korist implementacije ZTA za tvrtku.

Tehnički voditelji su inženjeri od uprave tvrtke zaduženi za ispravan tehnički rad pojedinih servisa. Kao najbolji poznavatelji arhitekture pojedinih servisa, ovo su osobe tehnički kompetentne da provode procjene rizika i implementiraju korektivne radnje nad servisima.

Poslovni koordinatori su poslovni korisnici zaduženi za ispunjenje poslovnih očekivanja pojedinih servisa. Za deset sigurnosnih servisa implementiranih u sklopu sigurnosne inicijative, riječ je o inženjerima koji vrlo kvalitetno poznaju poslovne procese vezane uz svoje servise, te su zato sudjelovali u procjeni rizika i implementaciji korektivnih radnji nad servisima.

Korektivne i preventivne radnje definirane su kao „poboljšanja procesa organizacije koja se poduzimaju kako bi se uklonili uzroci nesukladnosti ili drugih neželjenih situacija“ [27]. Konkretno, korektivne radnje su „radnje poduzete za uklanjanje uzroka nesukladnosti ili drugih

neželjenih situacija, kako bi se spriječilo njihovo ponavljanje“ [27], dok su preventivne radnje „radnje poduzete kako bi se spriječila pojava takvih nesukladnosti, općenito kao rezultat analize rizika“ [27]. Za potrebe ovog rada, sve promatrane radnje diskutirane su kao korektivne radnje.

Nezavisna korektivna radnja termin je koji se standardno koristi u ISMS dokumentaciji i procesima tvrtke, a definira se kao korektivna radnja s jedinstvenim uzrokom rizika koji druge korektivne radnje ne dijele.

Tehnički dug definira se kao „trošak dodatne prerade izazvan izborom najbržeg rješenja, a ne najučinkovitijeg rješenja“ [28]. Iako je tehnički dug pojam izvorno kreiran za područje razvoja softvera, on se danas koristi i za slučajeve gdje organizacija donese nekvalitetnu stratešku odluku koja joj se čini oportuna danas (npr. nećemo uvesti novu verziju operativnog sustava nego ćemo zadržati stare Windowse; produljit ćemo vijek upotrebe poslužitelja sa pet na osam godina), ali ta odluka može donijeti mnoge probleme u vrlo bliskoj budućnosti (npr. stari Windowsi brzo izgube podršku proizvođača i time postanu ranjivi na javno objavljene sigurnosne ranjivosti; poslužitelji se počnu više kvariti, dijelovi im postanu teže dobavljivi, održavanje im postane značajno skuplje) i traži više vremena i veća sredstva za popravak takve loše odluke nego da se odmah donijela kvalitetna odluka.

1.2 Opseg rada, ograničenja i pretpostavke

Tijekom izrade ovog rada korištene su sljedeće pretpostavke u opsegu rada, sigurnosti, metodologije procjene rizika, financija, metodologije analize troškova i koristi, ograničenja mjerenja, odobravanja i verifikacija prikupljenih podataka, te ostale pretpostavke.

1.2.1. Opseg

Predmet razmatranja je sama tvrtka Energent d.o.o., bez povezanih društava i tvrtki kćeri. Od svih rizika koje je moguće identificirati u okruženju rada tvrtke Energent d.o.o., ovaj rad će razmatrati samo operativne ICT rizike, dok druge vrste rizika poput strateških i druge vrste operativnih rizika poput financijskih neće biti uzimani u razmatranje. Sama definicija i opseg pojma sigurnosne inicijative kako je korišten u ovom radu jasno su postavljeni u odgovarajućoj sekciji rada (2.7). Strukturirani intervjui održani su putem elektroničke pošte, a obuhvatili su dvije osobe najpozvanije da izvrše tražene procjene:

- rukovoditelja IT okruženja tvrtke
- rukovoditelja OT okruženja tvrtke.

1.2.2. Sigurnost

Zbog sigurnosno osjetljive tematike rada, poduzeti su određeni koraci u svrhu anonimizacije i pseudonimizacije izrađenih analiza i to kako slijedi:

- tvrtka poslodavac autora ovog rada je preimenovana u Energent d.o.o.
- imena svih servisa su preimenovana su da bi se sakrilo ime proizvođača tehnologije i funkcija samih servisa (npr. „3Com mreža“ bio bi preimenovan u „Servis broj 32“)
- evidencija imovine nije deklarirana na nivou konfiguracijske jedinice (engl. *configuration item* - CI) na kojem je to učinjeno unutar same tvrtke kao osnovne jedinice imovine sukladno biblioteci najboljih praksi za upravljanje IT uslugama (engl. *Information Technology Infrastructure Library* – ITIL), već je imovina anonimizirana kroz korištenje „servisa“ kao najniže konfiguracijske jedinice imovine i nad servisima su provedene procjene rizika
- nisu iskazana imena i prezimena ljudi koji su ispunjavali ankete, odnosno sudjelovali u procjeni rizika, već su umjesto toga iskazane njihove uloge u organizaciji; voditelji IT službe i OT službe nisu autoru dali svoju suglasnost da se njihova imena objave u sklopu ovog rada.
- nisu iskazani konfiguracijski parametri za licenciranje pojedinih projekata unutar sigurnosne inicijative (broj korisnika, memorijsko zauzeće, broj virtualnih poslužitelja, diskovni prostor, broj i vrsta licenci…)
- nisu referencirani na odgovarajući način podaci preuzeti iz profila tvrtke ili njezinih financijskih izvješća jer bi se tako izravno imenovala tvrtka, ali je u takvim slučajevima na početku potpoglavlja jasno naznačeno da su podaci preuzeti iz korporativnih materijala.

1.2.3. Metodologija procjene rizika

Upotrijebljena metodologija procjene rizika je krajnje jednostavna za primjenu i to do te mjere da je u svojoj jednostavnosti smanjeno precizna u izražavanju rizika za pojedinu prijetnju. Metodologija procjene rizika ima inherentnu osobinu da će da će veliki broj rizika biti evaluiran kao „žuti“ odnosno granično prihvatljiv, ili „crven“ odnosno neprihvatljiv. Razlog je u samoj metodologiji, odnosno matematičkoj činjenici da množenje vjerojatnosti i utjecaja s minimalnim vrijednostima „jedan“ i maksimalnim vrijednostima „tri“ daje samo sedam mogućih ishoda evaluacije rizika za neku kombinaciju „vjerojatnost x utjecaj“ (1, 2, 3, 4, 6, 8,

9) od kojih se dva (4,6) smatraju „žutim“ rizicima i dva (8,9) „crvenim“ rizicima, što upućuje na očekivano veliki broj „žutih“ i „crvenih“ rizika u konačnoj matrici upravljanja rizicima za sve rizike iz „Kataloga rizika“ aplicirane na sve servise iz „Kataloga servisa“. Velika većina žutih rizika tretirana je u obje provedene procjene rizika kao prihvatljiva i na njima se uglavnom nisu otvarale korektivne radnje, a što sama metodologija upravljanja rizicima ni na koji način ne zabranjuje.

1.2.4. Financije

Kod izračuna ukupnog troška vlasništva (engl. *Total Cost of Ownership* - TCO) uvođenja sigurnosne inicijative, uzimale su se u obzir sljedeće pretpostavke:

- troškovi svakog sastavnog dijela sigurnosne inicijative sastoje se od:
  - projektnih izravnih troškova uvođenja u poslovanje
  - izravnih troškova održavanja tijekom prvih pet godina produkcijskog rada
  - troškova plaća radnika tvrtke za sudjelovanje u projektnom uvođenju
  - troškova plaća radnika tvrtke za sudjelovanje u održavanju tijekom prvih pet godina produkcijskog rada
- srednja mjesečna plaća prosječnog radnika u IT i OT tehničkim službama je 18.000,00 kuna u bruto iznosu kao trošak poslodavca, a radi pojednostavljenja pretpostavka je da će se da je ovo konstanta kroz cijeli izračun jer će se eventualni porast plaća kompenzirati odljevom najboljih i najskupljih radnika i zapošljavanjem slabije plaćenih zamjena, a što se u promatranom razdoblju 2018.-2022. pokazalo kao točna pretpostavka jer su plaće na tržištu rasle bitno brže od plaća u državnom poduzeću, pa su najbolji ljudi redovno odlazili (utjecaj ovog trenda na profil rizika tvrtke je bio minimalan jer se tvrtka praktično u potpunosti okrenula korištenju vanjskih partnera za sve ključne procese oko brige o servisima)
- radni mjesec sadrži 22 radna dana
- trošak održavanja licenci kroz period od pet godina računat će se tako da će se upotrijebiti stvarni trošak korištenja kupljenih licenci u periodu od pet promatranih godina
- svi projekti definirani u opsegu sigurnosne inicijative izvodit će se i u IT i u OT okruženju tvrtke osim gdje to tehnički nema smisla implementirati; npr. OT služba nema vlastita klijentska računala i sustav odgovora na prijetnje putem automatizirane reakcije na prijetnju (engl. *Endpoint Detection and Response* – EDR) nego oboje koristi putem usluga IT službe
- inflatorni učinak na cijene tijekom razdoblja od pet godina je ispao zanemariv za sve praktične potrebe ovog rada [6], ali je bez obzira na to uključen u sve iskazane troškove.

Tvrtka je osnovnim ugovorom uvijek kupila licence s obveznom prvom godinom održavanja i projektne usluge, te obvezno drugu i treću godinu održavanja licenci, a potom bi prije isteka inicijalnog ugovora ugovorila u jedinstvenom ugovoru četvrtu i petu godinu održavanja licenci. Obzirom da su svi ugovori provedeni i financijski realizirani, razumno je zaključiti da su svi eventualni inflatorni učinci sadržani u ugovornim cijenama. Iako je 2022. godina kao zadnja godina promatranog petogodišnjeg razdoblja imala značajnu inflaciju prije objava službenih podataka procijenjenu na 13,5% [7], ovo nije imalo učinka na trošak Energenta d.o.o. jer su održavanja licenci za period 2021.-2022. ugovarana u drugoj polovici 2020. godine.

- trošak amortizacije na rok od pet godina je nula jer su svi projekti ugovoreni i isporučeni kao servisi u oblaku odnosno samo usluge, bez kapitalnih ulaganja na koje bi se amortizacija mogla primjenjivati; ovo je vidljivo u tablici 12. (procjena rizika nakon sigurnosne inicijative) gdje su servisi sigurnosne inicijative označeni ID oznakama SISZIOP-054 do SISZIOP-063, oznaka kategorije servisa je svugdje „aplikacija u oblaku“)
- prosječni trošak održavanja licenci je oko 20% godišnje, što uključuje trošak proizvođačkog održavanja licenci i radove ugovornog partnera vezane uz održavanje licenci
- rukovoditelji IT i OT službe su prije formiranja i ispunjavanja strukturiranog upitnika potvrdili da nemaju konkretne financijske podatke o zahtjevima za promjenu koji su provedeni nad promatranim servisima tijekom petogodišnjeg razdoblja jer su isti provedeni kroz više različitih modela (zasebne narudžbenice, prenamijenjeni budžeti, kroz slične ugovore s istim partnerima), no suglasni su da je riječ o zanemarivim iznosima koji kumulativno svakako ne dosežu 40.000,00 eura u pet godina, pa zbog relativno niskog procijenjenog iznosa i praktične nedostupnosti čvrstih podataka nisu posebno uključeni u analize u ovom radu
- riječ „vlasništvo“ tu treba shvatiti uvjetno, odnosno kao povijesni pojam jer pojedine tehnologije sigurnosne inicijative nisu licencirane po modulu kupovine, već najma, no to ni na koji način ne mijenja metodologiju rada
- za potrebe konverzije kunskih iznosa u eure korišten je tečaj 1 EUR = 7,53 kuna, a euro je korišten kao referentna valuta za usporedbu financijskih iznosa u ovog radu.

1.2.5. Metodologija analize troškova i koristi

Ovaj rad koristi logiku kojom su sve promjene u profilu rizika tvrtke u promatranom petogodišnjem razdoblju rezultat isključivo provedbe sigurnosne inicijative. Korištena je premisa da je sigurnosna inicijativa za implementaciju ZTA nositelj svih pomaka u profilu rizika u tvrtki jer je u promatranom periodu bila jedina inicijativa tvrtke usmjerena na povećanje kibernetičke sigurnosti. No unutar relativno dugog razdoblja od pet godina puno drugih događaja (rat u Ukrajini, rast cijena ugljikovodika u svijetu, promjene uprava u tvrtki, povećanje regulirane tarife o kojoj ovise prihodi tvrtke 2020. godine rezultiralo je dizajniranjem projekata sa kvalitetnijim i skupljim tehnologijama) u unutrašnjem i vanjskom kontekstu moglo je imati utjecaj na profil rizika, a korištena metodologija nema mogućnost procijeniti koliki pomak u profilu rizika snosi provedba sigurnosne inicijative, a koliko drugi nezavisni događaji u kontekstu organizacije. Da bismo dokazali premisu da je sigurnosna inicijativa jedini nositelj promjene u profilu rizika tvrtke tijekom promatranog razdoblja bilo bi potrebno koristiti kao kontrolnu skupinu sličnu tvrtku koja se bavi istom djelatnošću, a koja u promatranom razdoblju nije provodila sigurnosnu inicijativu. Takve tvrtke na hrvatskom tržištu jednostavno nema jer je Energent d.o.o. monopolist. Obzirom da smo proveli analizu i mjerenja bez korištenja kontrolne skupine, ovdje moramo ostaviti mogućnost da je u ovoj metodologiji prisutna određena pristranost (engl. *bias*).

1.2.6. Mjerenja, odobravanja i verifikacija prikupljenih podataka

Provedbu procjene rizika iznijeli su tehnički voditelji i poslovni koordinatori, zapise o provedenoj procjeni rizika u oba slučaja odobrili su rukovoditelji IT i OT službi, a potvrdila ih je i prihvatila uprava tvrtke posebnim odlukama (svake godine).

Verifikacija projektnog upravljanja nad uvođenjem tehničkih kontrola u sklopu sigurnosne inicijative i samih zapisa o provedenoj procjeni rizika bili su u promatranom petogodišnjem razdoblju predmet interne kontrole (četiri puta), interne prosudbe informacijske sigurnosti prema ISO27001:2013 (četiri puta redovno i jednom izvanredno), vanjske prosudbe kibernetičke sigurnosti (tvrtka Bureau Veritas, četiri puta) te zakonske vanjske revizije (eng. *audit*) kibernetičke sigurnosti od strane ZSIS-a (tri puta).

Podaci prikupljeni putem strukturiranih intervjua nisu posebno verificirani jer su prikupljeni izravno do odgovornih osoba (rukovoditelji IT i OT službi).

1.2.7. Ostalo

Autor rada je ujedno i autor svih tablica i grafova sadržanih u ovom radu.

Korišten je pojam „korektivne radnje“ i za stvarne korektivne radnje i za preventivne radnje za rizike koji se još nisu realizirali, a u svrhu pojednostavljenja relativno složene terminologije korištene u ovom radu.

1.3 Korištene metodologije, metrike i alati

U srži ovog specijalističkog rada je procjena isplativosti uvođenja složene sigurnosne inicijative kroz proces analize troškova i koristi. Uspoređuju se resursi potrebni za implementaciju sigurnosne mrežne ZTA kroz seriju složenih projekata povezanih u jedinstveni projektni program (u daljnjem tekstu: sigurnosna inicijativa) sa, uvjetno govoreći, „koristima“ u profilu rizika koje će Energent d.o.o. dobiti implementacijom ZTA. S obzirom na to da je riječ o usporedbi kvantificiranih troškova (vrijeme, plaće, projekti) s promjenama u profilu rizika koja je po svojoj prirodi nematerijalni podatak, konačna usporedba bit će izvedena koristeći iskustvo samog autora rada u ovoj problematici temeljem provedenih anketa s ključnim operativnim voditeljima IT i OT okruženja u Energentu d.o.o., te komparacijom sljedećih deset objektivnih metrika za usporedbu profila rizika prije i poslije implementacije sigurnosne inicijative. Ove metrike predstavljaju uobičajeni način kvantitativne usporedbe atributa profila rizika tvrtke iz godinu u godinu i sastavni su dio izvješća koje nadležnim državnim tijelima tijekom zakonskih redovnih audita tvrtka predaje kao dokaz trendova u upravljanju rizicima, pa su iste metrike korištene i za potrebe ovog rada:

1. prosječna vrijednost rizika po servisu: predstavlja indikator generalnog stanja rizika za neki servis (jedinica mjere je vrijednost rizika u bodovima; mogući raspon 1-9, manje je bolje)
2. maksimalna razlika u prosječnom riziku dva servisa: predstavlja mjeru raspršenosti rizika po različitim rizicima, odnosno daje uvid u maksimalno odstupanje u rizičnosti za dva rizika tvrtke (jedinica mjere je vrijednost rizika u bodovima; mogući raspon 1-9, manje je bolje)
3. prosječni broj "crvenih" rizika po servisu: predstavlja mjeru rizičnosti za sve rizike u „Katalogu rizika“ gdje veliki prosječni broj „crvenih“ rizika ukazuje na visoku mjeru rizičnosti u prosjeku za sve servise tvrtke (manje je bolje)

4. prosječni broj "žutih rizika" po servisu: predstavlja mjeru rizičnosti za sve rizike u „Katalogu rizika“ gdje veliki prosječni broj „žutih“ rizika ukazuje na visoku mjeru rizičnosti u prosjeku za sve servise tvrtke (manje je bolje)
5. udjel "crvenih" rizika u ukupnim rizicima: predstavlja mjeru rizičnosti za sve rizike u „Katalogu rizika“ gdje veliki prosječni broj „crvenih“ rizika ukazuje na visoku mjeru rizičnosti u prosjeku za sve servise tvrtke (postotak; raspon 0-100%, manje je bolje)
6. udjel "žutih" rizika u ukupnim rizicima: predstavlja mjeru rizičnosti za sve rizike u „Katalogu rizika“ gdje veliki prosječni broj „žutih“ rizika ukazuje na visoku mjeru rizičnosti u prosjeku za sve servise tvrtke (postotak; raspon 0-100%, manje je bolje)
7. prosječan broj korektivnih radnji po servisu: predstavlja mjeru rizičnosti za sve rizike u „Katalogu rizika“ gdje veliki prosječni broj korektivnih ukazuje na visoku mjeru rizičnosti u prosjeku za sve servise tvrtke (manje je bolje)
8. ukupan broj nezavisnih korektivnih radnji: predstavlja mjeru rizičnosti gdje veliki broj nezavisnih korektivnih radnji ukazuje na potrebu u za većim brojem zahvata kojima će se otkloniti uzroci rizika (manje je bolje)
9. prosječna financijska vrijednost nezavisne korektivne radnje: predstavlja mjeru rizičnosti gdje velika prosječna vrijednost nezavisne korektivne radnje ukazuje da su uzroci rizika teže prirode i traže veća sredstva da bi ih se otklonilo (manje je bolje)
10. ukupna vrijednost nezavisnih korektivnih radnji predstavlja mjeru rizičnosti gdje velika ukupna financijska vrijednost nezavisnih korektivnih radnji ukazuje da su uzroci rizika teže prirode, odnosno da ih tih uzorka veći broj i da ih je skuplje ukloniti (euro; manje je bolje).

Proces usporedbe koja je korišten tijekom izrade ovog specijalističkog rada uključuje tri diskretna koraka:

1. definicija profila rizika kojima je Energent d.o.o. trenutno izložen u smislu rizika informacijskih i komunikacijskih tehnologija (engl. *information and communication technology* – ICT) u stanju implementiranih tehničkih kontrola i procesa kibernetičke sigurnosti na samom početku 2018. godine
2. definicija profila rizika kojima će Energent d.o.o. biti izložen na samom kraju 2022. godine u smislu ICT rizika u stanju implementiranih tehničkih kontrola i procesa kibernetičke sigurnosti kroz uvođenje ZTA

3. usporedba očekivane pozitivne promjene u profilu rizika tvrtke i za to procijenjenog utroška resursa, analiza opravdanosti pokretanja projekta pod takvim okolnostima, te razmatranje u kojoj bi situaciji i okolnostima te sigurnosne inicijative bilo opravdano.

Za potrebe provedbe koraka 1. i 2., odnosno za sve potrebe analize i upravljanje rizicima korištena je kvazi-kvantitativna metodologija Ministarstva financija Republike Hrvatske. Definirana dokumentom „Smjernice za upravljanje rizicima u poslovanju institucija javnog sektora, verzija 2.0.“ [8]. Ova metodologija je namijenjena institucijama koje sukladno „Zakonu o sustavu unutarnjih kontrola u javnom sektoru“ imaju obvezu uspostaviti i razvijati upravljanje rizicima, a što među ostalima uključuje trgovačka društva i druge pravne osobe utvrđene u Registru trgovačkih društava i drugih pravnih osoba obveznika davanja „Izjave o fiskalnoj odgovornosti“ koji objavljuje Ministarstvo financija. Ukratko, metodologija je bazirana na evaluaciji vjerojatnosti i utjecaja za svaku promatranu prijetnju nad nekom imovinom (u ovom slučaju servisom), dakle riječ je o matrici rizika. Za razliku od recimo BS 7799-3:2017 [9], treba uočiti da ova metodologija ne uzima u obzir vrijednost imovine (engl. *asset value*) kao faktor u procjeni rizika što svakako ne doprinosi dobivaju jasnije slike o stanju rizika nad pojedinim servisom. Možda je ova metodologija najbliža onome što preporuča američki NIST u svojim uputama za provedbu procjene rizika [10] gdje se također kao varijable koriste isključivo vjerojatnost i utjecaj, no NIST proces dozvoljava po pet različitih vrijednosti ulaznih varijabli koji onda rezultiraju u kvazi-kvantitativne vrijednosti rizika 0-4, 5-20, 21-79, 80-95 i 96-100 te dvadeseti pet različitih diskretnih vrijednosti rizika. Kod metodologije Ministarstva financija nije posebno sretan odabir skale kojom se dozvoljene vrijednosti obje varijable definiraju od jedan do tri iako je sama metodologija dozvoljavala i drukčija rješenja, no Energent d.o.o. je ovaj odabir usvojio odlukom svoje uprave kako bi što jednostavnije svojim radnicima približio proces procjene rizika. Time se kao izlaz procesa procjene rizika dobivaju vrlo grubo granulirane vrijednosti rizika gdje imamo samo sedam diskretnih stanja koje vrijednost rizika može poprimiti (1, 2, 3, 4, 6, 8, 9), što onda naravno daje relativno brz rezultat, ali sa slabom vidljivosti rizika (engl. *visibility*). Obzirom da je metodologija Ministarstva financija bila zadana odlukom uprave tvrtke, ona je korištena u ovom radu jer nije bilo praktičnog načina da autor rada tehničkim voditeljima i poslovnim koordinatorima, dakle ljudima koji su zaista provodili procjene rizika, preporuči odnosno uvjetuje neku drugu metodologiju.

Metrika rizika predstavlja sustav prikupljanja, procjene, mjerenja i usporedbe rezultata koji ukazuju na način, rezultata, uvjete i posljedice koje nastaju radi djelovanja čimbenika rizika.

Za potrebe izrade ovog rada i procjene rizika, te evaluaciju potrebnih korektivnih radnji korištene su smjernice i pragovi sadržani u dokumentu tehničkog tijela za ocjenu sukladnosti operatorima ključne usluge u energetskom sektoru, tvrtke „Zavod za sigurnost informacijskih sustava“ (ZSIS). Dokument se zove „Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama 'Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga' i provođenje ocjene sukladnosti“ iz listopada 2019. godine [11], a njegova primjena predmet je audita od strane ZSIS-a koji se provodi jednom u maksimalno dvije godine. Dokument nije obvezujući i osnovna mu je namjena služiti kao implementacijski vodič za operatore kritične infrastrukture prilikom ostvarivanja sukladnosti s mjerama sigurnosti, ali istodobno i kao vodič za nadležna sektorska tijela, tehnička tijela za ocjenu sukladnosti, vanjske i interne revizore koji će provoditi nadzor sukladnosti kod tzv. operatora ključnih usluga [12]. Konačna evaluacija rizika dobivena na ovaj način ukazuje da je riječ o kvazi kvantitativnoj metodi koja se bazira na egzaktno mjerenim, odnosno procijenjenim metrikama, no konačni „izlaz“ ne odgovara na pitanje o financijskim vrijednostima realizacije pojedinih rizika, pa ne možemo govoriti o kvantitativnoj metodi u pravom smislu tog pojma.

1.4 Postupak procjene rizika sukladno odabranoj metodologiji

1.4.1. Utvrđivanje vjerojatnosti realizacije rizika

Utvrđivanje vjerojatnosti realizacije rizika sukladno odabranoj metodologiji definirana je sljedećom tablicom vjerojatnosti, pri čemu su kao izvor podataka služili povijesni podaci podrške (engl. *help desk*) tvrtke. Za svaki rizik potrebno je odrediti vjerojatnost njegovog ostvarenja, koristeći sljedeću skalu vjerojatnosti ostvarenja rizika.

Tablica 1 - Tablica vjerojatnosti realizacije rizika

Tablica vjerojatnosti realizacije rizika	1	1- Niska vjerojatnost	Vrlo nevjerojatni događaji, nema primjera da su se dogodili u našim okolnostima, najviše jednom u 10 godina
	2	2 - Srednja vjerojatnost	Vjerojatan događaj, slični incidenti događaju se otprilike barem 2x u 10 godina
	3	3 - Visoka vjerojatnost	Dogodit će se u bliskoj budućnosti, događa se 1x godišnje ili češće

1.4.2. Utvrđivanje utjecaja realizacije rizika

Utvrđivanje utjecaja realizacije rizika sukladno odabranoj metodologiji definirana je sljedećom tablicom utjecaja, pri čemu su kao izvor podataka služili povijesni podaci podrške, odnosno dnevnicima (eng. *log*) korektivnih i preventivnih radnji gdje se vodi evidencija o troškovima implementacije pojedine korektivne ili preventivne radnje. Za svaki rizik potrebno je odrediti utjecaj njegovog ostvarenja, koristeći sljedeću skalu utjecaja ostvarenja rizika.

Tablica 2 - Tablica utjecaja realizacije rizika

Tablica utjecaja realizacije rizika	1	1 - Nizak utjecaj	Financijski gubitak manji od 200.000 kn ili nema štete za ugled
	2	2 - Srednji utjecaj	Financijski gubitak između 200.000 kn i 2.000.000 kn ili negativni medijski natpisi, prilozi u jednom izdvojenom mediju, ogovaranja na tržištu bez argumenata
	3	3 - Visok utjecaj	Ljudske žrtve ili ozljede; ili financijski gubitak barem 2.000.000 kn ili negativni medijski natpisi, prilozi u nacionalnom dnevnom tisku, uglednim poslovnim magazinima, Internet portalima, televiziji

1.4.3. Mjerenje i određivanje rizika

Jednom kad su za svaku krupu informacijske imovine određeni faktori vjerojatnosti i utjecaja, jednostavnim množenjem ovih faktora dobiva se faktor rizika, pojednostavljeno rizik za tu grupu imovine i prateću prijetnju. Sukladno metodologiji koju koristimo, maksimalni rizik je devet. Ovisno o tome koji je dobiveni umnožak (rizik), vlasnik rizika će imati jasnu sliku o idućim potezima koji se od njega očekuju. Ako je umnožak vjerojatnosti i utjecaja „crven“ (šest i veći), takav rizik nije prihvatljiv i mora se tretirati. Ako je umnožak vjerojatnosti i utjecaja žut (tri ili četiri), takav rizik je prihvatljiv i ne mora se tretirati, ali je preporučljivo inicirati tretman kroz odgovarajuću korektivnu/preventivnu radnju te je odluka ostavljena vlasniku rizika. Ako je umnožak vjerojatnosti i utjecaja „zelen“ (jedan ili dva), takav rizik je prihvatljiv i ne mora se tretirati.

Tablica 3 - Matrica rizika

MATRICA RIZIKA		Vjerojatnost		
		1	2	3
Utjecaj	3	3	6	9
	2	2	4	6
	1	1	2	3

1.4.4. Maksimalna prihvatljiva razina rizika

Maksimalna prihvatljiva razina rizika za Energent d.o.o. je 5, a definirana je odgovarajućom odlukom uprave tvrtke koja je dio ISMS sustava. Svi rizici veći od pet smatraju se neprihvatljivo visokima i zahtijevaju dodatnu analizu i utvrđivanje korektivnih mjera za tretman tih rizika. Kuriozitet je da se ishod „pet“ ne može matematički dobiti kao vrijednost rizika nad nekim servisom jer je rizik prema korištenoj metodologiji umnožak vjerojatnosti (1-3) i utjecaja (1-3), iz čega je razvidno da pet nije moguć ishod operacije množenja. Za sve praktične potrebe i u svrhu ovog rada, rizici koji zahtijevaju otvaranje korektivne radnje su „crveni“ rizici s vrijednostima rizika šest ili devet.

1.4.5. Povjerljivost imovine

Temeljem podataka koji su prikupljeni kroz navedene aktivnosti, za svaku grupu imovine odredit će se nivo provjerljivosti informacijske imovine koristeći prikladnu skalu kojom je definirano što pojedini nivo provjerljivosti označava, odnosno koju vrstu utjecaja može imati na tri atributa sigurnosti pojedine grupe informacijske imovine (povjerljivost, cjelovitost, raspoloživost) [29]. Podaci će se vrednovati uzimajući u obzir najgori mogući scenarij u svakom razmatranom slučaju.

Tablica 4 - Klasifikacija povjerljivosti informacijske imovine

KRITIČNOST	POVJERLJIVOST	CJELOVITOST	RASPOLOŽIVOST
VISOKO KRITIČNO	Najosjetljivije informacije iz poslovanja odnosno	Informacije čija cjelovitost ne	Informacije koje moraju biti raspoložive unutar 4

Tajno (za povjerljivost)	sve informacije koje su zakonom, drugim propisom, općim ili drugim aktom donesenim na temelju zakona, određene tajnima	smije biti narušena ni u kojem slučaju	sata od zahtjeva za informacijom
KRITIČNO Povjerljivo (za povjerljivost)	Osjetljive informacije iz poslovanja	Informacije čije narušavanje cjelovitosti može uzrokovati manje financijske gubitke, ili dovesti do negativnog publiciteta u manjoj mjeri onemogućiti pružanje usluga i odvijanje poslovnih procesa	Informacije koje moraju biti raspoložive unutar 48 sati (2 radna dana) od zahtjeva za informacijom
NORMALNO Interno (za povjerljivost)	Informacije za internu uporabu u okviru poslovnih procesa odnosno informacije nužne za vršenje dnevnih aktivnosti	Sve ostale informacije koje nemaju posebnih zahtjeva za cjelovitošću i mogu se jednostavno i brzo nabaviti iz drugih izvora a njihova promjena ne izaziva osobito štetne posljedice.	Informacije koje moraju biti raspoložive unutar tjedan dana od zahtjeva za informacijom a ne narušavaju ugled i imidž te odvijanje procesa i pružanje usluga korisnicima no utječu na pad performansi sustava.

Javno (za povjerljivost)	Informacije dostupne široj javnosti		

Vidljivo je i da pojedini dijelovi imovine sadrže osobne podatke, što onda te servise čini i obradama osobnih podataka u smislu „Zakona o zaštiti osobnih podataka“ [30], a što zbog mogućih posljedica u slučaju ostvarenja rizika krađe podataka svakako utječe na profil rizika tih servisa. Potrebno je napomenuti da su ova četiri nivoa provjerljivosti korištena *ad hoc* tijekom prve procjene rizika 2018. godine, odnosno nije postojao nikakav pisani dokument odnosno formalna skala po kojoj bi se proces jednoznačno definirao i uniformirao za sve dionike koji su provodili samu procjenu rizika. Time je krajnji rezultat uistinu dao četiri navedena nivoa provjerljivosti, no kroz proces koji nije garantirao ponovljivost i konzistentnost jer je tek usmeno komuniciran dionicima. Tak tijekom 2022. godine, autor rada je formalizirao ovaj proces procjene povjerljivosti servisa kroz interne dokumente tvrtke, a koristeći materijale (poglavito gornju tablicu) koje je susreo na postdiplomskom studiju „Informacijske sigurnosti“ na FER-u Zagreb tijekom 2022. godine. Procjena rizika provedena nakon provedbe sigurnosne inicijative krajem 2022. godine pratila je ovaj proces i krajnji rezultat kategorizacije povjerljivosti svakog pojedinog servisa je svakako pouzdaniji i konzistentniji od onog iz 2018. godine.

1.4.6. Prikupljanje podataka i zaduženja

Prikupljanje podataka je izvršeno u razdoblju od lipnja 2021. (prije početka implementacije sigurnosne inicijative) do studenog 2022. (dovršena implementacija sigurnosne inicijative) Slijedi popis provedenih aktivnosti prikupljanja podataka korištenih u ovom radu, s naznakom procjene utrošenih čovjek-sati za svaku pojedinu aktivnost:

- procjenu rizika za servise IT službe u godinama 2018. (redovna procjena) i 2022. (izvanredna procjena), dodatno uključujući određivanje povjerljivosti pojedinih servisa; ukupno utrošeno 275,5 čovjek-sati
- procjenu rizika za servise OT službe u godinama 2018. (redovna procjena) i 2022. (izvanredna procjena) dodatno uključujući određivanje povjerljivosti pojedinih servisa; ukupno utrošeno 314,0 čovjek-sati
- analizu podataka/informacija iz planskih dokumenata tvrtke, izvještaja, primjenjive regulative; ukupno utrošeno 5 čovjek-sati

- analizu podataka iz *help deska;* ukupno utrošeno 1,5 čovjek-sati
- analizu podataka iz logova preventivnih i korektivnih radnji; ukupno utrošeno 6,5 čovjek-sati
- analizu izvješća unutarnje i vanjske revizije; ukupno utrošeno 1,5 čovjek-sati
- analizu podataka iz profila i financijskih izvješća tvrtke; ukupno utrošeno 2,0 čovjek-sata
- ugovore o nabavi IT i OT službi; ukupno utrošeno 5,5 čovjek-sati
- ugovore o održavanju IT i OT službi; ukupno utrošeno 2,0 čovjek-sati
- ispunjavanje strukturiranih upitnika od strane rukovoditelja IT i OT službi (priloženo kao Dodatak 3); ukupno utrošeno 7,0 čovjek-sati.

Autor rada je kroz svoju funkciju u tvrtki mogao samostalno pristupiti podacima iz planskih dokumenata tvrtke, izvještaja i primjenjive regulative, profila i financijskih izvješća tvrtke, logova korektivnih i preventivnih radnji, te izvješćima unutarnje i vanjske revizije. Podaci iz *help deska* i procjene rizika dobiveni su od rukovoditelja IT službe i rukovoditelja OT službe. Potrebno je napomenuti da su oba rukovoditelja sa tehničkim voditeljima i poslovnim koordinatorima morali napraviti izvanrednu procjenu rizika za sve svoje servise na kraju 2022. godine jer bi se redovna procjena rizika čekala do travnja 2023. što nije dolazilo u obzir obzirom na rokove izrade ovog rada. Posebno kvalitetni i upotrebljivi ulazni podaci dobiveni su također od rukovoditelja IT i OT službe kroz ispunjavanje strukturiranog upitnika, a kojim su iskazani svi traženi financijski iznosi vezani uz desetke ugovora o nabavi i ugovora o održavanju, te procjene utroška vremena vlastitih radnika na poslovnima implementacije i održavanja pojedinih servisa. Finalne korekcije financijskih parametara (troškovi korektivnih radnji, troškovi implementacije i održavanja servisa) dopunjeni kroz email komunikaciju sa rukovoditeljima IT i OT službi su kroz studeni 2022. kad su svi relevantni ugovorni iznosi postali finalno poznati.

Procjena utrošenih čovjek-sati dionika (kumulativno 620,5 čovjek-sati) za svaku naznačenu aktivnost prikupljanja podataka dobivana je naknadno tijekom prosinca 2022. kroz izravne razgovore s dionicima i njihove usmeno procijenjene utrošene vremenske resurse.

1.4.7. Timovi i procjena utroška vremena

Osobe koje su sudjelovale u procjeni rizika za 2018. i 2022. godinu (dionici) uključuju:

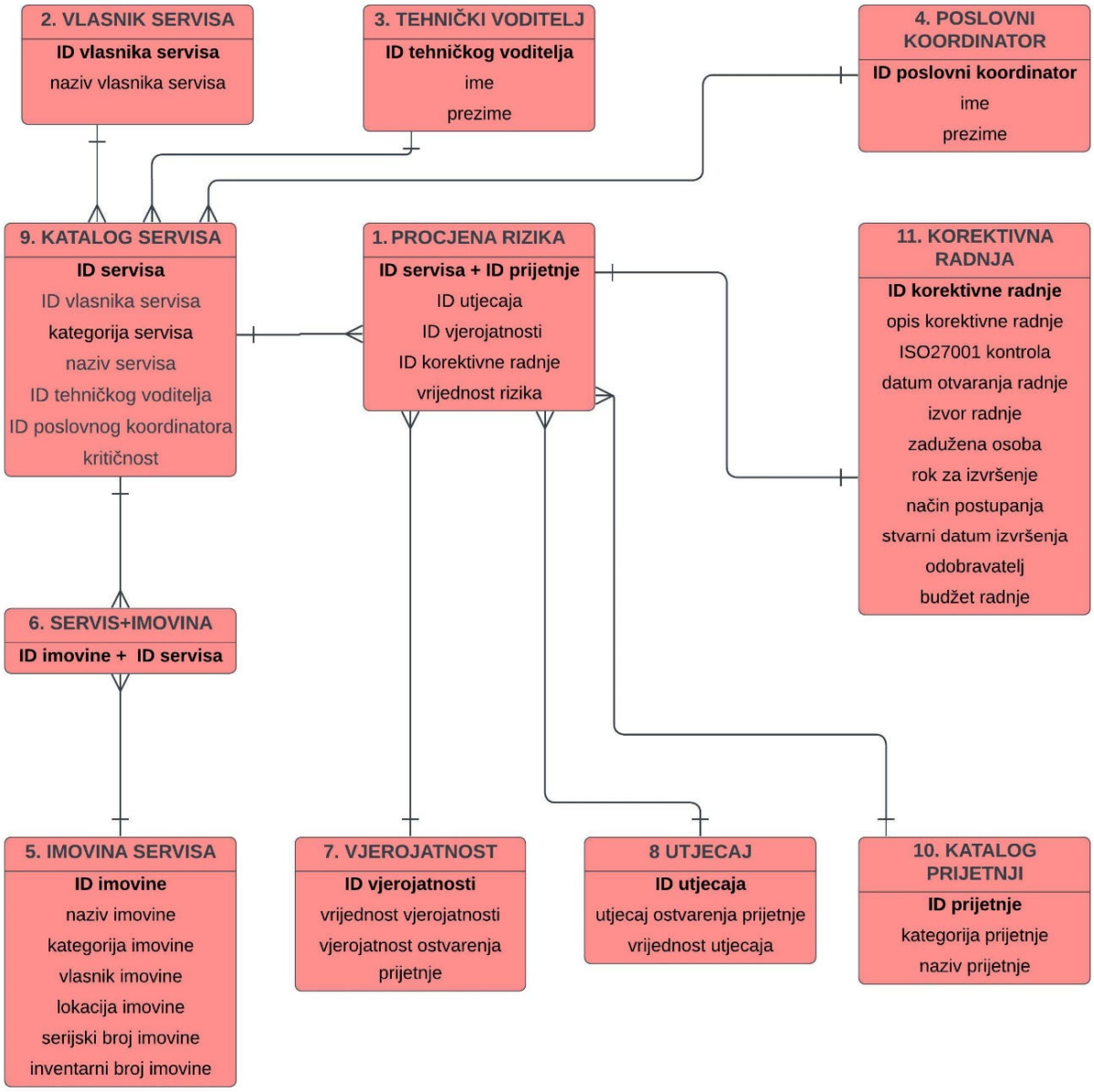
- rukovoditelji IT i OT područja u tvrtki

tehnički voditelji i poslovni koordinatori servisa tvrtke.

1.4.8. Konceptualni model baze podataka za procjenu rizika

Proces procjene rizika uključuje više uzastopnih koraka koje dionici, konkretno tehnički voditelji i poslovni koordinatori servisa, moraju provesti prije nego predaju svoju dokumentaciju u Microsoft Excelu nadležnom rukovoditelju IT ili OT službe. Potrebno je prepoznati entitete i veze kako bi mogli izraditi konceptualni model rezultirajuće baze podataka. Model entiteti-veze (eng. entity-relationship model) je model za konceptualno modeliranje podataka koji za opis modela podataka upotrebljava koncepte: entitet, veza i atribut.

Slika 1. prikazuje konceptualni model podataka [31] u grafičkom obliku, uključujući veze između pojedinih entiteta i njihovu kardinalnost. Primarni ključ svakog entiteta je otisnut masnim slovima.



Slika 1 - Dijagram entiteti-veze konceptualnog modela baze podataka

2. SIGURNOSNA INICIJATIVA - ZTA MREŽA

2.1 Definicija mreže nultog povjerenja

Na tvrtke koje se odluče na uvođenje ZTA kao da se odnosi citat bivšeg američkog predsjednika Theodorea Roosevelta: „Ništa na svijetu nije vrijedno imati ili činiti osim ako ne znači napor, bol, poteškoće.“ [32]

Model nultog povjerenja spominje se još od 2003. godine [33] pa sve do publikacije Forrester Research [34] ubrzo nakon čega su Google i Cisco preuzeli model [35] u svoje materijale. Referentnim opisom koncepta smatra se publikacija SP 800-207 američkog „Nacionalnog instituta za standarde i tehnologiju" (engl. *National Institute of Standards and Technology* - NIST) koja je dala definiciju arhitekture nultog povjerenja kao „evoluirajući skup paradigmi kibernetičke sigurnosti koje pokreću obranu od statičnih perimetara temeljenih na mreži do fokusa na korisnike, imovinu i resurse" [5].

Model nultog povjerenja je sigurnosni koncept, logički okvir razmišljanja koji eliminira pretpostavku sigurne mreže. U ZTA sav mrežni promet je po definiciji nesiguran, te organizacije moraju verificirati i osigurati sve mrežne resurse, limitirati i dinamički provoditi kontrolu pristupa i kontrolirati sav promet na mreži [36]. NIST je proširio opseg mrežne sigurnosti sa zaštite podataka i servisa na sve organizacijske mrežne resurse uključujući sve uređaje, infrastrukturne komponente, aplikacije, virtualne resurse i servise u oblaku [5].

Kao zanimljiva paralela poznatog citata pruskog generala von Clausewitza da je „osnovno organizacijsko načelo svakog društva ono ratno“ [37], osnovna je organizacijska pretpostavka nultog povjerenja da je mreža popustila pod napadom i da je aktivni napadač prisutan i prikriven negdje u LAN-u. Američka Nacionalna sigurnosna agencija (engl. *National Security Agency* - NSA) definira ZTA kao „skup dizajnerskih principa, odnosno kao koordiniranu kibernetičku i upravljačku strategiju baziranu na saznanju da prijetnje postoje i unutar i izvan tradicionalnih granica mreže“ [38], arhitekturu koja „traži da organizacija kontinuirano propituje premisu da svaki korisnik, uređaj i mrežna komponenta trebaju implicitno biti smatrani sigurnima zbog svoje pozicije na mreži“ [38].

Važno je napomenuti da ZTA mreža ne postoji, već postoji samo koncept ZTA koji je primjenjiv na neku mrežu, a što se vidi i iz NIST opisa koji vlastitu definiciju ZTA naziva „apstraktnom“ [5], te navodi da je „nulto povjerenje“ bazirano na „razvijajućem skupu paradigmi kibernetičke sigurnosti“ [5].

2.2 Svrha ZTA mreže

Moderne poslovne mreže koriste desetke aplikacija smještenih na razvedenim vlastitim poslovnim mrežama, te u više međusobno nepovezanih servisa u oblaku različitih pružatelja usluga. Dio tih aplikacija povezan je na servise državnih i regulatornih tijela na temelju regulatornih zahtjeva, primjerice Porezna uprava, FINA e-Računi, Hrvatski zavod za mirovinsko osiguranje (HZMO), Hrvatski zavod za zdravstveno osiguranje (HZZO). Poslovni korisnici zemljopisno su razmješteni po poslovnim lokacijama i na kućnom radu, a računalni uređaji su u vlasništvu organizacije, unajmljeni od treće strane ili u vlasništvu radnika kroz korištenje privatnih računala u vlasništvu samih radnika (engl. *bring your own device* - BYOD model). Ovo nije specifičan oblik neke posebno komplicirane mrežne organizacije nego sasvim realan prikaz srednjih i većih hrvatskih tvrtki koje imaju više zemljopisnih ogranaka i ambiciju za rad unutar jedinstvenog tržišta Europske Unije (engl. *European Union* – EU).

Uz zakonske obveze koje se nameću u smislu kibernetičke zaštite državnih institucija i kritične infrastrukture, državna su ministarstva i agencije te pogotovo operatori energetskih, transportnih i komunikacijskih sustava stavljeni u poziciju da moraju tražiti novi koncept mrežne sigurnosti jer dosadašnji način više ne funkcionira. Taj traženi koncept treba organizacijama omogućiti da se njihove poslovne mreže ne samo šire i razvijaju u skladu s potrebama organizacije, nego da se taj razvoj dogodi pod određenim uvjetima koji će dovesti do konvergencije mrežne kibernetičke sigurnosti. Umjesto da svaka od takvih organizacija traži vlastita rješenja, pronalazi jedinstvene koncepte i rješava samostalno sve probleme koje takva transformacija zasigurno donosi organizaciji, razumno bi bilo usvojiti sveobuhvatni pristup sigurnosti mreže koji je sve te faktore već uzeo u obzir. ZTA kao moguća strategija mrežne sigurnosti za takve organizacije može ponuditi dokumentirane principe dizajna i građevne elemente definirane na način koji je tehnički nezavisan od pojedinih proizvođača tehnologije.

Iako se današnji korporativni rukovoditelji za informacijsku sigurnost (engl. *Chief Information Security Officer* - CISO) i IT/OT timovi stručnjaka bave svim vrstama kibernetičkih prijetnji, realno je konstatirati da je glavni fokus na prevenciji infekcije *ransomwareom*. *Ransomware* ili ucjenjivački softver je „oblik zlonamjernog softvera koji šifrira datoteke žrtve tako da im se ne može pristupiti, a napadač tada zahtijeva da žrtva plati otkupninu kako bi im nesmetan pristup podacima bio obnovljen“ [39]. On predstavlja je ultimativni kibernetički napad današnjice koji u novijom inačicama dodatno ucjenjuje napadnutu tvrtku prijetnjom da će ih izložiti poruzi i reputacijskom riziku tako da će posebno osjetljive datoteke učiniti javno dostupnima i tako osramotiti žrtvu pred javnošću i poslovnim partnerima. Pojedini *ransomware*

operateri ne prežu niti od situacija gdje ucjenjuju i treće strane do čijih su osjetljivih podataka došli krađom podataka od tvrtke žrtve. Prosječna isplata otkupnine napadačima iznosi 170.404,00 američkih dolara, a tvrtke u prosjeku imaju dodatni trošak povratka u redovni rad i sanacije posljedica napada u prosječnom iznosu od 1.850.000,00 američkih dolara, što uključuje troškove kao što su nedostupnost ključnih poslovnih procesa, utrošeni sati radnika i trošak kupovine sigurnosnih uređaja radi prevencije ponovnog napada [39].

2.3 Prednosti i mane ZTA koncepta

Zaštita organizacijskih podataka i sigurnost mrežnog pristupa osnovne su koristi implementacije koncepta nultog povjerenja. Razumno je očekivati da će organizacija imati lakši posao pripreme za bilo kakvu reviziju u smislu prikupljanja i prezentacije podataka s mreže s obzirom na to da je svaki događaj na mreži adekvatno logiran. Realna korist je i očekivano skraćivanje vremena detekcije u slučaju proboja mreže od strane napadača, kao i smanjenje općenito profila rizika za proboj s obzirom na sve kontrole koje se smatraju sastavnim dijelom koncepta. Administratori i agenti centralne službe sigurnosnog operativnog centra (engl. *security operations center* - SOC) agenti će dobiti kvalitetan uvid u kompletan mrežni promet i eventualne probleme i anomalije u tom prometu. Također, očekivano je i povećanje organizacijske kontrole nad tipično raspršenim servisima u oblaku [35].

Dodatne koristi se pojavljuju u danas vrlo aktualnom području sigurnosti trećih strana ili sigurnosti dobavnog lanca (engl. *supply chain security* - sigurnost dobavljačkog lanca) jer se određene restrikcije uvode i za ona računala i korisnike koji nisu pod izravnom kontrolom organizacije, ali je organizacija u nekom poslovnom odnosu s tim trećim stranama. Tipično se ovo odnosi na pružatelje usluga i tvrtke koje dobavljaju i održavaju IT/OT opremu. Računalo treće strane na ZTA korporativnoj mreži bi imalo minimalno potrebna pristupna prava, bilo bi smješteno u odgovarajući virtualni LAN i kontinuirano praćeno dok god je na korporativnoj mreži. Pokušaj komunikacije kompromitiranog računala prema napadaču na Internetu bi bio momentalno blokiran kroz pristupne liste, a potom bi bili podignuti odgovarajući alarmi i notifikacije. Sustav za analitiku ponašanja korisnika i uređaja na mreži (engl. *User and Entity Behaviour Analytics* - UEBA) bi uočio bilo kakve pokušaje lateralnog pomicanja po mreži, te bi orkestracijom zaustavio takav pokušaj, a odmah i obavijestio IT administratore organizacije [38].

Samo uvođenje nultog povjerenja kao koncepta može biti vrlo izazovno, pogotovo u ranijim fazama procesa. Velika količina zastarjele tehnologije, karakteristična za mnoge veće

organizacije s jakom Internetskom prisutnošću i mrežom fizičkih ogranaka, te tehnički dug organizacije u smislu stupnja razvoja svojih IT i OT digitalnih procesa u odnosu na tehničke sposobnosti potrebne za suprotstavljanje sasvim izvjesnim kibernetičkim napadima s Interneta, predstavljaju ozbiljan problem s kojim se mnoge organizacije izbjegavaju suočiti. Proces se smatra relativno sporim, financijski izazovnim i radno intenzivnim za tehničke radnike i tvrtkama koje se odvaže uvesti ZTA.

2.4 Segmenti ZTA mreže

Kritično je da organizacije prihvate da je prvi korak u implementaciji nultog povjerenja uspostava procesa vladanja (engl. *governance*), odnosno inicijalna uspostava evidencija svih mrežnih resursa i njihova klasifikacija prema sigurnosnim kriterijima. Da bi se koncept nultog povjerenja ispravno pokrenuo, potrebno je razumjeti gdje se nalaze svi podaci na mreži, kako su klasificirani i tko im treba biti u stanju pristupiti. Ovo je mukotrpan početak koji se ne smije preskočiti jer bez njega nema niti prave analize rizika niti mogućnosti se da pravilno definiraju kontrolne pristupne liste, a otvara se mogućnost za puno frustracija kasnije kad se počnu otkrivati propusti napravljeni preskakanjem ovog koraka [40].

Različiti autori daju različiti nivo detalja o tome što smatraju obveznim dijelovima ZTA, odnosno je li pojedini građevni blok obvezan ili nije. Ovdje je napravljen presjek tih mišljenja i odabrani su oni dijelovi oko kojih se svi autori s popisa literature koji se bave imenovanjem obveznih dijelova ZTA slažu da bez tih elemenata nema prave arhitekture nultog povjerenja [5] [33] [41]. Treba primijetiti da tu i dalje moraju postojati servisi koji nisu povezani izravno sa sigurnosnim kontrolama, ali su nužni za ispravan rad bilo koje mreže (npr. imenički servis).

1. Sustav za upravljanje identitetima

   Predstavlja sustav koji upravlja identitetima mrežnih korisnika, te daje odgovarajućim korisnicima minimalnu vrstu pristupa u točno određeno vrijeme. Ovaj sustav je centralna točka ZTA [33].
2. 802.1x

   Tehnologija za kontrolu pristupa mreži bazirano na tome koji se korisnik i kojeg uređaja pokušava spojiti na neki mrežni resurs.
3. Vatrozid sljedeće generacije

   Osim klasične funkcije vatrozida, ispunjava i funkcionalnosti prevencije i detekcije upada u mrežu (engl. *Intrusion Prevention System* – IPS, odnosno engl. *Intrusion*

Detection System - IDS), neke funkcionalnosti zaštite i kontrole nad aplikacijama, te uslugu obavještavanja o prijetnjama (engl. *threat intelligence*) iz oblaka.

4. Sustav za upravljanje privilegiranim pristupom

   Sustav za upravljanje privilegiranim pristupom (engl. *privileged access management* - PAM) čuva pristup kritičnim resursima mreže tako da koristi posebni proces za upotrebu i čuvanje identiteta korisnika s privilegijama iznad onih koje imaju obični uredski korisnici, npr. administratori pojedinih sustava ili infrastrukture. Korisnici povišene razine pristupa pristupaju svojim šifriranim vjerodajnicama pohranjenim u sigurnom PAM sustavu u tzv. „sefu“ (engl. *vault*).

5. UEBA

   Sustav strojnog učenja koji detektira anomalije u ponašanju mrežnih resursa i boduje njihov rizik kroz kontinuirani proces evaluacije ponašanja korisnika i uređaja na mreži organizacije.

6. Sustav za orkestraciju

   Predstavlja set scenarija i okidača za automatizirano izvođenje odgovora na različite scenarije (orkestracija) u trenutcima kad UEBA izračuna da je neki mrežni resurs prikupio dovoljno negativnih bodova za aktivaciju nekog predefiniranog automatiziranog odgovora.

7. Analiza klijentskih logova i automatizirani odgovor na prijetnje

   Sustav baziran na klijentima koji ima sposobnost prikupljanja i analize logova s klijenata u realnom vremenu, te upotrebu EDR-a. Nova inačica nekadašnjih antivirus rješenja baziranih na karakterističnom ponašanju virusa kod infekcije.

8. Višefaktorska autentifikacija

   Metoda autentifikacije na mrežu i servise na njoj gdje korisnik uz korisničko ime i lozinku koristi i drugi faktor, uobičajeno jednokratni kod koji dobije iz npr. Google Authenticatora ili slične aplikacije.

9. Segmentacija mreže

   Predstavlja arhitekturni pristup kojim se mreža podijeli u više virtualnih logičkih segmenata ili podmreža s kojima se postiže lokalizacija mrežnih problema, bolja kontrola prometa između segmenata i veća sigurnost u smislu prevencije lateralnog pomaka po mreži.

10. *Proxy* i reverzni *proxy*

Organizacija mora svoje poslovne korisnike štititi od identifikacije u trenutku kad oni pristupaju nekom resursu na Internetu tako da se svi korisnici anonimiziraju iza posrednih (engl. *proxy*) poslužitelja. U suprotnom smjeru, reverzni *proxy* poslužitelj ispred cijele organizacije prima zahtjev nepoznatog klijenta s Interneta za pristupom nekom poslužitelju u organizaciji, te služi kao posrednik i za anonimizaciju poslužitelja organizacije kad im se pristupa s Interneta.

2.5 Ključni principi nultog povjerenja

Koncepte nultog povjerenja traži promjenu načina razmišljanja postavljajući određene temeljne principe u središte filozofije kako će se mreža dalje razvijati i osiguravati. NIST standard je prvi detaljno definirao i pojasnio sedam osnovnih postulata mrežne arhitekture nultog povjerenja [5]:

1. Svi izvori podataka i informatički servisi na mreži su mrežni resursi.
   Ovo uključuje sve klase uređaja u podatkovnom centru, aplikacije, baze podataka, servise u oblaku, uređaje Interneta stvari (engl. *Internet of Things* - IoT), osobna računala i mrežnih pisača, uključujući BYOD uređaje koji trebaju pristup na poslovnu mrežu. Ako uređaj u nekom poslovnom procesu traži Internet protokol (engl. *Internet Protocol* – IP) adresu na poslovnoj mreži ili komunicira s njom u smislu razmjene podataka, onda je tu riječ o mrežnom resursu.
2. Sve komunikacije na mreži moraju uvijek biti sigurne bez obzira na lokaciju na mreži.
   Sama lokacija na mreži ne implicira nikakvo povjerenje, odnosno jednako se promatra i provjerava novi uređaj koji s perimetra traži pristup na LAN kao i uređaj koji traži izlaz na Internet. I jedan i drugi uređaj moraju proći isti proces i iste kriterije autentifikacije i autorizacije. Komunikacija se mora odvijati kriptirano s kraja na kraj u svrhu zaštite integriteta i tajnosti podataka koji se razmjenjuju.
3. Pristup mrežnih resursima se evaluira i dozvoljava kod svakog pojedinog novog zahtjeva za resursima. Bilo koji do bilo kojeg mrežnog resursa se odobrava za svaki pojedini slučaj zasebno, te se uvijek odobrava minimalni mogući pristup za zatraženi slučaj. Odobrenje pristupa na jedan mrežni resurs ne donosi nikakvu implicitnu prednost kod idućeg zahtjeva za pristupom, pristup se uvijek odobrava eksplicitno.
4. Pristup mrežnim resursima se evaluira i dozvoljava putem dinamičke politike pristupa i drugih obrazaca ponašanja korisnika u mrežnoj okolini. Organizacija će na početku putovanja u nulto povjerenje definirati što su njezini resursi, tko su njezini korisnici, te

koju vrstu pristupa ti korisnici i ti resursi imaju na poslovnoj mreži. Korisnički identitet će se voditi centralno u nekom federiranom repozitoriju za sve mrežne identitete, a kakav je npr. Microsoft imenički servis (engl. *Active Directory* - AD). Uređaji se mogu definirati tako da im se ustanovljava potrebna verzija operativnog sustava ili aplikacija, lokacija na mreži, vrijeme u koje se traži pristup, prethodno promatrano ponašanje uređaja i instalirani certifikati. Ponovno se primjenjuje načelo minimalnog pristupa u svrhu restrikcije vidljivosti resursa na mreži i pristupa na te iste resurse.

5. Integritet i sigurnosni status svih mrežnih resursa se kontinuirano nadgleda i provjerava. Niti jednom mrežnom resursu se inherentno ne vjeruje. Mreža bazirana na ZTA mora provoditi kontinuirano promatranje i dijagnostiku te evaluirati stanje za svaki resurs kod svakog zahtjeva za pristupom ovisno o riziku koji se kontinuirano dinamički kalkulira.
6. Dinamička autentifikacija i autorizacija resursa na mreži se provodi prije svakog novog mrežnog pristupa. Bilo koja ZTA organizacija mora imati jasnu sliku o evidencijama svojih identiteta, vjerodajnica, pristupnih lista i resursa. Višefaktorska autentifikacija se smatra standardom za sve mrežne resurse unutar ZTA. Politika pristupa je dinamička i definirana u ovisnosti o više relevantnih parametara kao što su vremenska ograničenja, sa svrhom postizanja balansa između upotrebljivosti i sigurnosti.
7. Prikupljaju se informacije o trenutnom stanju resursa, mrežne infrastrukture i mrežnih komunikacija radi analize i unapređenja sigurnosnog stanja mreže. Organizacija će skupljati podatke o sigurnosnom stanju svakog mrežnog resursa, mrežnom prometu i zahtjevima za pristup, analizirati te podatke i sve zaključke upotrijebiti za reviziju dinamičke politike pristupa i osiguranja njezine primjene.

2.6 Institucionalizacija ZTA kroz zakonske inicijative

Organizacija donosi poslovnu odluku na najvišem upravljačkom nivou da želi uvesti koncept nultog povjerenja na svojoj poslovnoj mreži kao svoju ključnu strategiju mrežne sigurnosti i generirati plan arhitekture nultog povjerenja baziran na ključnim ZTA principima. Na istom nivou davat će se suglasnost za značajna ulaganja u smislu financijskih i ljudskih resursa [36] i to na nivoima koji bi mogli predstavljati izazov i za najmotiviranije organizacije.

Obzirom da sigurnosni model nultog povjerenja nije jedinstveni produkt ili usluga koje se mogu komercijalno nabaviti i instalirati po nekom uniformom modelu za sve tvrtke, ključni preduvjet za bilo kakav početak adopcije ovog koncepta je zakonski ili tržišno stvorena

politička želja za promjenom manifestirana u prvom redu kroz promjenu poslovne i sigurnosne kulture [36]. U Sjedinjenim Državama događaju se promjene u shvaćanju kibernetičke sigurnosti iskazane kroz izvršni nalog (engl. *executive order*) 13636 iz 2013. i pogotovo izvršni nalog 14028 iz 2021. [42], američkog predsjednika nakon incidenta s ucjenjivačkim virusom na operatoru naftovoda *Colonial Pipeline*), dok se u Europskoj Uniji od 2016. godine postoji nešto sveobuhvatnija „Direktiva za mrežne i informacijske sustave“ (engl. *Network and Information Systems* – NIS), s oznakom EU 2016/1148 [43]. I jedna i druga sigurnosna inicijativa definiraju tvrtke pružatelje velikih infrastrukturnih usluga u sektorima energetike, transporta, komunalija i telekomunikacija kao operatore ključnih usluga sa zakonskim obvezama uvođenja tehničkih i organizacijskih mjera za zaštitu svojeg poslovanja.

Mreže nultog povjerenja tek će ući u svakodnevne teme mrežne sigurnosti, u Hrvatskoj pogotovo, obzirom da je u ožujku 2022. NSA u jednom od svojih ključnih javno dostupnih dokumenata namijenjenih kao smjernice za američke državne institucije izrijekom potvrdila da „u potpunosti podržava sigurnosni ZTA model nultog povjerenja“ [44]. Američko Ministarstvo obrane u svojem dokumentu arhitekture mreže još 2010. godine uvodi ZTA kao fundamentalni organizacijski koncept vlastite mrežne arhitekture [45]. Hrvatske institucije u ovom smislu nisu još ažurirale svoje smjernice, ali s Hrvatskom u Sjevernoatlantskom savezu (engl. *North Atlantic Treaty Organization* - NATO) nije nerazumno očekivati da slične preporuke uskoro zažive na stranicama Sigurnosno-obavještajne agencije (SOA) ili ZSIS-a i postanu dio nacionalnih preporuka za institucije hrvatske države i operatore ključne usluge u smislu EU NIS Direktive i njezinih transpozicija u nacionalna zakonodavstva država članica.

2.7 Definicija i opseg projektnog programa za uvođenje ZTA

Program sigurnosne inicijative uvođenja arhitekture nultog povjerenja sastoji se od deset međusobno nadopunjujućih i vremenski ograničenih projekata usko povezanih kroz zajedničku strategiju, sigurnosnu arhitekturu, poslovne ciljeve, proračun i rizike.

Program sigurnosne inicijative se sastoji od deset individualnih projekata, koji se podudaraju s segmentima ZTA mreže nabrojanim u poglavlju 2.4.

Razlog zašto su odabrani upravo ovi elementi ZTA je jednostavan: u trenutku pokretanja sigurnosne inicijative, tvrtka nije imala implementiranu niti jednu od ovih tehnologija niti na IT niti na OT dijelu mreže, pa nije bilo potrebe da se postojeće rješenje zamjenjuje novim. Navedene tehnologije ušle su u odabir nužnih projekata sukladno željama rukovoditelja IT i

OT službi, a sukladno financijskim projekcijama troškova koje su tad procjenjivane, dok su ostale projektne ideje otpale zbog financijskih (bile su preskupe), vremenskih (implementacija bi trajala predugo), projektnih (predloženi projekt mora ići među prvima, a vrlo je složen i može zakočiti kasnije projekte) ili funkcionalnih razloga (nisu nudile sigurnosne koristi kao ovih deset). Važno je napomenuti da se unutar Energenta d.o.o. IT mreža i OT mreža planiraju, grade i održavaju u potpuno odvojenim stručnim službama, prema odvojenim procesima, pod nadzorom različitih direktora, koristeći vlastite opsege implementacije i specifičnosti okuženja i broja korisnika sustava, pa je realno za očekivati da će implementacija npr. privilegiranog pristupa rezultirati sasvim različitim projektima u ova dva okruženja, kako tehnološki, tako i financijski. Osnovna ideja iza ove organizacijske strukture je da će OT sustavi, kao tehnološki ključni za provedbu kritičnih procesa tvrtke, biti zaštićeni s dvije različite filozofije kibernetičke obrane i različitim proizvođačima opreme prije nego napadač stigne do sustava za upravljanje industrijskim procesima i prikupljanje podataka (engl. *supervisory control and data acquisition* – SCADA). Iako je ovo skuplja strategija za implementaciju tvrtka čvrsto stoji iza nje, svjesna svoje nezamjenjive role na energetskog karti države. Sigurnosna inicijativa implementirana je kao zajednička organizacijska arhitektura sigurnosti na mreži tvrtke, ali su pristupi pojedinim projektima inicijative bili potpuni individualizirani od strane nadležnih stručnih službi.

3. DANAŠNJA POZICIJA TVRTKE U POSLOVNOM OKRUŽENJU

Energent d.o.o. je tvrtka koja ima status nacionalne kritične infrastrukture u Republici Hrvatskoj. Po definiciji iz „Zakona o kritičnim infrastrukturama“ [46], „nacionalne kritične infrastrukture su sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.“ Energetika je, uz komunikacije i zdravstvo, jedna od tri najizloženije vertikale prema učestalosti kibernetičkih napada, a direktori operatera energetske vertikale vjeruju „da će im se dogoditi značajni incident unutar iduće dvije godine, rezultirajući u narušenim dnevnim operacijama (85% anektiranih direktora), šteti za okoliš (74%) i gubitku ljudskih života (57%)“ [47]. Postoje četiri ozbiljna izazova [47] s kojima se generalno danas susreću slične energetske tvrtke u svijetu:

- nesklonost upravljačkih struktura da investiraju u kibernetičku sigurnost jer im se čini da čine dovoljno koči napredak energetskih tvrtki
- integracija IT i OT okruženja dovodi do rizika kakve prije nije trebalo adresirati, no sad je adresiranje nužno
- nedostatak kvalitetne kadrovske ekspertize u vlastitoj organizaciji
- iznimno kompleksni dobavljački lanci skrivaju kritične ranjivosti.

Preporuke vodećih svjetskih eksperata [47] u području sigurnosti u energetici uključuju savjete da se postojeći budžeti mudro investiraju u inicijative gdje mogu napraviti najviše pozitivnog utjecaja, da tvrtke naprave dubinske analize svojih procesa i dobavljačkog lanca i ustanove gdje su ranjivi, te da sredstva koja se troše na sigurnost kvalitetno balansiraju između nabave tehnologije i treninga sigurnosti svojih IT i OT stručnjaka.

3.1 Vanjski kontekst organizacije

Analiza vanjskog konteksta provedena je korištenjem metode PESTLE [48]. PESTLE je „strateški analitički alat koji se koristi za procjenu vanjskog okruženja i faktora koji utječu na poslovanje“ [49]. PESTLE akronim označava političke, ekonomske, društvene, tehnološke, pravne i ekološke čimbenike koji utječu na tvrtke i njihovo tržišno okruženje. PESTLE se nedavno razvio iz PEST analize nakon što su jačajuće sile globalizacije i jačajuće snage konkurencije na tržištu zajedno s drugim nizom čimbenika povećale važnost i potencijalni

utjecaj ekoloških i pravnih čimbenika na poslovanje. U svojoj srži, riječ je o strateškom alatu za analizu i razumijevanje vanjskog okruženja tvrtke, tržišta, poslovne pozicije tvrtke, njezinog tržišnog potencijala i tržišnih trendova.

Tablica 5 prikazuje PESTLE analizu vanjskog konteksta tvrtke Energent d.o.o., pri čemu su ključni dijelovi konteksta opisani narativno, a stanje i značaj s obzirom na tvrtku ocijenjeni na skali od 1-3 koristeći slijedeće referentne vrijednosti:

- Stanje: 1 – nepovoljno; 2 – djelomično povoljno; 3 – povoljno
- Značaj: 1 – nije značajno; 2 – neutralno; 3 – značajno.

Tablica 5 - PESTLE analiza vanjskog konteksta tvrtke

POLITIČKO OKRUŽENJE	
Tvrtka je izuzetno izložena prema rizicima vezanima uz globalnu geostratešku situaciju oko plina kao strateškog energenta, a to se posebno reflektira u rizicima vezanim uz kibernetičku sigurnost cijelog plinskog transportnog sustava. Tvrtka je u 100% vlasništvu Republike Hrvatske.	
Stanje	1 – nepovoljno
Značaj	3 – značajno
EKONOMSKO OKRUŽENJE	
Hrvatska kao članica Europske unije predstavlja relativno povoljno ekonomsko okruženje, ali postoji jasna inicijativa i na nivou EU i na nivou Hrvatske da se potrošnja plina kao energenta smanji zbog enormnog porasta cijene plina kao energenta u zadnjih 12 mjeseci. Moguća je recesija u Hrvatskoj do kraja 2022. godine.	
Stanje	1 – nepovoljno
Značaj	2 – neutralno
SOCIOLOŠKO OKRUŽENJE	
Depopulacija uzrokovana otvaranjem tržišta Europske unije, kao i nepovoljna demografska situacija negativno utječu na potrošnju u Republici Hrvatskoj. Moguća nadolazeća recesija vjerojatno će utjecati na građane Hrvatske da pokušaju smanjiti potrošnju energije, no s obzirom na to da svi energenti poskupljuju i da je hladnoća zime presudan	

faktor u određivanju potrošnje plina, a ne svijest građana, za ovaj faktor ne očekujemo da ima značajniji utjecaj.	
Stanje	1 – nepovoljno
Značaj	2 – neutralno
TEHNOLOŠKI TRENDOVI	
Tvrtka je usmjerena na kontinuirana tehnološka unaprjeđenja ne samo u osnovnom poslovanju, nego i u drugim poslovnim procesima, upravljanjem energijom, zaštiti okoliša i sigurnošću. Tvrtka je vrlo profesionalna, izrazito inženjerski organizirana i ustrojena, pri čemu je sama osnovna djelatnost postavljena u skladu sa svim poslovnim dobrim praksama i standardima koji je očekuju od tvrtke članice europskog plinskog transportnog sustava.	
Stanje	3 – povoljno
Značaj	3 – značajno
ZAKONSKE REGULATIVE	
Transport plina je visoko regulirana djelatnost. Odlukom Ministarstva gospodarstva od 31.10.2018. tvrtka je obveznik „Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga“ [12] iz čega proizlazi veliki broj obveza tvrtke u tehničkom, organizacijskom i procesnom smislu. Provedba analize rizika izravna je obveza iz spomenute „Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga“ (članak 11., stavci a i b). Maksimalna kazna za tvrtku operatora u Hrvatskoj iznosi oko 70.000 eura po dokazanom propustu u smislu kršenja zakona. Sukladno „Zakonu o tržištu plina“ [50], tvrtka je proglašena kao monopolist u segmentu transporta plina te nema konkurencije u pravom smislu te riječi za konkretno plin kao energent (postoje konkurentni energenti i njihovi operatori). „Opća uredba o zaštiti podataka“ [30] traži „tehničke i organizacijske mjere“ za zaštitu osobnih podataka u obradama tih podataka koje provode tvrtke poput Energenta d.o.o. Maksimalna kazna u Hrvatskoj iznosi deset milijuna eura po dokazanom propustu u smislu kršenja zakona. Europska Unija je svojom „Strategijom kibernetičke sigurnosti“ [51] postavila političke prioritete, a nadolazeće zakonske inicijative na nivou EU poput „Direktive o otpornosti kritičnih subjekata“ (engl. *critical entities resilience* – CER) [52] i „Direktive o mjerama za	

visoku zajedničku razinu kibernetičke sigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148“, poznatije kao „Direktiva o mrežnim i informacijskim sustavima 2“ (engl. *Network and Information Systems 2* – NIS 2) [15] među ostalim jasno traže da operatori kritične infrastrukture održavaju sustav tehničkih i organizacijskih mjera kibernetičke zaštite baziranih na redovno provođenim analizama rizika, odnosno predstavlja**u** europski „zakonodavni okvir koji podrazumijeva značajnu nadogradnju kibernetičke sigurnosti, posebno u područjima koja se odnose na nadzor i provedbu“ **[53]**. NIS 2 uvodi kazne koje će za tvrtke poput Energenta d.o.o. iznositi do deset milijuna eura po dokazanom propustu u smislu kršenja zakona uz moguće suspendiranje rukovodeće osobe odgovore za kibernetičku sigurnost.	
Stanje	3 – povoljno
Značaj	3 – značajno
EKOLOŠKO OKRUŽENJE	
Tvrtka je izuzetno svjesna fosilne prirode energenta kojim se bavi, te ulaže svaki napor da se utjecaj na okoliš drži na tehnološkom minimumu. Tvrtka je nositelj aktivnih certifikata „Međunarodne organizacije za norme“ (engl. *International Organization for Standardization* – ISO) za kvalitetu (ISO9001), upravljanje okolišem (ISO14001), upravljanje informacijskom sigurnošću (ISO27001), upravljanje zdravljem i sigurnošću (ISO45001), te upravljanje energijom (ISO5001).	
Stanje	3 – povoljno
Značaj	3 – značajno

Informacije su prikupljene iz planskih dokumenata tvrtke, godišnjih izvještaja, baze primjenjive zakonske osnove i primjenjive regulative, te izvješća unutarnje i vanjske revizije. Osim što je PESTLE analiza alat koji čitatelju ovog rada omogućava bolje razumijevanje vanjskog okruženja u kojem Energent d.o.o. djeluje, ona ujedno ukazuje na potencijalno ključne motive uprave tvrtke za uvođenje ZTA. Naime, sva trenutna (Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga", „Opća uredba o zaštiti podataka“) i nadolazeća (NIS 2, CER) inzistira na primjerenim organizacijskim i tehničkim mjerama (u smislu sigurnosnih mrežnih sustava) i uvodi rastuće kazne i za pravnu osobu (financijska kazna) i za fizičku osobu direktora (privremena suspenzija od obavljanja dužnosti).

Iako ovo nigdje nije izričito navedeno na službeni način, razumno je pretpostaviti da su zakonske kazne bile glavni motiv za pokretanje sigurnosne inicijative.

3.2 Unutrašnji kontekst organizacije

Sljedeći podaci u najvećoj su mjeri su preuzeti iz dostupnih korporativnih materijala, profila tvrtke i financijskih izvješća tvrtke Energent d.o.o.

Misija tvrtke Energent d.o.o. je provoditi rolu operatora transportnog sustava plina i biti odgovoran za:

- transport i tranzit prirodnog plina
- vođenje (nadzor i upravljanje), održavanje te razvoj i
- izgradnju plinskoga transportnog sustava
- nediskriminirajući pristup transportnom sustavu kad je to
- ekonomski i tehničko-tehnološki razumno i opravdano.

Vizija tvrtke Energent d.o.o. je biti cijenjen i vodeći infrastrukturni energetski subjekt plinskoga gospodarstva Republike Hrvatske te važan strateški energetski partner regije i Europske unije, koji na transparentan i društveno odgovoran način svojim vlasnicima omogućava realizaciju energetskih obveza, a korisnicima siguran i pouzdan transport prirodnog plina, kao jednog od ekološki i ekonomski najprihvatljivijih opcija opskrbe energijom u uvjetima otvorenog tržišta.

Poslovni ciljevi tvrtke su kako slijedi:

- uravnoteženost naturalnih ciljeva, operativnih troškova i ulaganja s prihodima kroz provedbu planova razvoja i poslovanja,
- održivo poslovanje kroz likvidnost i solventnost trgovačkog društva,
- u cijelosti vlastito ulaganje u dugotrajnu imovinu,
- ostvarivanje razumne dobiti.

Opći ciljevi tvrtke su kako slijedi:

- zadovoljstvo korisnika transportnog sustava i njihovo povjerenje,
- uvažavanje potreba, interesa i sposobnosti radnika poticajnim sustavom nagrađivanja i napredovanja
- primjena načela održivog razvoja i promicanje suživota s prirodom,

- suradnja sa širom zajednicom i stanovništvom na područjima na kojima djeluje.

Obavljajući energetsku djelatnost transporta plina kao svoju osnovnu djelatnost, Energent d.o.o. jamči sigurnu, pouzdanu i kvalitetnu dopremu prirodnog plina od ulaza u plinski transportni sustav do primopredajnih mjerno-redukcijskih stanica distributera plina te izravnih i povlaštenih kupaca. Nadležan je za upravljanje nadzorom, održavanjem, razvojem i izgradnjom cijelog magistralnog plinskog transportnog sustava, kao i svim ostalim poslovima koji su nužni za tehničko funkcioniranje sustava.

Energent d.o.o. je vrlo solventna i likvidna tvrtka. Prihodi su stabilni i u cijelosti se ostvaruju prodajom transportnih kapaciteta u plinskom transportnom sustavu, pri čemu je usluga regulirana i cijena transporta određena od strane regulatora plinskog tržišta HERA-e (Hrvatska energetska regulatorna agencija).

Tvrtka je sama prilično komunikacijski introvertirana i gotovo nikad ne istupa u medijima. Gledajući strukturu 275 zaposlenika, tvrtka bi se mogla okarakterizirati kao relativno stara (prosječna starost zaposlenika je 50 godina), s pretežno srednjom strunom spremom (SSS) i visokom stručnom spremom (VSS), velikom većinom sindikalno organiziranima, ali pasivno (bez značajnijih aktivnosti sindikata u životu tvrtke). Velika većina radnika nikad nije radila za privatnog poslodavaca, a više od polovice radnika nikad nije radilo kod drugog poslodavca.

4. PROFIL RIZIKA PRIJE UVOĐENJA SIGURNOSNE INICIJATIVE

Korištenjem dokumenta „*Security Risk Assessment Methodology*“ [54] koji je udruga svih EU operatora transporta plina „*Gas Infrastructure Europe*“ s KPMG Advisoryem pripremio 2014. godine upravo za potrebe operatera transporta plina za Europsku Uniju, pregledavanjem dokumenta i njegovih priloga pronađena je duga lista potencijalnih prijetnji koje su stavljene u katalog prijetnji Energenta d.o.o. Potrebno je napomenuti da je KPMG metodologija procjene rizika vrlo detaljno raspisana i potpuno prilagođena velikim europskim operatorima plinske infrastrukture, čime bi bila idealna i za Energent d.o.o., no procjena je rukovodeće strukture tvrtke bila je da metodologija kompleksna do mjere da ju je praktično nemoguće lokalno implementirati na održiv način, te je donesena odluka da se koristi neusporedivo jednostavnija metodologija Ministarstva financija [8]. Odluka tvrtke je također bila da se od KPMG Advisorya preuzme osnovni katalog prijetnji koji je izrađen upravo za operatore transporta plina, te da se upotrijebi osnovna metodologija KPMG Advisorya za definiciju, klasifikaciju i evidentiranje imovine svih pojedinih servisa. Razlog zašto se nije išlo na punu upotrebu cjelovite metodologije KPMG Advisorya je opet u zaista složenom KPMG procesu koji je procijenjen kao podesan za veće tvrtke s većim brojem radnika i plinskih objekata na trasi plinovoda. Time je od tri ključna elementa KPMG Advisory metodologije (katalog prijetnji, evidencija imovine, procjena rizika) Energent d.o.o. preuzeo pojednostavljene verzije kataloga prijetnji i evidencije imovine, dok je procjenu rizika u potpunosti zamijenio onom Ministarstva financija.

Sve aktivnosti uspostave sustava procjene rizika, uključujući definicije politike upravljanja rizicima, uspostavu kataloga prijetnji i kataloga servisa, identifikaciju i klasifikaciju imovine i imenovanje vlasnika imovine, provedbu inicijalne procjene rizika, otvaranje korektivnih radnji i njihovo evidentiranje provedene su u sklopu internog projekta bez sudjelovanja vanjskih tvrtki, te je dovršetkom projekta krajem 2017. godine tvrtka imala osnovne organizacijske, kadrovske i procesne elemente procesa upravljanja rizicima.

4.1 Katalog prijetnji

Ovaj popis prijetnji korišten je u trenutku prije početka uvođenja sigurnosne inicijative i sadrži osamdeset i šest prijetnji podijeljenih u deset kategorija prijetnji.

- Kadrovske

- Financijske
- Treće strane
- Tehničke
- Političke
- Kriminal
- Okruženje
- Ugovori
- Zaštita ljudi i imovine
- Zakonodavne.

Iz KPMG Advisory kataloga prijetnji izbačene su one prijetnje koje su vlasnici servisa procijenili kao neprimjenjive za hrvatsko tržište. Preostale prijetnje nalaze se u priloženoj tablici broj 6. Riječ je o standardnom predlošku kataloga prijetnji koji se koristi u Energentu d.o.o. kad je u opsegu evaluacije cijela tvrtka.

Tablica 6 – Katalog prijetnji prije sigurnosne inicijative

KATEGORIJA PRIJETNJI	KATALOG PRIJETNJI
Kadrovske	Prijetnje korisnika servisa s namjerom (krađa podataka, uvođenje zlonamjernih programa, upada, prijevare, sabotaže itd.)
	Prijetnje korisnika servisa bez namjere (neznanje, nepoznavanje procedura, nedostatak svijesti o sigurnosti itd.)
	Nedostatak svijesti korisnika servisa o najboljim praksama u području kibernetičke sigurnosti
	Korisnici servisa koji imaju rolu u izvršenju ključne usluge nemaju više kapacitet/sposobnost da izvršavaju svoje dužnosti
	Prijetnje administratora servisa s namjerom (krađa podataka, uvođenje zlonamjernih programa, prijevare, sabotaže itd.)
	Prijetnje administratora servisa bez namjere (neznanje, nepoznavanje procedura, nedostatak svijesti o sigurnosti itd.)
	Nedostatak svijesti administratora servisa o najboljim praksama u području kibernetičke sigurnosti
	Administratori servisa koji imaju rolu u izvršenju ključne usluge nemaju više kapacitet/sposobnost da izvršavaju svoje dužnosti
	Neovlašteno rukovanje opremom
Financijske	Nisu odobrena sredstva za tretiranje identificiranih rizika
	Pogrešno su planirana sredstva za tretman identificiranih rizika
Treće strane	Krađa (IT vlasništvo, vozila, odjeća, komponenta specifična za web-lokaciju, informacije itd.)

	Fizičke prijetnje od trećih osoba prema zaposleniku (otmica, iznuda, nasilje nad zaposlenicima itd.)
	Fizičke prijetnje od trećih osoba prema objektima (sabotaža, fizički upadi, itd.)
	Prijetnje ugovornih partnera s namjerom (krađa, povreda povjerljivosti, prijevare, sabotaže itd.)
	Prijetnje ugovornih partnera bez namjere (neznanje, nepoznavanje procedura, nedostatak svijesti o sigurnosti itd.)
	Nedostatak svijesti ugovornih partnera o najboljim praksama u području kibernetičke sigurnosti
	Ugovorni partneri koji imaju rolu u izvršenju ključne usluge nemaju više kapacitet/sposobnost da izvršavaju svoje dužnosti
	Rizik od kašnjenja postupaka javne nabave zbog žalbi ili proceduralnih propusta
	Ispadi veze javne mobilne mreže
	Postupak javne nabave – „neozbiljni“ ponuditelji
Tehničke	ICT napadi i prijetnje trećih strana izvan tvrtke (napadi izvana, DDoS napadi, phishing, zlonamjerni softver i sl.)
	ICT kvarovi ili ispadi sustava usred lošeg ili nedovoljnog održavanja i brige o sustavu
	ICT napadi i prijetnje trećih strana unutar tvrtke (privatni USB ključevi, korištenje uočenih sigurnosnih propusta i sl.)
	ICT kvarovi ili ispadi sustava usred lošeg dizajna sustava ili nepodržane konfiguracije sustava
	ICT kvarovi ili ispadi sustava usred nedostatne fizičke sigurnosti ili sigurnosti okoliša (uvjeti čuvanja opreme)
	Nefunkcionalnost ili nedostupnost vanjskog servisa nužnog za rad ključne usluge
	ICT kvarovi ili ispadi sustava zbog neadekvatne kadrovske ekipiranosti informatičara
	Informatička oprema nije pohranjena i održavana u adekvatnim uvjetima okoliša (pristup, prašina, itd.)
	Neadekvatna licenciranost pojedinog servisa
	Neadekvatna segregacija dužnosti u sklopu upravljanja ključnom uslugom
	Neadekvatno upravljanje korisničkim pravima
	Nemogućnost povrata backupa u slučaju potrebe
	Nemogućnost hitne intervencije vlastitih radnika izvan radnog vremena
	Nisu ukinuta pristupna prava radnicima koji ta prava više nemaju
	Rashodovana oprema sadrži povjerljive podatke jer ih nitko nije obrisao na siguran način
	Prijenosni medij sadrži povjerljive podatke jer ih nitko nije obrisao na siguran način

	Poslovni korisnici s udaljene lokacije spajanju se na ključnu uslugu na nesiguran način
	Mrežna aktivna ili sistemska oprema nije adekvatno nadograđena zakrpama
	Mrežna aktivna ili sistemska oprema više nije podržana od proizvođača
	Promjene na ključnoj usluzi izvode se na nepropisan način i/ili nisu adekvatno dokumentirane i/ili odobrene
	Testiranja na segmentu ključne usluge ne provode se na propisani način
	Plan oporavka za segment ključne usluge nije operativno funkcionalan
	Gubitak podataka zbog *ransomware* prijetnji
	Korozijska oštećenja – propuštanje
	Puknuće plinovoda
	Prekid transporta zbog čistača ili uređaja za *in line* inspekciju
	Kvar opreme
	Neadekvatno održavanje postrojenja
	Neadekvatna kvaliteta plina – tekuća tehnološka nečistoća
Političke	Političke prijetnje (građanski neredi, nemiri, ratno stanje, itd.)
	Prijetnje aktivista / lokalne zajednice (demonstracije, prosvjedi, kampanje, blokade itd.)
	Prijetnje stranih sila (špijunaža, krađa informacija itd.)
Kriminal	Prijetnje od vandala (uništavanje, zapaljivost itd.)
	Teroristički / organizirani kriminal (napad eksplozivnim napravama, kemijski, biološki, radiološki napad)
	Krađa opreme
	Uništavanje opreme (namjerno ili nenamjerno)
Okruženje	Prijetnje povezane s potresom (udarni valovi, pukotine zemlje itd.)
	Prijetnje povezane s kopnom (klizišta, klizanje, itd.)
	Prijetnje vulkanske erupcije
	Prijetnje koje se odnose na snagu vjetra (tornado, oluja vjetra, itd.) uključujući kretanje materijala
	Prijetnje vezane uz snijeg (s neba, iz planina, itd.)
	Prijetnje vezane uz vodu (dinamičke) - izljev rijeke, plima, tsunami
	Prijetnje povezane s vatrom (požarna oluja, požar, urbana vatra, vrućina, itd.)
	Prijetnje s neba / iz svemira (munje, asteroidi, itd.)
	Biološke prijetnje (biljke, palo drveće, itd.)
	Zrakoplovne nesreće na zraku i na tlu
	Pomorske nesreće na luci, blizu cijene i izvan obale
	Nesreće na vozilima (automobilska nesreća / višestruka automobilska nesreća / prometna nesreća)
	Željezničke nesreće koje se događaju iznad ili ispod zemlje

	Prijetnje koje proizlaze iz susjednih tvrtki / kuća / osjetljivih ciljeva
	Epidemija koja se odvija na skali koja prelazi međunarodne granice, obično pogađa veliki broj ljudi
	Curenje plina na ključnim lokacijama za izvršavanje ključne usluge
	Curenje vode iz cijevi na ključnim lokacijama za izvršavanje ključne usluge
	Ispad struje na ključnim lokacijama za izvršavanje ključne usluge
	Šteta od glodavaca na ICT opremi
	Nemogućnost kontrole nad fizičkim pristupom opremi koja čini ključnu uslugu
Ugovori	Ugovor ne pokriva potreban opseg zbog greške u pisanju opsega
	Ugovorni dobavljač je izgubio financijsku sposobnost tijekom izvršenja ugovora
	Ugovorni dobavljač je izgubio tehničku sposobnost tijekom izvršenja ugovora
	Ugovorni dobavljač je izgubio stručnu sposobnost tijekom izvršenja ugovora
	Ugovorni dobavljač je izgubio pravnu sposobnost tijekom izvršenja ugovora
	Ugovorni dobavljač je izgubio poslovnu sposobnost tijekom izvršenja ugovora
Zaštita ljudi i imovine	Radovi u zaštitnoj zoni – najavljeni
	Radovi u zaštitnoj zoni – nenajavljeni
Zakonodavne	Zakonodavne i regulatorne prijetnje - čekanje na odluke tijela

4.2 Evidencija imovine

Temeljem podataka koji su prikupljeni kroz navedene aktivnosti prikupljanja podataka, sva informacijska imovina u opsegu detaljno je razrađena i definirana, te potom prema zajedničkom profilu prijetnji (engl. *threat profile*), grupirana u sljedeće kategorije informacijske imovine unutar opsega. Promatrano je ukupno 1496 imenovanih komada imovine u opsegu, a ta imovina grupirana je u ukupno 13 grupa imovine sukladno preporukama ZSIS-a [11] i to kako slijedi.

- Softverska sučelja
- Baze i aplikacije
- Hardver
- Izvedbena dokumentacija servisa
- Ugovori o podršci
- Ključni zaposlenici

- Fizičke lokacije
- Specifična znanja zaposlenika/stručnjaka
- Informacijska imovina
- Poslovni procesi
- Softver i licence
- Dobavljači i njihovi stručnjaci
- Vanjske usluge.

Za provedbu procjene rizika, primjenom „Kataloga prijetnji“ na stvarnu „Evidenciju imovine“ dobije se konačna tablica procjene rizika koja ima tisuće redova i koja bi bila nepodesna za tablični prikaz i bilo kakvu analizu unutar ovog rada. Redoslijed brojeva u imenima servisa ne ide točno po redu jer su određeni servisi ugašeni i više nisu dio „Kataloga servisa“, odnosno dio servisa nije u trenutku evidentiranja ovog „Kataloga servisa“ bio u produkciji već u nekoj fazi projektnog razvoja i implementacije. S obzirom na to da je napomenuto da se iz razloga anonimizacije neće diskutirati imovina ispod nivoa servisa, ugrađivanjem tog dodatnog kriterija dobije se sljedeći prikaz evidencije imovine koji je u svojoj biti pseudonimizirani „Katalog servisa“ tvrtke. Potrebno je uočiti da velika većina servisa sadrži osobne podatke u nekoj od svojih baza podataka. Iako ovaj rad ne diskutira posebno utjecaj zakonskog aspekta zaštite osobnih podataka, važno je primijetiti da ovako ekstenzivna obrada osobnih podataka izlaže tvrtku posljedicama u slučaju kibernetičkog napada ako bi takav napad rezultirao povredom tih osobnih podataka, primjerice njihovom krađom, uništenjem ili javnim objavljivanjem [30] s visokim kaznama za pravne osobe i odgovorne osobe.

Kumulativni prikaz „Evidencije imovine“ nam pokazuje da se 1496 jedinica imovine grupira u ZSIS-ove kategorije imovine, pa se onda dobije prikaz kao u tablici 7. Očekivana je velika količina hardverskih uređaja raspoređenih na velikom broju fizičkih lokacija na trasi nacionalne transportne energetske infrastrukture. Razvidno je da se tvrtka u većoj mjeri oslanja na vanjske dobavljače nego na vlastite zaposlenike zbog velikog volumena raznih sustava koje treba održavati, ali jesno su istaknuta specifična znanja zaposlenih stručnjaka unutar tvrtke koja ih čine teško zamjenjivima, pa takvi stručnjaci imaju bitno različiti profil rizika u odnosu na ostale zaposlenike. Za nastavak ove analize koristit ćemo činjenicu da su sve jedinice imovine evidentirane u „Evidenciji imovine“ raspodijeljene u 49 servisa kojima je vlasnik IT služba, te u 6 servisa kojima je vlasnik OT služba.

Tablica 7 – Evidencija imovine prije sigurnosne inicijative

EVIDENCIJA IMOVINE			
Rb.	**Kategorije imovine**	**Broj jedinica IT služba**	**Broj jedinica OT služba**
1	Softverska sučelja	41	11
2	Baze i aplikacije	61	11
3	Hardver	283	614
4	Izvedbena dokumentacija servisa	49	6
5	Ugovori o podršci	9	11
6	Ključni zaposlenici	6	6
7	Fizičke lokacije	12	109
8	Specifična znanja stručnjaka	4	7
9	Informacijska imovina	41	41
10	Poslovni procesi	11	11
11	Softver i licence	53	53
12	Dobavljači i njihovi stručnjaci	14	14
13	Vanjske usluge	9	9
	SVEUKUPNO:	**593**	**903**
	SVEUKUPNO:	**1496**	

4.3 Prikaz rezultata procjene rizika

Detaljan prikaz rezultata procjene rizika (uključena imovina, vrijednosti imovine, razine rizika za svu imovinu itd.) u zadanom opsegu mogu se pregledati u sljedećoj tablici 8.

Tablica 8 – Procjena rizika prije sigurnosne inicijative

PROCJENA RIZIKA						
Rb.	**ID imovine**	**Kategorija servisa**	**Prosječna vrijednost rizika (raspon 1-9)**	**Broj crvenih rizika po servisu**	**Broj korektivnih radnji po servisu**	**Vlasnik imovine**
1	SISZIOP-N-001	Standardni servis na LAN-u	2,61	9	10	IT služba
2	SISZIOP-Y-002	Standardni servis na LAN-u	2,61	9	10	IT služba
3	SISZIOP-N-003	Standardni servis na LAN-u	2,61	9	10	IT služba
4	SISZIOP-N-004	Standardni servis na LAN-u	2,61	9	10	IT služba
5	SISZIOP-Y-005	Standardni servis na LAN-u	2,55	8	9	IT služba

6	SISZIOP-N-006	Standardni servis na LAN-u	2,61	9	10	IT služba
7	SISZIOP-Y-007	Standardni servis na LAN-u	2,61	9	10	IT služba
8	SISZIOP-N-008	Aplikacija u oblaku	1,38	1	4	IT služba
9	SISZIOP-N-009	Aplikacija u oblaku	1,38	1	4	IT služba
10	SISZIOP-N-010	Standardni servis na LAN-u	2,61	9	10	IT služba
11	SISZIOP-N-011	Standardni servis na LAN-u	2,61	9	10	IT služba
12	SISZIOP-N-012	Standardni servis na LAN-u	2,61	9	10	IT služba
13	SISZIOP-N-013	Standardni servis na LAN-u	2,61	9	10	IT služba
14	SISZIOP-N-014	Standardni servis na LAN-u	2,61	9	10	IT služba
15	SISZIOP-N-015	Standardni servis na LAN-u	2,61	9	10	IT služba
16	SISZIOP-N-016	Standardni servis na LAN-u	2,61	9	10	IT služba
17	SISZIOP-N-017	Standardni servis na LAN-u	2,61	9	10	IT služba
18	SISZIOP-N-018	Standardni servis na LAN-u	2,61	9	10	IT služba
19	SISZIOP-N-019	Standardni servis na LAN-u	2,61	9	10	IT služba
20	SISZIOP-N-020	Aplikacija u oblaku	1,38	1	4	IT služba
21	SISZIOP-N-021	Standardni servis na LAN-u	2,61	9	10	IT služba
22	SISZIOP-N-022	Standardni servis na LAN-u	2,61	9	10	IT služba
23	SISZIOP-N-023	Standardni servis na LAN-u	2,61	9	10	IT služba
24	SISZIOP-N-024	Standardni servis na LAN-u	2,61	9	10	IT služba
25	SISZIOP-N-025	Aplikacija u oblaku	1,38	1	4	IT služba
26	SISZIOP-N-026	Standardni servis na LAN-u	2,61	9	10	IT služba
27	SISZIOP-N-028	Standardni servis na LAN-u	2,61	9	10	IT služba
28	SISZIOP-N-029	Standardni servis na LAN-u	2,61	9	10	IT služba
29	SISZIOP-N-030	Standardni servis na LAN-u	2,61	9	10	IT služba
30	SISZIOP-N-032	Standardni servis na LAN-u	2,61	9	10	IT služba
31	SISZIOP-N-033	Standardni servis na LAN-u	2,61	9	10	IT služba
32	SISZIOP-N-034	Standardni servis na LAN-u	2,61	9	10	IT služba
33	SISZIOP-N-035	Standardni servis na LAN-u	2,61	9	10	IT služba
34	SISZIOP-N-036	Standardni servis na LAN-u	2,61	9	10	IT služba
35	SISZIOP-N-037	Standardni servis na LAN-u	2,61	9	10	IT služba
36	SISZIOP-N-038	Aplikacija u oblaku	1,38	1	4	IT služba
37	SISZIOP-N-039	Standardni servis na LAN-u	2,61	9	10	IT služba
38	SISZIOP-N-040	Standardni servis na LAN-u	2,61	9	10	IT služba
39	SISZIOP-N-043	Aplikacija u oblaku	1,38	1	4	IT služba
40	SISZIOP-N-044	Aplikacija u oblaku	1,38	1	4	IT služba
41	SISZIOP-N-045	Aplikacija u oblaku	2,61	9	10	IT služba
42	SISZIOP-N-046	Aplikacija u oblaku	1,38	1	4	IT služba
43	SISZIOP-N-047	Aplikacija u oblaku	1,38	1	4	IT služba
44	SISZIOP-N-048	Aplikacija u oblaku	1,49	1	6	IT služba
45	SISZIOP-N-049	Aplikacija u oblaku	1,49	1	6	IT služba
46	SISZIOP-Y-050	Aplikacija u oblaku	1,49	1	6	IT služba
47	SISZIOP-N-051	Aplikacija u oblaku	1,38	1	4	IT služba
48	SISZIOP-Y-052	Aplikacija u oblaku	1,49	1	6	IT služba

49	SISZIOP-Y-053	Aplikacija u oblaku	1,49	1	6	IT služba
50	SUTSIPTK-Y-001	Ključni servis za poslovanje	2,07	3	11	OT služba
51	SUTSIPTK-Y-002	Ključni servis za poslovanje	2,05	3	12	OT služba
52	SUTSIPTK-Y-003	Ključni servis za poslovanje	2,01	3	11	OT služba
53	SUTSIPTK-Y-004	Ključni servis za poslovanje	2,02	3	12	OT služba
54	SUTSIPTK-Y-005	Ključni servis za poslovanje	2,03	3	12	OT služba
55	SUTSIPTK-Y-006	Ključni servis za poslovanje	1,81	0	9	OT služba
PROSJEČNO:			**2,22**	**6,09**	**8,65**	

Prosječna vrijednost rizika (stupac „Prosječna vrijednost rizika“) računa se na način da se za svaki pojedini servis uzme vrijednost procijenjenog rizika za svaku na taj servis primjenjivu prijetnju, pa se taj zbroj podijeli s brojem na taj rizik primjenjivih prijetnji. Primjer: servis SISZIOP-N-001 imao je u ovoj procjeni rizika 82 primjenjive prijetnje (vidljivo samo u bazi podataka procjene rizika), zbroj svih rizika za ostvarenje tih primjenjivih prijetnji bio je 214 (vidljivo samo u bazi podataka procjene rizika), što dijeljenjem daje prosječnu vrijednost rizika od 2,61.

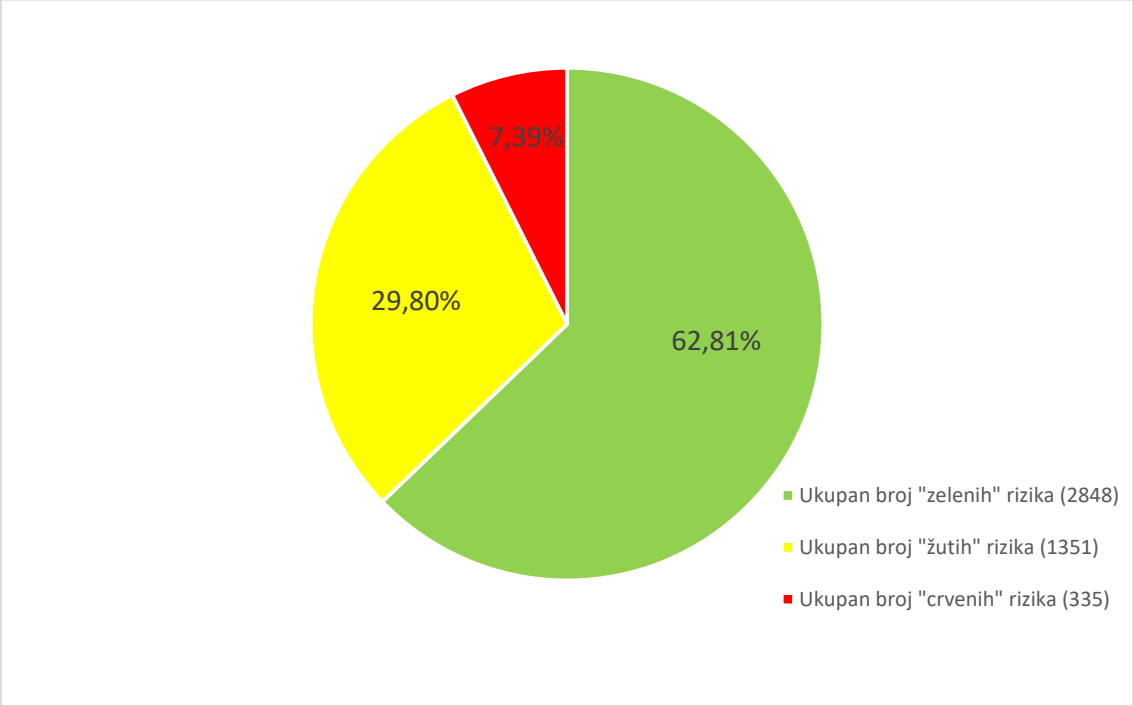
Broj visokih rizika (stupac „Broj crvenih rizika“) računa se na način da se izbroje sve na ovaj servis primjenjive prijetnje čiji je procijenjeni rizik 6 ili veći (maksimalno 9). Primjer: servis SISZIOP-N-001 imao je u ovoj procjeni rizika 82 primjenjive prijetnje s nekom procijenjenom vrijednošću rizika, a za 9 od tih 82 prijetnje rizik se pokazao da je 6 ili većom, pa jednostavnim brojanjem zaključujemo da ovaj servis ima 9 „crvenih“ rizika.

Broj korektivnih radnji (stupac „Broj korektivnih radnji po servisu“) računa se na način da se izbroje sve korektivne radnje otvorene u sklopu ove procjene rizika, a čiji je uzrok sadržan u postojanju „crvenih“ rizika vezanih uz svaki pojedini servis. Primjer: servis SISZIOP-N-001 imao je u ovoj procjeni rizika 9 primjenjivih prijetnji s procijenjenom vrijednošću rizika od 6 ili većom. Provjerom u "Logu korektivnih radnji" možemo ustanoviti da su ti rizici adresirani sa 10 korektivnih radnji, što je onda ubačeno u ovu tablicu. Slučajevi kad je za neki servis u tablici indiciran veći broj korektivnih radnji nego „crvenih“ rizika ukazuje na okolnost da su tehnički voditelj i poslovni koordinator promatranog servisa otvorili i dodatne korektivne radnje za neke od procijenjenih „žutih“ rizika. U istom primjeru servisa SISZIOP-N-001 imamo 9 „crvenih rizika“, 10 korektivnih radnji, a što znači da je i jedan „žuti“ rizik rezultirao otvaranjem odgovarajuće korektivne radnje.

Svi servisi koji ovdje predstavljaju evidenciju imovine s manjim odstupanjima se po profilu rizika mogu razvrstati u tri kategorije:

- svih šest servisa OT mreže (SUTSIPTK-Y-001 do SUTSIPTK-Y-006, koji se svi smatraju ključnima za poslovanje jer su nužni za rad osnovnih poslovnih procesa na terenu imaju nizak prosječan rizik od 2,00; izračun se radi na način da se za sve servise OT mreže zbroje vrijednosti „Prosječne vrijednosti rizika“ (ukupno 11,99) i podijele s brojem takvih servisa (ima ih 6)
- standardne uredske aplikacije smještene na LAN-u tvrtke („Kategorija servisa“ je „Standardni servis na LAN-u“, vlasnik IT služba), prosječan rizik iznosi 2,61; izračun se radi na način da se za sve servise kategorije „Standardni servis na LAN-u“ zbroje vrijednosti „Prosječne vrijednosti rizika“ (ukupno 86,07) i podijele s brojem takvih servisa (ima ih 33)
- aplikacije ili izmještene u računalni oblak u aranžmanu tvrtke ili izmještene kod vanjskih dobavljača koji ih onda održavaju opet u nekom oblaku (IT služba, niži nivoi rizika).

Generalno se može smatrati da je rizik na promatranoj imovini u kvalitetno kontroliranom stanju, odnosno da je riječ o stabilnom stanju rizika koje je rezultat višegodišnjeg promišljanja i kvalitetnog upravljanja rizicima, a što možemo vidjeti u činjenici da niti jedan servis u prosjeku nema situaciju koja bi tražila neke hitne zahvate, odnosno svi su servisi u prosjeku „zeleni“ prema tablici vrijednosti rizika. Broj „crvenih“ rizika po servisu je to veći što mu je prosjek rizika veći, što je i matematički logično. Interesantno je uočiti da je u svim servisima iskazan veći broj korektivnih radnji od broja crvenih rizika, a što ukazuje da su procjenitelji rizika (vlasnici imovine) korektivne radnje dodavali ne samo „crvenim“, nego i nekim „žutim“ servisima koje su smatrali posebno problematičnima.



Slika 2 - Prikaz procjene rizika obzirom na visinu rizika prije ZTA

Slika 2 pokazuje grafički prikaz procjene rizika prije uvođenja sigurnosne inicijative, a s promatrano s obzirom na procijenjenu visinu rizika i to kumulativno za sve servise. Dok je u naravi riječ o velikoj tablici s tisućama redova u Microsoft Excelu, ovakav prikaz nam daje mogućnost uočiti razdiobu broja rizika po "bojama", odnosno koliki su udjeli "crvenih", "žutih" i "zelenih" rizika u ukupnom broju procijenjenih rizika. Od ukupno 4534 promatranih rizika gledanih kao kombinacija parova evidencije imovine (55 servisa u „Katalogu servisa") i prijetnje (82,44 prosječno promatrane prijetnje po servisu):

- na 2848 rizika (62,81%) analiza je rezultirala s niskim (prihvatljivim) vrijednostima rizika („zeleni" rizici),
- na 1351 rizika (29,80%) analiza je rezultirala s graničnim (granično prihvatljivim) vrijednostima rizika („žuti" rizici),
- na 335 rizika (7,39%) analiza je rezultirala s visokim (neprihvatljivim) vrijednostima rizika („crveni" rizici).

Kao posljedica 335 „crvenih" rizika, identificirano je 476 korektivnih radnji koje vlasnici rizika moraju otvoriti u logu korektivnih i preventivnih radnji ISMS-a tvrtke, uz ogradu da će stvarno otvorenih korektivnih radnji (nezavisnih) biti svakako značajno manje jer će pojedine korektivne radnje istovremeno adresirati više identificiranih „crvenih" rizika.

4.4 Plan obrade rizika i određivanje protumjera

Prema popisu rizika koji zahtijevaju daljnju obradu, „crvenim“ odnosno visokim rizicima po automatizmu su dodijeljeni vlasnici rizika (ista organizacijska jedinica koja je i vlasnik servisa gdje su prepoznati ti „crveni“ rizici), te su od strane vlasnika rizika predložene određene mjere koje bi svojem implementacijom mogle dovesti do povoljnijeg profila prijetnje. Za svaki takav slučaj definirano je sljedeće:

- ID korektivne radnje
- relevantna kontrola iz ISO27001 [55]
- opis korektivne radnje
- datum otvaranja radnje
- izvor radnje (kako je korektivna radnja nastala ili tko ju je otvorio)
- zadužena osoba (imenom i prezimenom)
- rok za izvršenje
- način postupanja po rizicima
- stvarni datum izvršenja,
- odobravatelj (potvrđuje da je korektivna radnja zaista izvršena)
- budžet radnje.

Strategija upravljanja rizicima u tvrtki predviđa četiri načina postupanja po rizicima [56]:

- izbjegavanje rizika (engl. *risk avoidance*) – tako da se određene aktivnosti izvode drugačije ili se ne izvode
- prijenos rizika (engl. *risk tranference*) – putem konvencionalnog osiguranja ili prijenosom na treću osobu, tipično u procesu eksternalizacije (engl. *outsourcing*), npr. na ugovornog partnera
- prihvaćanje rizika (engl. *risk acceptance*) – kada su mogućnosti za poduzimanje mjera ograničene ili iziskuju prevelike troškove u odnosu na korist, s tim da rizik treba pratiti i osigurati da ostane na prihvatljivoj razini
- smanjivanje/ublažavanje rizika (engl. *risk reduction*) – poduzimanje mjera da se smanji vjerojatnost ili učinak rizika.

Analizom rizika informacijske sigurnosti generirane korektivne radnje vode se i prate u „Logu korektivnih radnji“. Rezultati provedenih analiza su prikazani u sljedećoj tablici 9.

Tablica 9 – Korektivne radnje prije sigurnosne inicijative

KOREKTIVNE RADNJE					
R. br.	**ID Nezavisne korektivne radnje**	**Prosječna vrijednost rizika**	**"Crvenih" rizika po servisu**	**Budžet za nezavisnu korektivnu radnju**	**Ukupni budžet za sve nezavisne korektivne radnje**
1	KR-2018-SISZIOP-004	2,24	6,53	€ 234.000,00	€ 2.344.000,00
2	KR-2018-SISZIOP-095			€ 710.000,00	
3	KR-2018-SISZIOP-096			€ 525.000,00	
4	KR-2018-SISZIOP-097			€ 385.000,00	
5	KR-2018-SISZIOP-098			€ 490.000,00	
6	KR-2018-SUTSIPTK-001	2,00	2,50	€ 311.000,00	€ 3.895.600,00
7	KR-2018-SUTSIPTK-002			€ 233.000,00	
8	KR-2018-SUTSIPTK-003			€ 115.000,00	
9	KR-2018-SUTSIPTK-004			€ 971.500,00	
10	KR-2018-SUTSIPTK-005			€ 411.000,00	
11	KR-2018-SUTSIPTK-006			€ 69.000,00	
12	KR-2018-SUTSIPTK-007			€ 545.000,00	
13	KR-2018-SUTSIPTK-008			€ 433.000,00	
14	KR-2018-SUTSIPTK-009			€ 196.000,00	
15	KR-2018-SUTSIPTK-010			€ 611,100,00	
		2,22	**6,09**	**€ 6.239.600,00**	**€ 6.239.600,00**

Primjer: prvih pet nezavisnih korektivnih radnji (redni brojevi 1-5 u stupcu „R.br.“; ID nezavisne korektivne radnje KR-2018-SISZIOP-004, KR-2018-SISZIOP-095, KR-2018-SISZIOP-096, KR-2018-SISZIOP-097, KR-2018-SISZIOP-098) imaju prosječnu vrijednost rizika 2,243 što je izračunato zbrajanjem prosječne vrijednosti rizika za svaki od 49 servisa IT službe (podaci u stupcu tablice 8, stupac “Prosječna vrijednost rizika”) i dijeljenjem s 49 (broj promatranih servisa). Također, svi servisi IT službe imaju prosječno 6,531 „crvenih“ rizika po servisu što je izračunato zbrajanjem prosječnog broja „crvenih“ rizika za svaki od 49 servisa IT službe (podaci u stupcu tablice 8, stupac “ Broj crvenih rizika po servisu ”) i dijeljenjem s 49 (broj promatranih servisa). Ovime je potvrđeno da su vlasnici rizika otvorili pet nezavisnih korektivnih radnji kojima su htjeli adresirati uzroke svih „crvenih“ i dijela „žutih“ rizika za sve servise IT službe (za one „žute“ rizike gdje su otvarane korektivne radnje). Zbrajanjem pojedinačnih budžeta tih pet nezavisnih korektivnih radnji (stupac „Budžet za nezavisnu korektivnu radnju“) dobiva se kumulativni budžet za adresiranje tih pet nezavisnih korektivnih radnji od 2.344.000,00 € (stupac “Ukupni budžet za sve nezavisne korektivne radnje”).

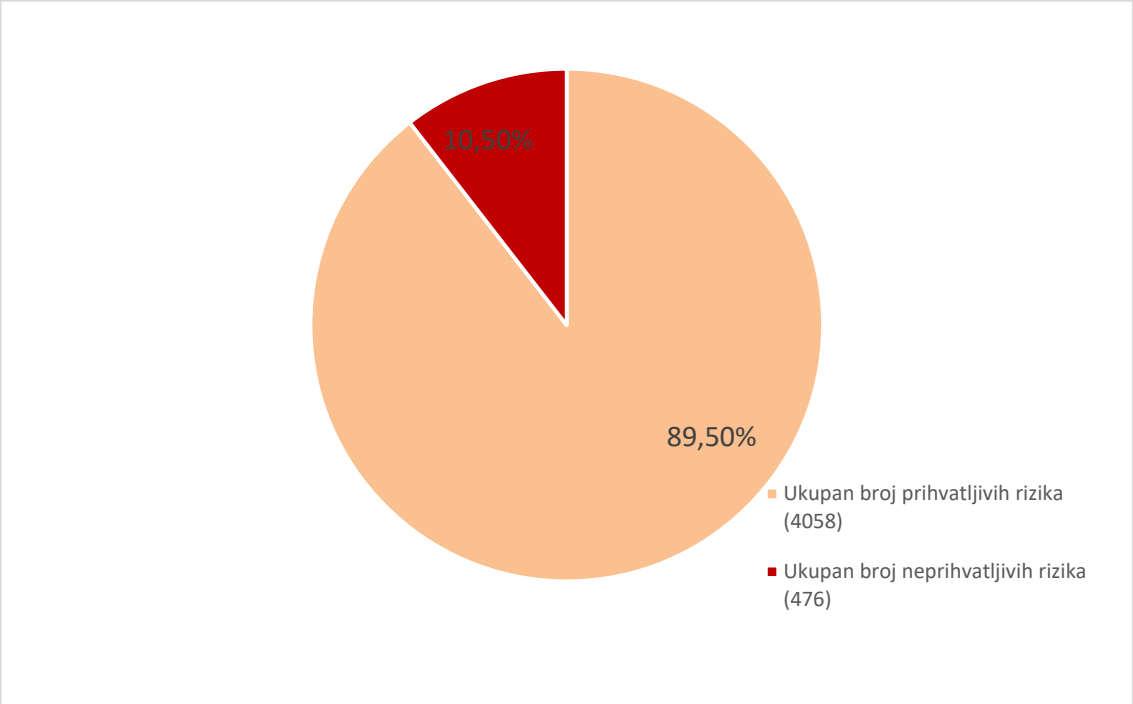
Uočljivo je da je OT služba u određenoj prednosti ispred IT službe po zrelosti svojih servisa u sigurnosnom smislu. Ne samo da je prosječni rizik OT servisa značajno niži (2,000) u odnosu na IT službu (2,243), već je vidljivo da po servisu OT služba definira značajno manje „crvenih rizika“ (2,500) u odnosu na broj „crvenih“ rizika po servisu IT službe (6,531) i otvara puno više nezavisnih korektivnih radnji (10, redni brojevi nezavisnih korektivnih radnji 6-15) u odnosu na IT službu (5, redni brojevi nezavisnih korektivnih radnji 1-5), definiranih kao korektivna radnja s jedinstvenim uzrokom rizika koji druge korektivne radnje ne dijele; OT služba za 7 svojih servisa definira 10 nezavisnih korektivnih radnji, dok IT služba za 49 svojih servisa identificira samo pet nezavisnih korektivnih radnji. Ovo ukazuje na strukturne probleme kod IT servisa gdje velika većina servisa dijeli određeni zajednički broj problema koji se očigledno mogu riješiti implementacijom pojedine zajedničke korektivne radnje. Veći broj nezavisnih korektivnih radnji opravdava i veći budžet za adresiranje tih korektivnih radnji kod OT službe (3.895.600,00 €, stupac “Ukupni budžet za sve nezavisne korektivne radnje” za stupac „R.br“ 6-15) u odnosu na IT službu (2.344.000,00 €, stupac “Ukupni budžet za sve nezavisne korektivne radnje” za stupac „R.br“ 1-5). Relativno veliki prosjek procijenjenog troška po svakoj nezavisnoj korektivnoj radnji obje službe ukazuje da „crveni“ rizici obje službe nisu rješivi jednostavnim organizacijskim, procesnim ili kadrovskim korekcijama, već traže ozbiljne investicije u tehnologiju. Uzroci nisu zasebno iskazani u priloženim tablicama, ali uključuju upravo razloge zbog kojih je i došlo do pokretanja sigurnosne inicijative: nedostatne tehničke kontrole za upravljanje privilegiranim računima, nemogućnost anonimizacije klijentskih računala kod pristupa pojedinim servisima na Internetu, nemogućnost filtriranja ulaznog prometa na aplikativnom nivou, nesposobnost detekcije malicioznih procesa na klijentskim računalima i automatiziranog zaustavljanja tih procesa, nemogućnost stalnog nadzora nad logovima uređaja na mreži i automatiziranog, orkestriranog odgovora na pojedine scenarije, itd. Sve su ovo legitimni rizici koje moderna mreža treba imati adresirane na strukturiran i konzistentan način, a taj okvir za implementaciju je identificiran kao ZTA.

Od iskazanih 127 korektivnih radnji (zbroj stupca „Broj korektivnih radnji po servisu“ u tablici 9.), tablica 10. pokazuje da je ukupan broj nezavisnih korektivnih radnji samo 15, što u praktičnom smislu znači da se s relativno malim brojem skupih zahvata mogu adresirati svi „crveni rizici“ definirani kroz procjenu rizika i za IT službu i za OT službu.

4.5 Popis prihvatljivih rizika

Od ukupno 4534 promatranih rizika gledanih kao kombinacija parova evidencije imovine i prijetnje servisa (vidljivo samo u bazi podataka procjene rizika), na osnovu kriterija za prihvaćanje rizika, procjena rizika je na 4058 rizika (89,50%) rezultirala s niskim (prihvatljivim) vrijednostima rizika (zelena boja), odnosno srednjim vrijednostima rizika (žuta boja) uz napomenu da ovo uključuje samo one vrijednosti „žutih“ rizika gdje su vlasnici rizika odlučili ne otvarati korektivne radnje. Ovi rizici mogu se smatrati prihvatljivim rizicima. Iz razloga praktičnosti sam popis ovih rizika nije zasebno uključen u ovaj rad, no vrijedi spomenuti da su ovi rizici, osim što su prihvatljivi prije implementacije sigurnosne inicijative, svakako očekivani da budu prihvatljivi i nakon njezine implementacije. Drugim riječima, prihvatljivi rizici nisu rizici na kojima će se vidjeti eventualni očekivani pozitivni efekti implementacije sigurnosne inicijative na profil rizika tvrtke.

Preostalih 476 rizika (10,50%) uključuju „crvene“ rizike s visokim (neprihvatljivim) vrijednostima rizika, odnosno rizike sa srednjim vrijednostima rizika (žuta boja) uz napomenu da ovo uključuje samo one vrijednosti „žutih“ rizika gdje su vlasnici rizika odlučili otvarati korektivne radnje. Ovo je prikazano na slici 3 kao grafički prikaz procjene rizika prije uvođenja sigurnosne inicijative kumulativno za sve servise, a obzirom na prihvatljivost rizika.



Slika 3 - Prikaz procjene rizika prije ZTA obzirom na prihvatljivost rizika

4.6 Određivanje preostalog rizika

Preostali rizik je onaj rizik koje je uočen i prelazi prag prihvatljive razine rizika, ali se predložene kontrole financijski ne isplate implementirati, a navedeni rizici ne mogu rezultirati troškom većim od troška implementacije predložene kontrole, kršenjem zakona ili regulative ili ljudskim ozljedama. Logika u evaluaciji kriterija je li neki rizik preostali rizik je prikazana u sljedećoj tablici, te je vidljivo da je preostali rizik samo jedan (uzrok planiran za tretiranje kroz korektivnu radnju KR-2018-SUTSIPTK-006 kod OT službe). Prema internoj proceduri, zadužena osoba za tu korektivnu radnju napravila je analizu mogućih rješenja predmetne korektivne radnje i predložila ih odobravatelju (tipično rukovoditelj OT službe) koji je ponuđena rješenja i prateće budžete procijenio neisplativima obzirom na vjerojatnost i utjecaj ostvarenja rizika u odnosu na predloženi trošak korektivne radnje, te je korektivna radnja zatvorena bez realizacije. Shodno tome, ova korektivna radnja nije išla u implementaciju, a povezani rizik prihvaćen je od strane rukovodstva tvrtke odgovarajućom pisanom odlukom.

Tablica 10 – Preostali rizik prije sigurnosne inicijative

PREOSTALI RIZIK						
R.br.	**Korektivna radnja**	**Vlasnik korektivne radnje**	**Trošak ostvarenja rizika bitno manji od troška implementacije mjere**	**Moguće kršenje zakona ili regulative**	**Moguće ljudske ozljede ili smrt**	**Preostali rizik**
1	KR-2018-SISZIOP-004	IT služba	NE	NE	NE	**NE**
2	KR-2018-SISZIOP-095	IT služba	NE	NE	NE	**NE**
3	KR-2018-SISZIOP-096	IT služba	NE	NE	NE	**NE**
4	KR-2018-SISZIOP-097	IT služba	NE	NE	NE	**NE**
5	KR-2018-SISZIOP-098	IT služba	NE	NE	NE	**NE**
6	KR-2018-SUTSIPTK-001	OT služba	NE	NE	NE	**NE**
7	KR-2018-SUTSIPTK-002	OT služba	NE	NE	NE	**NE**
8	KR-2018-SUTSIPTK-003	OT služba	NE	NE	NE	**NE**
9	KR-2018-SUTSIPTK-004	OT služba	NE	NE	NE	**NE**
10	KR-2018-SUTSIPTK-005	OT služba	NE	NE	NE	**NE**
11	KR-2018-SUTSIPTK-006	OT služba	DA	NE	NE	**DA**
12	KR-2018-SUTSIPTK-007	OT služba	NE	NE	NE	**NE**
13	KR-2018-SUTSIPTK-008	OT služba	NE	NE	NE	**NE**
14	KR-2018-SUTSIPTK-009	OT služba	NE	NE	NE	**NE**
15	KR-2018-SUTSIPTK-010	OT služba	NE	NE	NE	**NE**

4.7 Stupanj zrelosti u CISA ZTMM modelu prije ZTA

Američka agencija za kibernetičku sigurnost kritične infrastrukture CISA (engl. *Cybersecurity and Infrastructure Security Agency*) je izradila draft verziju svoje vlastitog modela [57] za usvajanje ZTA kao vodič i pomoć američkim operatorima kritične infrastrukture na putu do nultog povjerenja. CISA-in „Model Zrelosti Nultog Povjerenja“ (engl. „*Zero Trust Maturity Model*“) koristi tri diskretna nivoa zrelosti da bi razlikovao rastuće nivoe zaštite, detalja i kompleksnosti uspostavljenih kontrola na područjima zaštite identiteta, uređaja, mreže, aplikativnog opterećenja i podataka. Slika 4. prikazuje grafičku interpretaciju ZTMM.

	IDENTITET	UREĐAJ	MREŽA / OKRUŽENJE	APLIKATIVNO OPTEREĆENJE	PODACI
TRADICIONALNI	• zaporka ili MFA • ograničeno upravljanje rizicima	• ograničen pogled u zakonsku sukladnost • jednostavna evidencija imovine	• velika makrosegmentacija • minimalna enkripcija unutrašnjeg i vanjskog mrežnog prometa	• pristup je baziran na lokalnoj autorizaciji • minimalna integracija s radnim tijekom • ograničen pristup servisima u oblaku	• loša evidencija podataka • statička kontrola • nema enkripcije podataka
NAPREDNI	•MFA • djelomična federacija identiteta sa servisima u oblaku i servisima na mreži	• primijenjen obvezni pogled u zakonsku sukladnost • pristup podacima ovisi o sigurnosnoj razinu uređaja u trenutku inicijalnog pristupa	• velika makrosegmentacija • osnovna analitika	• pristup je baziran na centralnoj autorizaciji • bazična integracija s radnim tijekom	• pristup kontrolama je uz "najmanja pristupna prava" • podaci u oblaku su enkriptirani u mirovanju
OPTIMALNI	•kontinuirana validacija • analiza strojnim učenjem u stvarnom vremenu	• kontinuirani sigurnosni i validacijski nadzor nad uređajem • pristup podacima ovisi o sigurnosnoj analitici u stvarnom vremenu	• potpuno distribuirani mikroparametri ulaza i izlaza • zaštita od prijetnji putem strojnog učenja • sav promet je enkriptiran	• pristup se kontinuirano autorizira • snažna integracija s radnim tijekom	• dinamička podrška • svi podaci su enkriptirani
	VIDLJIVOST I ANALITIKA	AUTOMATIZACIJA I OKRESTRACIJA			UPRAVLJANJE

Slika 4 - Stupanj zrelosti u CISA ZTMM modelu prije ZTA

Bez ulaženja u detalje po pojedinim vertikalama modela iz sigurnosnih razloga, možemo konstatirati da je tvrtka prije uvođenja sigurnosne inicijative po svih pet područja postigla „tradicionalnu“ ocjenu zrelosti, odnosno najniži stupanj zrelosti u ovom modelu.

5. PROFIL RIZIKA NAKON UVOĐENJA SIGURNOSNE INICIJATIVE

Krajem 2022. godine procjena rizika ponovljena je koristeći ista tri ključna elementa KPMG Advisory metodologije (katalog prijetnji, evidencija imovine, procjena rizika) kao i pet godina ranije.

5.1 Katalog prijetnji

Katalog prijetnji je nakon uvođenja sigurnosne inicijative proširen za određeni broj novih prijetnji, no sve naknadno dodane prijetnje vezane su uz aplikativne servise koji su uvedeni u poslovanje tvrtke nakon početka uvođenja sigurnosne inicijative. Sve takve prijetnje nemaju vjerojatnost realizacije veću od nula osim na aplikativnim servisima kojima su inherentni, pa takve prijetnje nisu iz praktičnih razloga razmatrane tijekom evaluacije profila rizika nakon uvođenja sigurnosne inicijative. S obzirom na to da „*Gas Infrastructure Europe*“ od 2014. godine nije dao nove preporuke za operatere transporta plina za Europsku Uniju, niti je ažurirao svoj preporučeni popis prijetnji, za potrebe ovog rada korišten je isti katalog prijetnji kao i za evaluaciju stanja prije uvođenja sigurnosne inicijative.

5.2 Evidencija imovine

Evidencija imovine je u razdoblju od pet godina koliko je trajala implementacija sigurnosne inicijative narasla s 55 na 83 servisa, i to na 72 servisa IT službe i 11 servisa OT službe. Povećanje samog broja servisa za 28 možemo promotriti kao rezultat tri zasebne inicijative uvođenja u poslovanje tvrtke:

- Zakonske i regulatorne obveze, osam novih servisa (vezano uz elektroničke račune, digitalnu arhivu, razmjenu podataka o rezervaciji kapaciteta na europskoj burzi, zaštitu osobnih podataka, itd.)
- Digitalna transformacija poslovnih procesa, deset novih servisa (digitalizacija poslovnih procesa koji su se zasnivali na brojnim papirnatim obrascima i zapisima)
- Provedba ZTA sigurnosne inicijative, deset novih servisa.

Povećanjem broja servisa ukupan broj jedinica imovine je povećan s 1496 na 1848, odnosno za 23,53%. Evidencija imovine nakon uvođenja sigurnosne inicijative prikazana je u tablici 11. Promijenila se i nomenklatura označavanja servisa tako da je malo pojednostavljena, pri čemu su postojeći servisi retroaktivno preimenovani.

„Evidencija imovine“ kumulativno pokazuje da je ukupno 1848 jedinica imovine grupirano u ZSIS-ove kategorije imovine, pa se onda dobije prikaz kao u tablici 11.

Tablica 11 – Evidencija imovine nakon sigurnosne inicijative

EVIDENCIJA IMOVINE			
Rb.	**Kategorije imovine**	**Broj jedinica IT služba**	**Broj jedinica OT služba**
1	Softverska sučelja	51	21
2	Baze i aplikacije	73	21
3	Hardver	386	723
4	Izvedbena dokumentacija servisa	72	11
5	Ugovori o podršci	16	17
6	Ključni zaposlenici	6	6
7	Fizičke lokacije	12	109
8	Specifična znanja stručnjaka	4	7
9	Informacijska imovina	52	49
10	Poslovni procesi	11	11
11	Softver i licence	67	62
12	Dobavljači i njihovi stručnjaci	21	18
13	Vanjske usluge	11	11
	SVEUKUPNO:	**782**	**1066**
	SVEUKUPNO:	**1848**	

Uočava se da je količina imovine značajno narasla u samo pet godina uvođenja sigurnosne inicijative, ali ne samo zbog nje. Već smo na analizi broja servisa konstatirali da su brojne zakonske i regulatorne obveze, te zahtjevi digitalne transformacije rezultirali kako u brojnim novim servisima, tako i u brojnim novim jedinicama imovine od kojih se ti servisi sastoje.
Za nastavak ove analize koristit ćemo činjenicu da su sve jedinice imovine evidentirane u „Evidenciji imovine“ raspodijeljene u 72 servisa kojima je vlasnik IT služba, te u 11 servisa kojima je vlasnik OT služba.

5.3 Prikaz rezultata procjene rizika

Detaljan prikaz rezultata procjene rizika nakon provedene implementacije sigurnosne inicijative mogu se pregledati u sljedećoj tablici 12.

Tablica 12 – Procjena rizika nakon sigurnosne inicijative

PROCJENA RIZIKA						
Rb.	**ID imovine**	**Kategorija servisa**	**Prosječna vrijednost rizika (raspon 1-9)**	**Broj crvenih rizika po servisu**	**Broj korektivnih radnji po servisu**	**Vlasnik imovine**
1	SISZIOP-001	Standardni servis na LAN-u	2,11	2	2	IT služba
2	SISZIOP-002	Standardni servis na LAN-u	2,11	2	2	IT služba
3	SISZIOP-003	Standardni servis na LAN-u	2,11	2	2	IT služba
4	SISZIOP-004	Standardni servis na LAN-u	2,11	2	2	IT služba
5	SISZIOP-005	Standardni servis na LAN-u	2,55	3	3	IT služba
6	SISZIOP-006	Standardni servis na LAN-u	2,11	2	2	IT služba
7	SISZIOP-007	Standardni servis na LAN-u	2,11	2	2	IT služba
8	SISZIOP-008	Aplikacija u oblaku	1,38	0	0	IT služba
9	SISZIOP-009	Aplikacija u oblaku	1,38	0	0	IT služba
10	SISZIOP-010	Standardni servis na LAN-u	2,11	2	2	IT služba
11	SISZIOP-011	Standardni servis na LAN-u	2,11	2	2	IT služba
12	SISZIOP-012	Standardni servis na LAN-u	2,11	2	2	IT služba
13	SISZIOP-013	Standardni servis na LAN-u	2,11	2	2	IT služba
14	SISZIOP-014	Standardni servis na LAN-u	2,11	2	2	IT služba
15	SISZIOP-015	Standardni servis na LAN-u	2,11	2	2	IT služba
16	SISZIOP-016	Standardni servis na LAN-u	2,11	2	2	IT služba
17	SISZIOP-017	Standardni servis na LAN-u	2,11	2	2	IT služba
18	SISZIOP-018	Standardni servis na LAN-u	2,11	2	2	IT služba
19	SISZIOP-019	Standardni servis na LAN-u	2,11	2	2	IT služba
20	SISZIOP-020	Aplikacija u oblaku	1,10	0	0	IT služba
21	SISZIOP-021	Standardni servis na LAN-u	2,11	2	2	IT služba
22	SISZIOP-022	Standardni servis na LAN-u	2,11	2	2	IT služba
23	SISZIOP-023	Standardni servis na LAN-u	2,11	2	2	IT služba
24	SISZIOP-024	Standardni servis na LAN-u	2,11	2	2	IT služba
25	SISZIOP-025	Aplikacija u oblaku	1,10	0	0	IT služba
26	SISZIOP-026	Standardni servis na LAN-u	2,11	2	2	IT služba
27	SISZIOP-027	Standardni servis na LAN-u	2,11	2	2	IT služba
28	SISZIOP-028	Standardni servis na LAN-u	2,11	2	2	IT služba
29	SISZIOP-029	Standardni servis na LAN-u	2,11	2	2	IT služba
30	SISZIOP-030	Standardni servis na LAN-u	2,11	2	2	IT služba
31	SISZIOP-031	Standardni servis na LAN-u	2,11	2	2	IT služba
32	SISZIOP-032	Standardni servis na LAN-u	2,11	2	2	IT služba
33	SISZIOP-033	Standardni servis na LAN-u	2,11	2	2	IT služba
34	SISZIOP-034	Standardni servis na LAN-u	2,11	2	2	IT služba
35	SISZIOP-035	Standardni servis na LAN-u	2,11	2	2	IT služba

36	SISZIOP-036	Standardni servis na LAN-u	2,11	2	2	IT služba
37	SISZIOP-037	Standardni servis na LAN-u	2,11	2	2	IT služba
38	SISZIOP-038	Aplikacija u oblaku	1,10	0	0	IT služba
39	SISZIOP-039	Standardni servis na LAN-u	2,11	2	2	IT služba
40	SISZIOP-040	Standardni servis na LAN-u	2,11	2	2	IT služba
41	SISZIOP-041	Standardni servis na LAN-u	2,11	2	2	IT služba
42	SISZIOP-042	Standardni servis na LAN-u	2,11	2	2	IT služba
43	SISZIOP-043	Aplikacija u oblaku	1,10	0	0	IT služba
44	SISZIOP-044	Aplikacija u oblaku	1,10	0	0	IT služba
45	SISZIOP-045	Aplikacija u oblaku	2,11	2	2	IT služba
46	SISZIOP-046	Aplikacija u oblaku	1,10	0	0	IT služba
47	SISZIOP-047	Aplikacija u oblaku	1,10	0	0	IT služba
48	SISZIOP-048	Aplikacija u oblaku	1,10	0	0	IT služba
49	SISZIOP-049	Aplikacija u oblaku	1,10	0	0	IT služba
50	SISZIOP-050	Aplikacija u oblaku	1,10	0	0	IT služba
51	SISZIOP-051	Aplikacija u oblaku	1,10	0	0	IT služba
52	SISZIOP-052	Aplikacija u oblaku	1,10	0	0	IT služba
53	SISZIOP-053	Aplikacija u oblaku	1,10	0	0	IT služba
54	SISZIOP-054	Aplikacija u oblaku	1,10	0	0	IT služba
55	SISZIOP-055	Aplikacija u oblaku	1,10	0	0	IT služba
56	SISZIOP-056	Aplikacija u oblaku	1,10	0	0	IT služba
57	SISZIOP-057	Aplikacija u oblaku	1,10	0	0	IT služba
58	SISZIOP-058	Aplikacija u oblaku	1,10	0	0	IT služba
59	SISZIOP-059	Aplikacija u oblaku	2,11	2	2	IT služba
60	SISZIOP-060	Aplikacija u oblaku	2,11	2	2	IT služba
61	SISZIOP-061	Aplikacija u oblaku	1,10	0	0	IT služba
62	SISZIOP-062	Aplikacija u oblaku	1,10	0	0	IT služba
63	SISZIOP-063	Aplikacija u oblaku	1,10	0	0	IT služba
64	SISZIOP-064	Aplikacija u oblaku	1,10	0	0	IT služba
65	SISZIOP-065	Aplikacija u oblaku	1,10	0	0	IT služba
66	SISZIOP-066	Aplikacija u oblaku	1,10	0	0	IT služba
67	SISZIOP-067	Aplikacija u oblaku	2,11	2	2	IT služba
68	SISZIOP-068	Aplikacija u oblaku	2,11	2	2	IT služba
69	SISZIOP-069	Aplikacija u oblaku	2,11	2	2	IT služba
70	SISZIOP-070	Aplikacija u oblaku	2,11	2	2	IT služba
71	SISZIOP-071	Aplikacija u oblaku	2,11	2	2	IT služba
72	SISZIOP-072	Aplikacija u oblaku	2,11	2	2	IT služba
73	SUTSIPTK-001	Ključni servis za poslovanje	1,31	1	1	OT služba
74	SUTSIPTK-002	Ključni servis za poslovanje	1,31	1	1	OT služba
75	SUTSIPTK-003	Ključni servis za poslovanje	1,31	1	1	OT služba
76	SUTSIPTK-004	Ključni servis za poslovanje	1,31	1	1	OT služba
77	SUTSIPTK-005	Ključni servis za poslovanje	1,31	1	1	OT služba
78	SUTSIPTK-006	Ključni servis za poslovanje	1,10	0	0	OT služba

79	SUTSIPTK-007	Standardni servis na LAN-u	1,31	1	1	OT služba
80	SUTSIPTK-008	Standardni servis na LAN-u	1,31	1	1	OT služba
81	SUTSIPTK-009	Standardni servis na LAN-u	1,10	0	0	OT služba
82	SUTSIPTK-010	Standardni servis na LAN-u	1,10	0	0	OT služba
83	SUTSIPTK-011	Standardni servis na LAN-u	1,10	0	0	OT služba
PROSJEČNO:			**1,69**	**1,20**	**1,20**	

Stupac „Prosječna vrijednost rizika“ računa se tako da se za svaki pojedini servis uzme vrijednost procijenjenog rizika za svaku na taj servis primjenjivu prijetnju, pa se taj zbroj podijeli s brojem na taj rizik primjenjivih prijetnji. Primjer: servis SISZIOP-001 imao je u ovoj procjeni rizika 82 primjenjive prijetnje (vidljivo samo u bazi podataka procjene rizika), zbroj svih rizika za ostvarenje tih primjenjivih prijetnji bio je 173 (vidljivo samo u bazi podataka procjene rizika), što dijeljenjem daje prosječnu vrijednost rizika od 2,11. Servis je postojao i prije uvođenja sigurnosne inicijative, pa je upisan crnom bojom, dok su novi servisi (ušli u „Katalog servisa“ u razdoblju 2018.-2022.) označeni plavom bojom.

Broj crvenih rizika računa se tako da se izbroje sve na ovaj servis primjenjive prijetnje čiji je procijenjeni rizik 6 ili veći (maksimalno 9). Primjer: servis SISZIOP-001 imao je u ovoj procjeni rizika 82 primjenjive prijetnje s nekom procijenjenom vrijednošću rizika, a za dvije od tih 82 prijetnje rizik se pokazao da je 6 ili veći, pa jednostavnim brojanjem zaključujemo da ovaj servis ima dva „crvena“ rizika.

Broj korektivnih radnji računa se tako da se izbroje sve korektivne radnje otvorene u sklopu ove procjene rizika, a čiji je uzrok sadržan u postojanju „crvenih“ rizika vezanih uz svaki pojedini servis. Primjer: servis SISZIOP-001 imao je u ovoj procjeni rizika dvije primjenjive prijetnje s procijenjenom vrijednošću rizika od 6 ili većom. Provjerom u "Logu korektivnih radnji" možemo ustanoviti da su ti rizici adresirani sa dvije korektivne radnje, što je onda ubačeno u ovu tablicu. Slučajevi kad je za neki servis u tablici indiciran veći broj korektivnih radnji nego „crvenih“ rizika ukazuje na okolnost da su tehnički voditelj i poslovni koordinator promatranog servisa otvorili i dodatne korektivne radnje za neke od procijenjenih „žutih“ rizika. U istom primjeru servisa SISZIOP-001 imamo dva „crvena rizika“ i dvije korektivne radnje, a što znači da za ovaj servis nije niti jedan „žuti“ rizik rezultirao otvaranjem odgovarajuće korektivne radnje.

Iz tablice opet možemo uočiti nove uzorke i izvući sljedeće zaključke:

- svih šest servisa OT mreže iz kategorije ključnih servisa za poslovanje (SUTSIPTK -001 do SUTSIPTK-006) imaju vrlo nizak prosječan rizik od 1,28 (izračun se radi na

način da se za sve servise kategorije ključnih servisa zbroje vrijednosti „Prosječne vrijednosti rizika“ (ukupno 7,65) i podijele s brojem takvih servisa (ima ih 6))

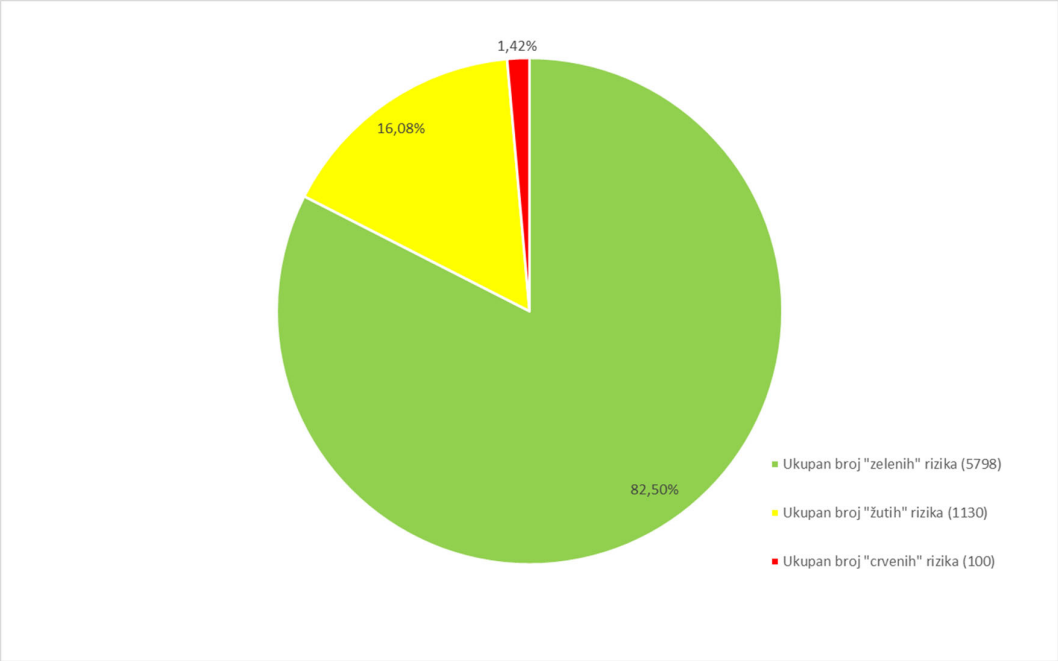
- standardne uredske aplikacije smještene na LAN-u tvrtke („Kategorija servisa“ je „Standardni servis na LAN-u“, vlasnik IT služba i OT služba), rizik se smanjio sa 2,61 prije sigurnosne inicijative na 2,01 (izračun se radi na način da se za sve servise te kategorije zbroje vrijednosti „Prosječne vrijednosti rizika“ (ukupno 84,43) i podijele s brojem takvih servisa (ima ih 42))
- aplikacije ili izmještene u računalni oblak u aranžmanu tvrtke ili izmještene kod vanjskih dobavljača koji ih onda održavaju opet u nekom oblaku imaju vrlo niske razine rizika
- svim dosadašnjim servisima je pao prosječan rizik s 2,22 (tablica 8 – procjena rizika prije sigurnosne inicijative, stupac „Prosječna vrijednost rizika“, gledano u zadnjem redu za sve servise) na 1,69 (tablica 12, stupac „Prosječna vrijednost rizika“, gledano u zadnjem redu za sve servise)
- novi servisi (plava boja) odmah su dobili vrlo niske vrijednosti procijenjenih rizika zbog dijeljene arhitekture mreže i rizika povezanih s korporativnim okruženjem koji su smanjeni u pet godina implementacije sigurnosne inicijative
- servisi se više ne dijele u tri jasne kategorije bazirano na dijeljenim profilima rizika, već je jasno uočljivo u tablici da su svi servisi u vrlo niskim vrijednostima prosječnih rizika po servisu (stupac „Prosječna vrijednost rizika“, teoretske vrijednosti su 1-9).

Generalno se može smatrati da je rizik na promatranoj imovini u vrlo kvalitetno kontroliranom stanju, odnosno da je riječ o stabilnom stanju rizika. Ne postoji niti jedan servis čija bi se situacija s rizicima mogla okarakterizirati kao problematična.

Od ukupno 7028 promatranih rizika gledanih kao kombinacija parova evidencije imovine i prijetnje:

- na 5798 rizika (82,50%) analiza je rezultirala s niskim (prihvatljivim) vrijednostima rizika („zeleni“ rizici),
- na 1130 rizika (16,08%) analiza je rezultirala s graničnim (granično prihvatljivim) vrijednostima rizika („žuti“ rizici),
- na 100 rizika (1,42%) analiza je rezultirala s visokim (neprihvatljivim) vrijednostima rizika („crveni“ rizici),

Kao posljedica 100 „crvenih“ rizika, identificirano je 100 korektivnih radnji koje vlasnici rizika moraju otvoriti u „Logu korektivnih radnji“ ISMS-a tvrtke, uz ogradu da će stvarno otvorenih korektivnih radnji (nezavisnih) biti svakako značajno manje jer će pojedine korektivne radnje istovremeno adresirati više identificiranih „crvenih“ rizika.



Slika 5 - Prikaz procjene rizika obzirom na visinu rizika nakon ZTA

Slika 5 pokazuje grafički prikaz procjene rizika prije uvođenja sigurnosne inicijative, a s promatrano s obzirom na procijenjenu visinu rizika i to kumulativno za sve servise. Dok je u naravi riječ o velikoj tablici s tisućama redova u Microsoft Excelu, ovakav prikaz nam daje mogućnost uočiti razdiobu broja rizika po “bojama”, odnosno koliki su udjeli “crvenih”, “žutih” i “zelenih” rizika u ukupnom broju procijenjenih rizika i usporedbu sa stanjem prije uvođenja sigurnosne inicijative.

5.4 Plan obrade rizika i određivanje protumjera

Plan obrade rizika nakon provedene sigurnosne inicijative je prikazan na sljedećoj tablici 13. Primjer: prve tri nezavisne korektivne radnje (redni brojevi 1-3 u stupcu „R.br.“; ID nezavisne korektivne radnje KR-2022-SISZIOP-033, KR-2022-SISZIOP-035, KR-2022-SISZIOP-039) imaju prosječnu vrijednost rizika 1,76 što je izračunato zbrajanjem prosječne vrijednosti rizika za svaki od 72 servisa IT službe (podaci u stupcu tablice 12, stupac “Prosječna vrijednost rizika”) i dijeljenjem s 72 (broj promatranih servisa).

Tablica 13 – Korektivne radnje nakon sigurnosne inicijative

KOREKTIVNE RADNJE					
R.br.	**Nezavisne korektivne radnje**	**Prosječna vrijednost rizika**	**Broj "crvenih" rizika po servisu**	**Budžet za nezavisnu korektivnu radnju**	**Ukupni budžet za sve nezavisne korektivne radnje**
1	KR-2022-SISZIOP-033	1,76	1,29	€ 12.300,00	€ 156.300,00
2	KR-2022-SISZIOP-035			€ 32.000,00	
3	KR-2022-SISZIOP-039			€ 112.000,00	
4	KR-2022-SUTSIPTK-001	1,23	0,64	€ 21.000,00	€ 103.000,00
5	KR-2022-SUTSIPTK-002			€ 45.000,00	
6	KR-2022-SUTSIPTK-003			€ 1.000,00	
7	KR-2022-SUTSIPTK-004			€ 24.900,00	
8	KR-2022-SUTSIPTK-010			€ 11.100,00	
		1,50	**0,96**	**€ 259.300,00**	**€ 259.300,00**

Također, svi servisi IT službe imaju prosječno 1,29 „crvenih“ rizika po servisu što je izračunato zbrajanjem prosječnog broja „crvenih“ rizika za svaki od 72 servisa IT službe (podaci u stupcu tablice 12, stupac “ Broj crvenih rizika po servisu ”) i dijeljenjem s 72 (broj promatranih servisa). Ovime je potvrđeno da su vlasnici rizika otvorili tri nezavisne korektivne radnje kojima su htjeli adresirati uzroke svih „crvenih“ i dijela „žutih“ rizika za sve servise IT službe (za one „žute“ rizike gdje su otvarane korektivne radnje). Zbrajanjem pojedinačnih budžeta tih pet nezavisnih korektivnih radnji (stupac „Budžet za nezavisnu korektivnu radnju“) dobiva se kumulativni budžet za adresiranje te tri nezavisne korektivne radnje od 156.300,00 € (stupac “Ukupni budžet za sve nezavisne korektivne radnje”).

Uočljivo je da je OT služba i dalje u određenoj prednosti ispred IT službe po zrelosti svojih servisa u sigurnosnom smislu, ali ta prednost više nije značajna jer obje službe drže svoje servise na vrlo stabilnim i niskim vrijednostima rizika. OT služba definira praktično upola manje „crvenih rizika“ po servisu (0,64 OT službe prema 1,29 IT službe, vrijednosti u tablici u stupcu „Broj crvenih rizika po servisu“) i otvara i dalje više nezavisnih korektivnih radnji (OT služba za 11 svojih servisa je definirala 7 „crvenih“ servisa (vidljivo samo u bazi podataka procjene rizika) i 5 nezavisnih korektivnih radnji, dok IT služba za 72 svoja servisa identificira 93 „crvenih“ rizika (vidljivo samo u bazi podataka procjene rizika) i ukupno samo tri nezavisne korektivne radnje. Ovo ukazuje na otklonjene sistemske probleme kod IT servisa i daljnje smanjenje profila rizika za postojeće, ali i sve nove servise. Budžet po korektivnoj radnji i dalje

značajno veći kod IT službe (€ 52.100,00 za IT službu, € 20.600,00 za OT službu. Dramatičan pad procijenjenog troška po korektivnoj radnji obje službe ukazuje da su sistemski problemi uočeni prije pet godina uistinu adresirani implementacijom sigurnosne inicijative i trajno otklonjeni.

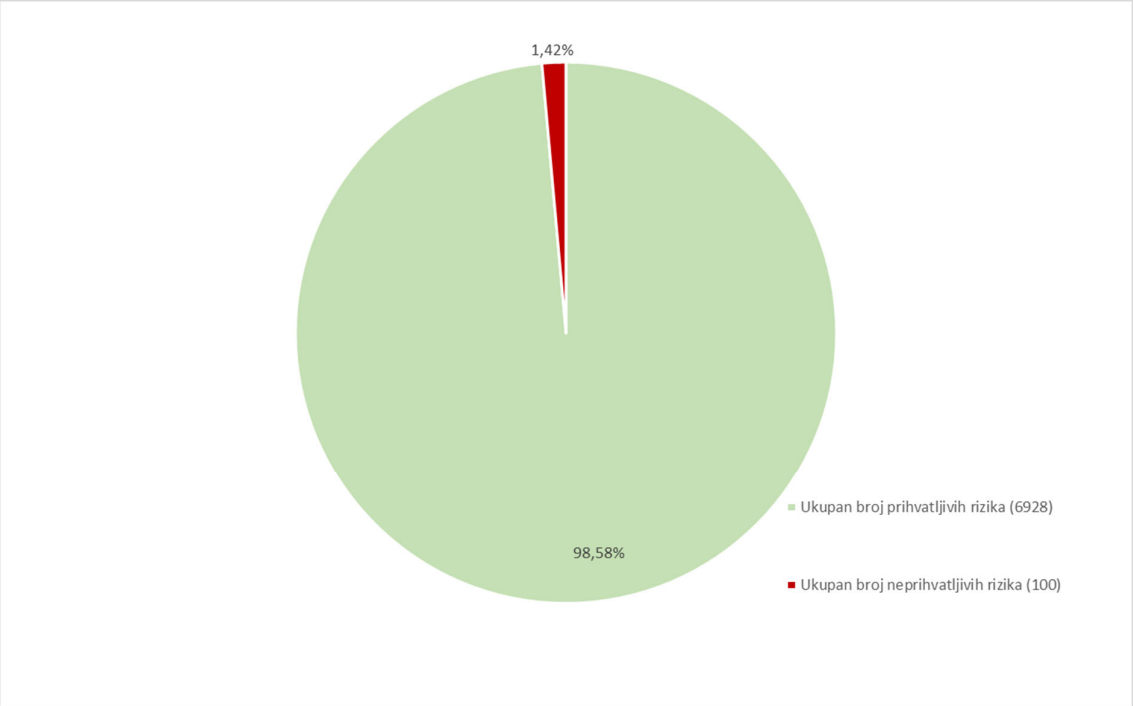
Tablica 13. pokazuje da je ukupan broj nezavisnih korektivnih radnji samo osam, što u praktičnom smislu znači da se s relativno malim brojem relativno jeftinijih zahvata mogu adresirati svi preostali „crveni rizici“ definirani kroz procjenu rizika i za IT službu i za OT službu.

5.5 Popis prihvatljivih rizika

Od ukupno 7028 promatranih rizika gledanih kao kombinacija parova evidencije imovine i prijetnje servisa (vidljivo samo u bazi podataka procjene rizika) i na osnovu kriterija za prihvaćanje rizika, procjena rizika je na 6928 rizika (98,58%) rezultirala s niskim (prihvatljivim) vrijednostima rizika (zelena boja), odnosno srednjim vrijednostima rizika (žuta boja) uz napomenu da ovo uključuje samo one vrijednosti „žutih“ rizika gdje su vlasnici rizika odlučili ne otvarati korektivne radnje. Ovi rizici mogu se smatrati prihvatljivim rizicima.

Preostalih 100 rizika (1,42%) uključuju „crvene“ rizike s visokim (neprihvatljivim) vrijednostima rizika, odnosno rizike sa srednjim vrijednostima rizika (žuta boja) uz napomenu da ovo uključuje samo one vrijednosti „žutih“ rizika gdje su vlasnici rizika odlučili otvarati korektivne radnje.

Preostalih 476 rizika (10,50%) uključuju „crvene“ rizike s visokim (neprihvatljivim) vrijednostima rizika, odnosno rizike sa srednjim vrijednostima rizika (žuta boja) uz napomenu da ovo uključuje samo one vrijednosti „žutih“ rizika gdje su vlasnici rizika odlučili otvarati korektivne radnje. Iz razloga praktičnosti sam popis ovih rizika nije zasebno uključen u ovaj rad, već je ova analiza kumulativno prikazana na slici 6 kao grafički prikaz procjene rizika kumulativno za sve servise poslije uvođenja sigurnosne inicijative, a obzirom na prihvatljivost rizika.



Slika 6 - Prikaz procjene rizika nakon ZTA obzirom na prihvatljivost rizika

5.6 Određivanje preostalog rizika

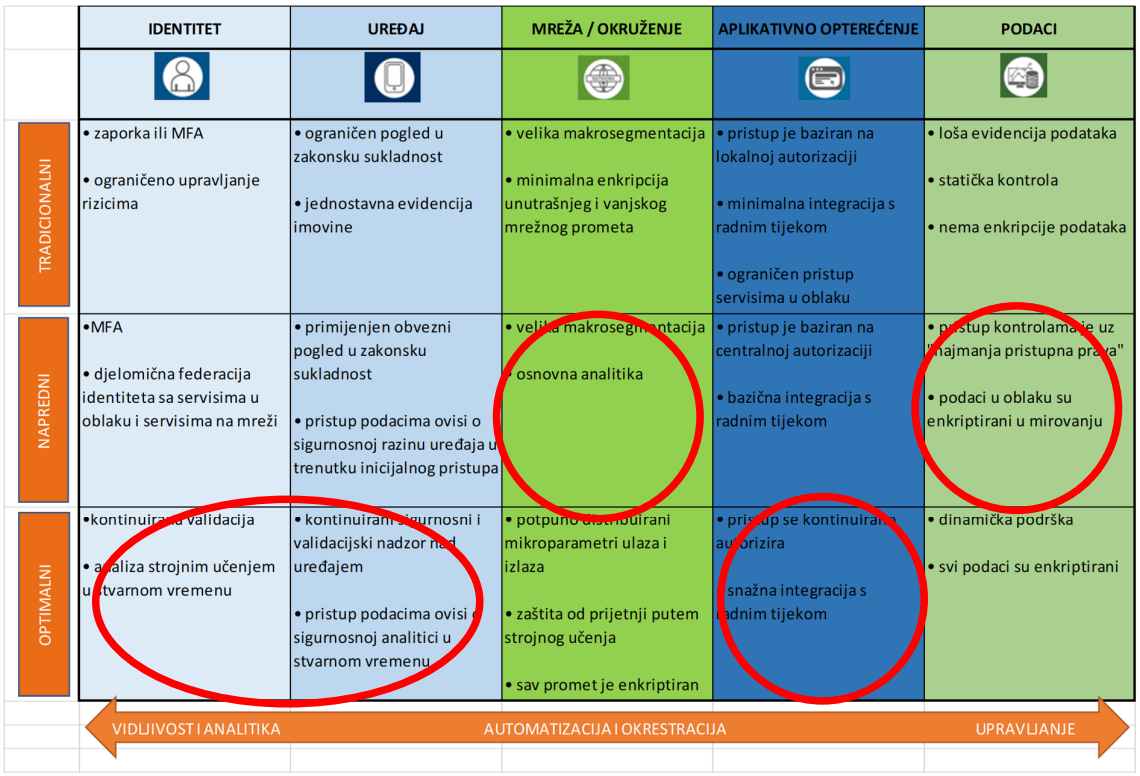
Logika u evaluaciji kriterija je li neki rizik preostali rizik je prikazana u sljedećoj tablici broj 14. Napominjemo da ovdje nije iskazan jedini preostali rizik iz razdoblja prije implementacije sigurnosne inicijative (uzrok planiran za tretiranje kroz korektivnu radnju KR-2018-SUTSIPTK-006 kod OT službe) jer je taj rizik blagovremeno prihvaćen od strane rukovodstva tvrtke odgovarajućom pisanom odlukom. Novog preostalog rizika nema, odnosno sve je „crvene“ rizike moguće tretirati.

Tablica 14 – Preostali rizik nakon sigurnosne inicijative

PREOSTALI RIZIK						
R.br.	**Korektivna radnja**	**Vlasnik korektivne radnje**	**Trošak ostvarenja rizika bitno manji od troška implementacije mjere**	**Moguće kršenje zakona ili regulative**	**Moguće ljudske ozljede ili smrt**	**Preostali rizik**
1	KR-2022-SISZIOP-033	IT služba	NE	NE	NE	**NE**
2	KR-2022-SISZIOP-035	IT služba	NE	NE	NE	**NE**
3	KR-2022-SISZIOP-039	IT služba	NE	NE	NE	**NE**
4	KR-2022-SUTSIPTK-001	OT služba	NE	NE	NE	**NE**

5	KR-2022-SUTSIPTK-002	OT služba	NE	NE	NE	**NE**
6	KR-2022-SUTSIPTK-003	OT služba	NE	NE	NE	**NE**
7	KR-2022-SUTSIPTK-004	OT služba	NE	NE	NE	**NE**
8	KR-2022-SUTSIPTK-010	OT služba	NE	NE	NE	**NE**

5.7 Stupanj zrelosti u CISA ZTMM modelu nakon ZTA



Slika 7 - Stupanj zrelosti u CISA ZTMM modelu nakon ZTA

Slika 7. pokazuje stupanj zrelosti prema ZTMM u 2022. godini. Bez ulaženja u detalje po pojedinim vertikalama modela iz sigurnosnih razloga, možemo konstatirati da je tvrtka nakon uvođenja sigurnosne inicijative u tri područja (zaštita identiteta, uređaja i aplikativnog opterećenja) postigla „optimalnu“ ocjenu zrelosti (najviši stupanj u ovom modelu), dok je u preostala dva područja (zaštita mreže i podataka) postigla „naprednu“ ocjenu zrelosti (srednji stupanj u ovom modelu).

6. EFEKTI PROVEDBE ZTA SIGURNOSNE INICIJATIVE

Prije evaluacije samih metrika procjene rizika potrebno je sagledati promjene u opsegu procjene rizika, odnosno promjenu okoline koju tvrtka štiti od kibernetičkih rizika. Da bismo to učinili definirali smo osam osnovnih brojčanih parametara (tablica 15) koji na objektivan način (pukim brojanjem) opisuju rast opsega procjene rizika. I dalje govorimo o samo jednoj pravnoj osobi koja posluje na 109 fizičkih lokacija. Tu nije bilo promjena u pet godina tijekom sigurnosne inicijative, ali to su ujedno i jedine dvije veličine koje nisu rasle u navedenom razdoblju. Dok za broj poslovnih korisnika možemo reći da je rastao u zanemarivoj mjeri, broj servisa u vlasništvu je rastao za više od 50%, a broj jedinica imovine za 23,53% što je veliko povećanje za kratak period od pet godina. Takvo povećanje opsega rezultiralo je iznimno visokim povećanjem broja evaluiranih rizika za više od 55%. Redovna komunikacija vezano uz redovna održavanja servisa sad se provodi sa 65% više ugovornih partnera, a sve to mora provoditi samo dvanaest informatičkih radnika, jedan manje nego prije početka uvođenja sigurnosne inicijative. Lako je uočiti da je opseg posla značajno narastao, a broj osoblja vlasnika servisa se ne samo nije povećao već se smanjio, stavljajući time velike dodatne odgovornosti na preostale članove IT i OT službi.

Tablica 15 – Usporedba promjene opsega procjene rizika

USPOREDBA PROMJENE OPSEGA PROCJENE RIZIKA				
Rb.	**Metrika**	**PRIJE sigurnosne inicijative**	**POSLIJE sigurnosne inicijative**	**POMAK**
1	Broj pravnih osoba u opsegu	1	1	0.00%
2	Broj fizičkih lokacija	109	109	0.00%
3	Broj poslovnih korisnika	268	273	1.87%
4	Broj servisa u vlasništvu	55	83	50.91%
5	Ukupni broj jedinica imovine u vlasništvu	1496	1848	23.53%
6	Ukupno zaposlenih radnika u IT + OT službama	13	12	-7.69%
7	Ukupno ugovora o tehničkoj podršci u realizaciji	20	33	65.00%
8	Ukupan broj evaluiranih rizika	4534	7028	55.01%

Crvena polja s indiciranim promjenama u odnosu na stanje opsega prije sigurnosne inicijative ukazuju na nepovoljna kretanja parametara opsega (veći opseg je rizičniji) , a narančasta polja

ukazuju na nepromijenjene vrijednosti promatrane metrike. Zelena polja ukazivala bi na poboljšane vrijednosti promatranih parametara opsega, no njih u ovoj tablici nema.

6.1 Uspostava tehničkih kontrola

Sve promjene u sigurnosnom profilu tvrtke između 2018. i 2022. mogu se promatrati kao svjesno inicirane i provedene promjene od strane same tvrtke te kao neplanirane promjene u unutrašnjem i vanjskom kontekstu tvrtke. Sigurnosna inicijativa rezultirala je sa uvođenjem deset novih tehničkih kontrola na mreži tvrtke, koje su ustanovljene kao građevni elementi ZTA mreže u poglavlju 2.4.

Te tehničke kontrole uvedene su kao formalni servisi u „Katalog servisa“ na način da im je je definiran opseg servisa, određen im je vlasnik servisa, imenovani si im tehnički voditelji i poslovni koordinatori, evidentirana im je imovina, stavilo ih se u produkcijski rad, te su se potom nad tim servisima počeli procjenjivati rizici. Od procjene rizika prije sigurnosne inicijative (2018.) i procjene rizika nakon sigurnosne inicijative (2022.), uvođenje tehničkih kontrola kroz sigurnosnu inicijativu predstavlja jedini slučaj u promatranom periodu (2018.-2022.) gdje je tvrtka svjesno išla na podizanje kibernetičke sigurnosti tvrtke. Ostali novoevidentirani servisi u 2022. kojih u 2018. nije bilo u „Katalogu servisa“ odnose se na nove servise u sklopu provedbe digitalne transformacije (10 novih servisa) i zakonskih prilagodbi (8 novih servisa).

6.2 Promjene u ključnim metrikama rizika

Kako to tablica 16. pokazuje, bazična metrika prosječne vrijednosti rizika (redak broj 1) smanjena je provedbom sigurnosne inicijative za 23,81% na 1,688, što je sjajan rezultat za period pet godina, no ta je metrika još bolja i značajnija ako uzmemo u obzir da je tvrtka imala vrlo dobru situaciju s rizicima i prije sigurnosne inicijative (prosječna vrijednosti rizika 2,216, raspon vrijednosti rizika 1-9), pa je ovo smanjenje vrjednije ako se uoči niska baza od koje se krenulo prije pet godina. Maksimalna razlika u prosječnom riziku dva servisa (redak broj 2) jedina je od deset promatranih metrika koja je pogoršala svoju vrijednost nakon provedbe sigurnosne inicijative, no to je bilo i izgledno za očekivati, jer je prilično nevjerojatno očekivati da se baš svi servisi uniformno smanjiti svoj profil rizika.

Tablica 16 – Usporedba promjena u ključnim metrikama rizika

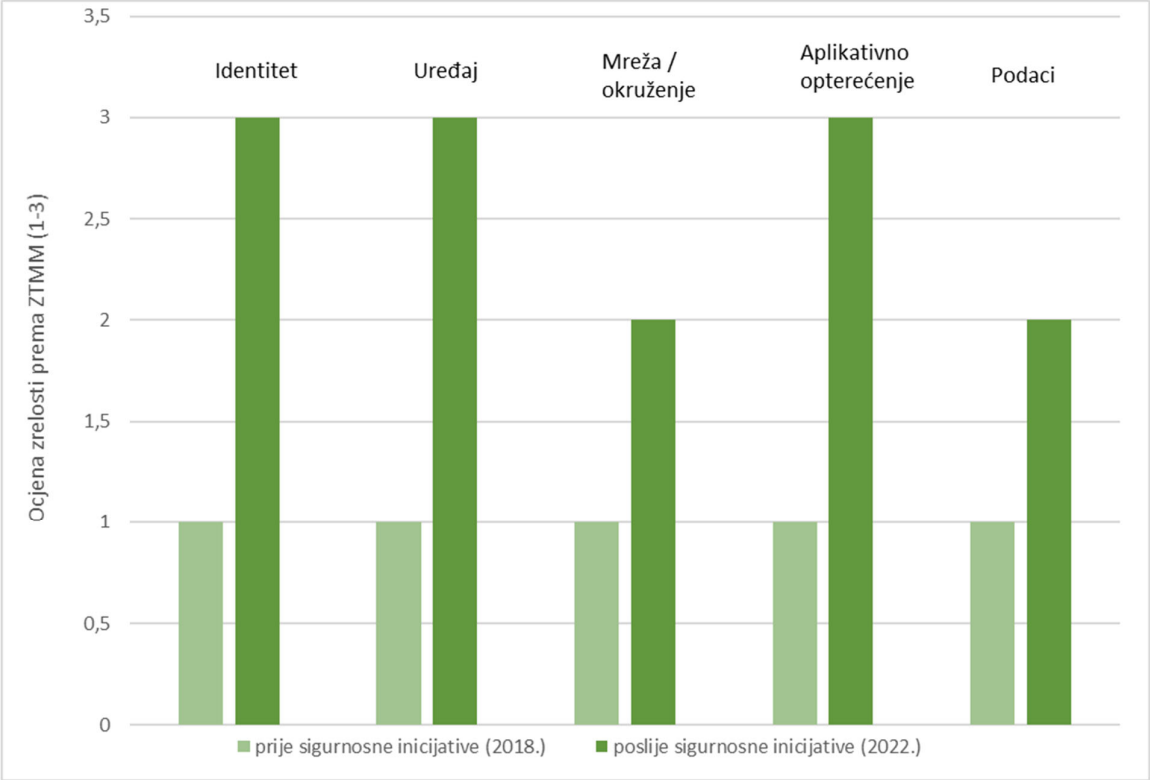
USPOREDBA PROMJENA U KLJUČNIM METRIKAMA				
Rb.	**Metrika**	**PRIJE sigurnosne inicijative**	**POSLIJE sigurnosne inicijative**	**POMAK**
1	Prosječna vrijednost rizika po servisu	2,22	1,69	-23.81%
2	Maksimalna razlika u prosječnom riziku dva servisa	1,23	1,45	17.87%
3	Prosječni broj "crvenih" rizika po servisu	6,09	1,20	-80.22%
4	Prosječni broj "žutih rizika" po servisu	24,56	13,61	-44.57%
5	Udjel "crvenih" rizika u ukupnim rizicima	7,39%	1,42%	-80.74%
6	Udjel "žutih" rizika u ukupnim rizicima	29,80%	16,08%	-46.04%
7	Prosječan broj korektivnih radnji po servisu	8,65	1,20	-86.08%
8	Ukupan broj nezavisnih korektivnih radnji	15	8	-46.67%
9	Prosječna vrijednost nezavisne korektivne radnje	€ 415.973,33	€ 32.412,50	-92.21%
10	Ukupna vrijednost nezavisnih korektivnih radnji	€ 6.239.600,00	€ 259.300,00	-95.84%
11	Broj sigurnosnih tehničkih kontrola	21	31	47.62%

Metrika prosječnog broja „crvenih“ rizika po servisu (redak broj 3) pala je za više od 80%, a metrika prosječnog broja „žutih“ rizika po servisu (redak broj 4) pala je za više od 44% oboje jasni indikatori značajnog prosječnog poboljšanja rizičnosti svih servisa. Slično su se korigirali i udjel „crvenih“ rizika u ukupnom broju servisa (redak broj 5, pad od više od 80%) i udjel „žutih“ servisa u ukupnom broju servisa (redak broj 6, pad od više od 46%). Prosječan broj korektivnih radnji po servisu (redak broj 7) se smanjio više od 86%, a broj preostalih nezavisnih korektivnih radnji (redak broj 8) pao je za više od 46% uz napomenu da je svih 15 originalnih korektivnih radnji iz 2018. u međuvremenu riješeno, te je današnjih osam potpuno novi set korektivnih radnji. Prosječna vrijednost (u eurima) današnje nezavisne korektivne radnje (redak broj 9) umanjena je za više od 92% u odnosu na prije pet godina, a ukupna vrijednost svih nezavisnih korektivnih radnji (redak broj 10, u eurima) je umanjena za više od 95%, sve jasni indikatori tektonske promjene u profilu rizika svih servisa u „Katalogu servisa“. Današnji „crveni“ rizici manji su i jeftiniji za adresirati, manje ih je i rjeđi su među ukupnim rizicima. Crvena polja s indiciranim promjenama u odnosu na stanje metrika prije sigurnosne inicijative ukazuju na nepovoljna kretanja metrika, a zelena polja ukazuju na poboljšane vrijednosti promatrane metrike. Narančasta polja ukazivala bi na nepromijenjene vrijednosti promatrane metrike, ali njih u ovoj tablici nema. Konačno, broj sigurnosnih tehničkih kontrola se povećao za deset u odnosu na 2018. (redak broj 11), a što je izravan rezultat uvođenja sigurnosne inicijative.

Novouvedeni aplikativni servisi ne samo da nisu generirali nove značajnije rizike i konzekventno odgovarajuće korektivne radnje, nego su se svojim profilom rizika uklopili u generalno sniženi profil rizika ostalih servisa zbog dijeljene arhitekture mreže svih LAN-baziranih servisa. Dodatno, sve korektivne radnje poslije uvođenja sigurnosne inicijative odnose se na upravljanje rizicima servisa koji nisu povezana sa sigurnosnom inicijativom, pa budžet procijenjen za osam nezavisnih korektivnih radnji iz 2022. nije relevantan za usporedbu s troškovima ulaganja u ZTA. S obzirom na to da tvrtka nije prethodno koristila niti jednu od fundamentalnih tehnologija koje definiraju ZTA, možemo reći da je praktično sav rizik i IT i OT segmenata mreže bio inherentni rizik nepostojanja ZTA mreže, pri čemu inherentni rizik definiramo kao „prirodna razina rizika svojstvena procesu prije primjene kontrola za sprječavanje i ublažavanje rizika“ [58]. Dok smo ranije konstatirali da se promjene u broju servisa mogu atribuirati paralelnim inicijativama zakonskih i regulatornih usklađivanja, digitalne transformacije i sigurnosne inicijative, razumno je zaključiti da je promjena u profilu rizika praktično u potpunosti uzrokovana sigurnosnom inicijativom i njezinim efektima.

6.3 Promjene u stupnju zrelosti prema CISA ZTMM

Analiza je pokazala da je provedbom sigurnosne inicijative došlo do uspostave više tehničkih kontrola (potpoglavlje 6.2) i potom pozitivnih promjena u različitim metrikama rizika (potpoglavlje 6.3) u tvrtki. Ove promjene dovele su i do značajnog pomaka u stupnju zrelosti prema CISA ZTMM, a koje su vidljive na slici 8. Ako ocjene „tradicionalnog“ stupnja zrelosti vrednujemo sa jednim bodom, „ocjene „naprednog“ stupnja zrelosti vrednujemo s dva boda i „optimalnog“ stupnja zrelosti vrednujemo s tri boda, rezultat ove promjene u zrelosti možemo uočiti u priloženom grafičkom prikazu. Vidljiv je jasan napredak u svih pet kategorija sigurnosti modela.



Slika 8 - Promjena u metrici stupnja zrelosti u modelu CISA ZTMM

Prosječnu ocjenu zrelosti za 2018. godinu (u bodovima) dobit ćemo slijedećem formulom:

POZ2018 = (OZI2018 + OZU2018 + OZMO2018 + OZAO2018 + OZP2018) / 5

gdje su POZ2018 „prosječna ocjena zrelosti ZTA sustava tvrtke u 2018.“, OZI2018 je „prosječna ocjena zrelosti identiteta u 2018.“, OZU2018 je „prosječna ocjena zrelosti uređaja u 2018.“, OZMO2018 je „prosječna ocjena zrelosti mreže/opterećenja u 2018.“, OZAO2018 je „prosječna ocjena zrelosti aplikativnog opterećenja u 2018.“, a OZP2018 je „prosječna ocjena zrelosti podataka u 2018.“. Uvrštavanjem u formulu dobiva se:

POZ2018 = (OZI2018 + OZU2018 + OZMO2018 + OZAO2018 + OZP2018) / 5

POZ2018 = (1 + 1 + 1 + 1 + 1) / 5 = 1.0 bod

Slična formula promijenjena je na situaciju u 2022. godini.

POZ2022 = (OZI2022 + OZU2022 + OZMO2022 + OZAO2022 + OZP2022) / 5

gdje su POZ2022 „prosječna ocjena zrelosti ZTA sustava tvrtke u 2022.“, OZI2022 je „prosječna ocjena zrelosti identiteta u 2022.“, OZU2022 je „prosječna ocjena zrelosti uređaja u 2022.“, OZMO2022 je „prosječna ocjena zrelosti mreže/opterećenja u 2022.“, OZAO2022 je „prosječna ocjena zrelosti aplikativnog opterećenja u 2022.“, a OZP2022 je „prosječna ocjena zrelosti podataka u 2022.“. Uvrštavanjem u formulu dobiva se:

POZ2022 = (OZI2022 + OZU2022 + OZMO2022 + OZAO2022 + OZP2022) / 5

POZ2022 = (3 + 3 + 2 + 3 + 2) / 5 = 13 / 5 = 2,6 bodova

6.4 Druge koristi od uvođenja ZTA

Uz ključne koristi od smanjenja nivoa rizika po svim servisima u tvrtki, provedba sigurnosne inicijative donijela je Energentu d.o.o. i druge koristi. U te koristi svakako ubrajamo jasnu vidljivost mreže i događaja na njoj, te lakše uočavanje pokušaja proboja od strane napadača, te potom reaktivno dizajn mreže zaustavlja propagaciju napadača po resursima mreže i prevenira pokušaj napadača da pokuša preuzeti poslovne podatke s mreže tvrtke i kopirati ih negdje na Internetu [59]. Model ZTA omogućava provedbu digitalne transformacije jer je ZTA u svojoj srži puno lakše implementirati na nove tehnologije za razliku od starog hardvera i naslijeđenih (engl. *legacy*) aplikacija koje jednostavno nemaju sposobnost usklađivanja s osnovnim postulatima ZTA. ZTA također „poboljšava organizacijsku usklađenost smanjenjem nalaza revizije jer od organizacija zahtijevaju postavljanje snažnih mehanizama provjere autentičnosti, autorizacije i šifriranja“ [60]. Ovo se definitivno pokazalo točnim jer tvrtka sad ima logove za sve vrste mrežnih događaja, pogotovo za kontrolu pristupa na ključne mrežne resurse. Iako pojedini autori tvrde da ZTA smanjuje i kapitalnu i operativnu razinu troškova u odnosu na druge modele [59] [60], alternativa tvrtkama nisu samo drugi modeli mrežne sigurnosne arhitekture, nego i nepostojanje modela, a onda je teško govoriti o bilo kakvih uštedama. Te se pokazalo da je slučaj i u Energentu d.o.o. jer je nivo ulaganja tvrtke i u kapitalne investicije i troškove održavanja u IT/OT segmentu porastao otprilike tri puta o odnosu na 2017. godinu, zadnju prije početka uvođenja ZTA.

7. UTROŠENI RESURSI ZA PROVEDBU SIGURNOSNE INICIJATIVE

Ključni utrošeni resursi za provedbu sigurnosne inicijative identificirano su kako slijedi: vrijeme potrebno za provedbu sigurnosne inicijative, financijska sredstva potrebna za nabavu roba i usluga nužnih za uspostavu tehničkih kontrola, radno vrijeme vlastitih zaposlenika utrošeno na provedbu sigurnosne inicijative i politička podrška upravljačke strukture tvrtke.

7.1 Vrijeme

Cjelokupna provedba sigurnosne inicijative sa svim svojim sastavnicama trajala je 60 uzastopnih mjeseci u periodu od siječnja 2018. do prosinca 2022. godine. Cjelokupni program od deset projekata definiran je kroz osamnaest dokumentacija za javno nadmetanje, raspisan i ugovoren, te projektno implementiran unutar predviđenih rokova. Uspoređujući se s drugim sličnim poslovnim subjektima, razumno je zaključiti da je sigurnosna inicijativa provedena vrlo brzo i po planu, bez ijedne odgode, poništenja javnog nadmetanja ili raskida ugovora. I u takvim povoljnim okolnostima tvrtki je trebalo točno pet godina za provedbu programa i stavljanje u produkcijski rad. Program je toliko kvalitetno planiran i pripremljen da niti uzurpacija poslovnih procesa i skretanje fokusa na interventne poslovne potrebe uslijed COVID-19 pandemije i zagrebačka dva zemljotresa nisu poremetila realizaciju programskog plana sigurnosne inicijative.

7.2 Sredstva

Sredstva uložena u sigurnosnu inicijativu i rezervacija sredstava za prvih pet godina ulaska servisa u produkcijski rad mogu se dočarati tek kad se svi izravni troškovi (projektni troškovi i troškovi održavanja) stave u jedinstvenu tablicu broj 17. Iznosi su u potpunosti definirani kao rezultat obrazaca koje su rukovoditelji IT i OT službe popunjavali tijekom strukturiranih intervjua. Prazno polje u tablici troškova indikator je da taj sustav tehnički nema smisla implementirati u sklopu projekta; primjer bi bio EDR u OT okruženju, gdje OT služba ne koristi vlastita Windows računala već isključivo ona pod nadzorom IT službe, pa bi tu bilo nerazborito ići u bilo kakvu implementaciju EDR tehnologije. Treba uzeti u obzir da je samo po jedna osoba popunjavala ove procjene jer je samo jedna osoba (rukovoditelj) u svakoj od službi upućena u raspon i vrstu troškova koji su se akumulirali tijekom promatranih pet godina sigurnosne inicijative, odnosno koji su ugovoreni za potrebe održavanja servisa po ulasku u produkcijski rad. Time su se za potrebe ovog rada prikupili stvarni troškovi iz prve ruke osoba koje su odobravali račune na projektima, ali isto tako treba napomenuti da nema nikakve

kontrole od rukovoditelja dostavljenih iznosa, što znači da su u tim iznosima moguće i određene greške.

Treba uočiti da su projektni, odnosno investicijski troškovi značajno niži od očekivanja ako ta očekivanja definiramo kao zbroj svih budžeta petnaest nezavisnih korektivnih radnji iz 2018. godine (6.239.600,00 €).

Tablica 17 – Pregled projektnih investicija

SIGURNOSNA INICIJATIVA - PREGLED PROJEKTNIH INVESTICIJA				
Rb.	**Projekt**	**Vrijednost projekta - IT okruženje**	**Vrijednost projekta - OT okruženje**	**Ukupna vrijednost investicije**
1	Sustav za upravljanje identitetima	€ 234.500,00	€ 143.200,00	**€ 377.700,00**
2	802.1x	€ 111.000,00	€ 98.000,00	**€ 209.000,00**
3	Vatrozid sljedeće generacije	€ 240.000,00	€ 135.000,00	**€ 375.000,00**
4	Upravljanje privilegiranim pristupom	€ 185.000,00	€ 65.000,00	**€ 250.000,00**
5	UEBA	€ 444.000,00	€ 133.000,00	**€ 577.000,00**
6	Sustav za orkestraciju	€ 112.000,00	-	**€ 112.000,00**
7	EDR	€ 91.000,00	-	**€ 91.000,00**
8	Višefaktorska autentifikacija	€ 79.000,00	€ 103.000,00	**€ 182.000,00**
9	Segmentacija mreže	€ 56.000,00	€ 189.000,00	**€ 245.000,00**
10	Proxy i reverzni *proxy*	€ 145.000,00	€ 133.000,00	**€ 278.000,00**
SVEUKUPNO:		**€ 1.697.500,00**	**€ 999.200,00**	**€ 2.696.700,00**

Razlog leži u stvarnim, odnosno realiziranim cijenama projekata koje su bile bitno niže od procijenjenih budžeta korektivnih radnji, a koje su posljedica od uprave tvrtke korigiranih iznosa odobrenih za pojedine korektivne radnje, te tržišne vrijednosti projekata postignute na javnim nadmetanjima. Potrebno je spomenuti da je za sve implementirane projekte ugovorena tehnologija koja ulazi u top pet najboljih svjetskih proizvođača konkretne vrste rješenja po *Gartner Magic Quadrant* prikazima, pa postoje razlozi za vjerovati da velika razlika između procijenjenih iznosa korektivnih radnji i realiziranih projektnih iznosa nije rezultat degradacije kvalitete, ali je razlika uistinu prevelika da se ne bi posumnjalo u strukturu i dosljednost procesa procjenjivanja korektivnih radnji u tvrtki. Treba uočiti da sustav za orkestraciju i EDR tehnologija nisu implementirani u IT okruženje jer za to na kraju nije bilo niti tehničke potrebe s obzirom na to da je IT služba svojim implementacijama u potpunosti zaštitila i OT servise bez potrebe za dvostrukom implementacijom. Zanimljivo je da su procijenjeni troškovi korektivnih radnji uključivali isključivo troškove projekata, te su projektni budžeti diskutirani

i odobravani u tim gabaritima. Troškovi održavanja IT/OT licenci, te troškovi vlastitih ljudi nisu niti u jednom trenutku bili predmet rasprave, a sljedeće tablice (tablica 18, tablica 19) pokazuju da je uprava tvrtke morala dobiti i te budžete kao ulazne podatke kod odlučivanja o pokretanju pojedinog projekta jer je riječ o zaista značajnim iznosima koji, zbrojeni ovako na jednom mjestu i na strukturirani način, daju sasvim drugu sliku oko stvarnih ulaganja u uvođenje ZTA.

Troškovi održavanja svih deset projekata su u realizaciji, no niti na jednom od sustava nisu još došli blizu kraja petogodišnjeg razdoblja koje je unaprijed odobreno od upravljačkog tijela tvrtke.

Tablica 18 – Troškovi održavanja projekata

SIGURNOSNA INICIJATIVA - TROŠAK ODRŽAVANJA						
IT/OT OPREMA I LICENCE						
Rb.	**Projekt**	**Trošak održavanja 1. godina**	**Trošak održavanja 2. godina**	**Trošak održavanja 3. godina**	**Trošak održavanja 4. godina**	**Trošak održavanja 5. godina**
1	Sustav za upravljanje identitetima	€ 41.547,00	€ 80.755,00	€ 82.370,00	€ 84.017,00	€ 85.697,00
2	802.1x	€ 22.990,00	€ 46.899,00	€ 47.837,00	€ 48.794,00	€ 49.770,00
3	Vatrozid sljedeće generacije	€ 41.250,00	€ 73.750,00	€ 75.225,00	€ 76.730,00	€ 78.265,00
4	Upravljanje privilegiranim pristupom	€ 27.500,00	€ 61.200,00	€ 62.424,00	€ 63.672,00	€ 64.945,00
5	UEBA	€ 63.470,00	€ 146.562,00	€ 149.493,00	€ 152.483,00	€ 155.533,00
6	Sustav za orkestraciju	€ 12.320,00	€ 41.392,00	€ 42.220,00	€ 43.064,00	€ 43.925,00
7	EDR	€ 10.010,00	€ 20.420,00	€ 20.828,00	€ 21.245,00	€ 21.670,00
8	Višefaktorska autentifikacija	€ 20.020,00	€ 29.948,00	€ 30.547,00	€ 31.158,00	€ 31.781,00
9	Segmentacija mreže	€ 26.950,00	€ 54.978,00	€ 56.078,00	€ 57.200,00	€ 58.344,00
10	Proxy i reverzni proxy	€ 30.580,00	€ 99.246,00	€ 101.231,00	€ 103.256,00	€ 105.321,00
	UKUPNO PO GODINAMA:	**€ 296.637,00**	**€ 655.150,00**	**€ 668.253,00**	**€ 681.619,00**	**€ 695.251,00**
	UKUPNO SVIH PET GODINA:	**€ 2.996.910,00**				

Tablica 18. sumira sve troškove održavanja projekata sigurnosne inicijative na period od pet godina.

7.3 Zaposlenici

ZTA se ne može uvesti u neku organizaciju bez sposobnog i motiviranog tehničkog osoblja. Pogotovo u državnom sektoru, a državni sektor predstavlja većinu operatora kritične infrastrukture u Hrvatskoj, nje realno očekivati da će sve, pa niti većina organizacija, imati te

stručne kapacitete. Uz to, tehničko osoblje će samo po sebi trebati proći određenu transformaciju u smislu dodatne edukacije i osvješćivanja o karakteristikama, koristima i načinu korištenja ZTA principa. Ako organizacije uspiju i privući tehnički ekipu za uvođene ZTA, i educirati i osvijestiti radnike, te pokrenuti implementaciju ranijih faza plana za uvođenje ZTA, trenutna situacija na tržištu rada u Hrvatskoj dovela bi sasvim sigurno do povećanog interesa privatnih tvrtki koje imaju ogroman apetit za stručnim osobljem cijelog spektra profila, a pogotovo ako je riječ o vrlo modernom i primjenjivom konceptu za koji bi mnogi gospodarski subjekti u državi mogli biti zainteresirani. Državne organizacije imat će praktično izgubljenu borbu s privatnim sektorom oko kompenzacije svojih tehničkih radnika, a onda posljedično i njihove dugoročne retencije. Gubitkom ključnih radnika ne samo da će se organizacija naći stručno potkapacitirana u ranim fazama puta prema nultom povjerenju, nego će se do tog trenutka izvršene investicije doći u pitanje jer ih neće tko imati dovršiti u projektnom smislu, odnosno u smislu održavanja i budućih nadogradnji. Čak i kvalitetna ekipiranost i motivacija IT radnika nije garancija da će se ići glatko jer je put do ZTA adopcije dug i tehnički zahtjevan, pa je uočeno da dolazi do zamorenosti i projektnim poslom, i stalnim promišljanjem sigurnosti u svakom koraku rada na mreži, kao i stalnim osjećajem da je organizacija pod kontinuiranim kibernetičkim napadom (engl. *firefighting*, gašenje požara) [38]. U paralelnom hodu s projektima sigurnosne inicijative, u Energentu d.o.o. implementirani su servisi nastali kao posljedica tekuće digitalne transformacije, te servisi koji su nastali uslijed zakonskih i regulatornih zahtjeva. Implementacija dvadesetak zahtjevnih projekata u pet godina je ozbiljan plan i za projektno vičnije i kadrovski opremljenije tvrtke od Energenta d.o.o. Uz to, povećanjem opterećenja rada kroz projektne inicijative i dodatna održavanja postojeći su radnici tehničkih službi doživjeli više odlazaka kvalitetnog kadra. Iako su odlazni radnici tipično vrlo brzo zamijenjeni alternativnim radnicima, ukupan broj tehničkih radnika u IT i OT službama se na kraju programa sigurnosne inicijative smanjio, kako nam pokazuje tablica 15. Strukturirani intervjui pokazali su koliko je projektni i kroz održavanje uloženi ljudski faktor investiran u sigurnosnu inicijativu. Koristeći u projektnim pretpostavkama definiranu prosječnu plaću od 18.000 kuna bruto po radniku, te promatrajući trošak na nivou pet godina perioda održavanja po ulasku svih deset projekata u produkciju, ukupan utrošak radnika može se aproksimirati sljedećim tablicama 19 i 20.

Tablica 19 – Sigurnosna inicijativa - trošak radnika na projektima

SIGURNOSNA INICIJATIVA - TROŠAK RADNIKA NA PROJEKTIMA			
Rb.	PROJEKT	PROJEKT	UKUPNI trošak radnika
		Količina vlastitih čovjek-dana - PROJEKT	
1	Sustav za upravljanje identitetima	120,00	€ 13.038,76
2	802.1x	35,00	€ 3.802,97
3	Vatrozid sljedeće generacije	120,00	€ 13.038,76
4	Upravljanje privilegiranim pristupom	160,00	€ 17.385,02
5	UEBA	80,00	€ 8.692,51
6	Sustav za orkestraciju	24,00	€ 2.607,75
7	EDR	22,00	€ 2.390,44
8	Višefaktorska autentifikacija	100,00	€ 10.865,64
9	Segmentacija mreže	43,00	€ 4.672,22
10	Proxy i reverzni proxy	85,00	€ 9.235,79
UKUPNO:		**789,00**	**€ 85.729,86**

Primjer prvog reda tablice 19 navodi da je za projekt „Sustav za upravljanje identitetima“ utrošena vlastita količina čovjek-dana svojih radnika iznosila 120 čovjek-dana. Iznos „Ukupnog troška radnika“ u tablici dobiven je korištenjem slijedeće formule:

UTR = (KVČD/22) x (PMPRkn*TEČAJ)

gdje je UTR „Ukupni trošak radnika“ (u eurima), KVČD je „Količina vlastitih čovjek-dana“ (u čovjek-danima), PMPRkn „prosječna mjesečna plaća radnika (u kunama), u pretpostavkama je navedeno da iznosi 18.000,00 kuna bruto), a TEČAJ je tečaj eura korišten u ovom radu (u kunama, u pretpostavkama je navedeno da 1 € = 7,53 kune). Fiksni broj 22 je broj radnih dana u prosječnom mjesecu (navedeno u pretpostavkama). Uvrštavanjem u formulu dobiva se:

UTR = (120 čovjek-dana / 22 dana) x (18.000 kn / 7,53 kn/€)

UTR = 13.038,76 €

Uz sam tehnički podatak o količini uloženog ljudskog kapitala u sigurnosnu inicijativu, važno je uočiti i opterećenje pod kojim tehnički radnici IT i OT službi rade od kad su implementirani svi individualni projekti i pušteni u produkcijski rad. Prije uvođenja sigurnosne inicijative, tvrtka je brinula o 55 servisa (tablica 8, stupac „ID imovine“ pokazuje sve servise pojedinačno)

korištenjem ukupno trinaest informatičara (tablica 15, metrika „Ukupno zaposlenih radnika u IT + OT službama“, stupac „PRIJE sigurnosne inicijative“). Slijedeća formula nam daje prosječnu opterećenost radnika informatičara:

PORI = BS / BRI

gdje je PORI „prosječno opterećenje radnika informatičara“ (jedinica mjere je broj servisa po radniku informatičaru), BS je „broj servisa“, a BRI je „broj radnika informatičara“.
Uvrštavanjem u formulu dobiva se:

PORI = BS / BRI
PORI = 55 servisa / 13 radnika informatičara
PORI = 4,23 servisa po radniku informatičaru (prije sigurnosne inicijative).

Briga o informatičkom servisu je relativno zahtjevna zadaća ako se briga o servisu provodi savjesno i dosljedno, pa ovaj broj predstavlja nemalo opterećenje za prosječnog informatičara. Nakon provedene sigurnosne inicijative, broj informatičara pao je s trinaest na dvanaest (tablica 15), a broj servisa u „Katalogu servisa“ povećao se s 55 na 83 (tablica 15, metrika „Ukupno zaposlenih radnika u IT + OT službama“, stupac „POSLIJE sigurnosne inicijative“). Homogenom raspodjelom radnog opterećenja gdje „svi rade sve", ako je posao moguće tako organizirati, dobiva se prosječna opterećenost broja servisa po radniku informatičaru korištenjem iste formule:

PORI = BS / BRI
PORI = 83 servisa / 12 radnika informatičara
PORI = 6,92 servisa po radniku informatičaru (poslije sigurnosne inicijative).

Riječ je o dugoročno neodrživom opterećenju informatičara koji rade za državnu tvrtku, a čija posljedica može biti ili značajan pad standarda brige o pojedinom servisu ili daljnji odlasci stručnih ljudi iz tvrtke. U samim financijskim tablicama ova opterećenja se ne vide i ne kvantificiraju kao „koristi“ ili „troškovi“, no ovu nelogičnost tvrtka bi morala otkloniti novim zapošljavanjem stručnjaka u najkraćem roku. Razlog zašto ova prijetnja nije iskazana u novoj analizi rizika leži u činjenici što je ovdje riječ o kadrovskom riziku, a ne ICT operativnim rizicima koje su radnici IT i OT službe naučeni provoditi. Odgovornost za rješavanje ove situacije laži u nadležnim direktorima iznad IT i OT službi i organizacijskoj jedinici za

kadrovska pitanja, te konačno na upravi tvrtke kojoj bi trebalo biti u interesu zaštititi svoje ulaganje u ZTA.

Tablica 20 – Sigurnosna inicijativa - trošak radnika na održavanju

SIGURNOSNA INICIJATIVA - TROŠAK RADNIKA NA ODRŽAVANJU							
Rb.	PROJEKT	ČOVJEK-DANI ZA ODRŽAVANJE					UKUPNI trošak radnika na održavanju
		Godina 1	Godina 2	Godina 3	Godina 4	Godina 5	
1	Sustav za upravljanje identitetima	120,00	54,00	54,00	54,00	54,00	**€ 36.508,51**
2	802,1x	32,00	24,00	24,00	24,00	24,00	**€ 13.908,01**
3	Vatrozid sljedeće generacije	78,00	48,00	48,00	48,00	48,00	**€ 29.337,22**
4	Upravljanje privilegiranim pristupom	105,00	48,00	48,00	48,00	48,00	**€ 32.270,94**
5	UEBA	43,00	36,00	36,00	36,00	36,00	**€ 20.318,74**
6	Sustav za orkestraciju	15,00	12,00	12,00	12,00	12,00	**€ 6.845,35**
7	EDR	28,00	24,00	24,00	24,00	24,00	**€ 13.473,39**
8	Višefaktorska autentifikacija	40,00	36,00	36,00	36,00	36,00	**€ 19.992,77**
9	Segmentacija mreže	54,00	48,00	48,00	48,00	48,00	**€ 26.729,47**
10	Proxy i reverzni proxy	120,00	42,00	42,00	42,00	42,00	**€ 31.293,03**
UKUPNO:		**635,00**	**372,00**	**372,00**	**372,00**	**372,00**	**€ 230.677,46**

Primjer prvog reda tablice 20 navodi da je za projekt „Sustav za upravljanje identitetima“ utrošena vlastita količina čovjek-dana svojih radnika iznosila 120 čovjek-dana za prvu godinu, te po 54 čovjek-dana za svaku od iduće četiri godine produkcijskog rada. Iznos „Ukupnog troška radnika na održavanju“ u tablici dobiven je korištenjem slijedeće formule:

UTRO = (UKVČD/22) x (PMPRkn*TEČAJ)

gdje je UTRO „Ukupni trošak radnika na održavanju“ (u eurima), UKVČO je „Količina vlastitih čovjek-dana na održavanju“ (u čovjek-danima), PMPRkn „prosječna mjesečna plaća radnika (u kunama), u pretpostavkama je navedeno da iznosi 18.000,00 kuna bruto), a TEČAJ je tečaj eura korišten u ovom radu (u kunama, u pretpostavkama je navedeno da 1 € = 7,53 kune). Fiksni broj 22 je broj radnih dana u prosječnom mjesecu (navedeno u pretpostavkama).

Ukupna količina vlastitih čovjek-dana na održavanju dobiva se formulom:

UKVČO = KVČDyr1 + KVČDyr2 + KVČDyr3 + KVČDyr4 + KVČDyr5

UKVČO = (120 + 54 + 54 + 54 + 54) čovjek-dana

UKVČO = 336 čovjek-dana

Korištenjem prethodne formule dobiva se ukupni trošak radnika na održavanju:

UTRO = (UKVČD/22) x (PMPRkn*TEČAJ)

UTRO = (336 čovjek-dana / 22 dana) x (18.000 kn / 7,53 kn/€)

UTRO = 36.508,51 €

7.4 Politička podrška upravljačke strukture tvrtke

Realno je za očekivati da će ovakva promjena u načinu razmišljanja dovesti do povećanih financijskih izdataka, i to i u smislu kapitalnih ulaganja u tehničke kontrole i u smislu redovnih godišnjih troškova održavanja povećane infrastrukture. Ovo povećanje može biti značajno u odnosu na nivoe financijskih izdataka na koje su organizacija navikle u dosadašnjem načinu održavanja sigurnosti svoje mreže. Podrška upravljačke odnosno vlasničke strukture je ovdje presudna jer bez te podrške uvođenje ZTA nema realne šanse za uspjeh [38]. Izvjesno je da je upravljačka garnitura menadžera Energenta d.o.o. dala nedvojbenu i kontinuiranu podršku tehničkim službama u implementaciji sigurnosne inicijative, te da je ta podrška manifestirana i kroz odobrenja potrebnih financijskih sredstava i kroz presudne formalne odluke i presijecanja kojima su „gašeni požari“ izazvani od nedovoljno motiviranih pojedinaca, a koji su požari kroz tako dugi vremenski period implementacije povremeno buktali na pojedinim projektima. Možda ova vrsta ulaganja resursa nije intuitivno odmah evidentna, ali je ona bila značajna, evidentna i presudna u uspjehu implementacije ZTA programa, i to do mjere u kojoj je predstavljala razliku između uspjeha Energenta d.o.o. i drugih državnih i privatnih tvrtki koje ovakvu inicijativu ili nisu bile u stanju pokrenuti ili jednom pokrenute projekte nisu uspjeli dovesti do kraja.

Ova vrsta ulaganja ne može se na smislen način kvalitetno kvantificirati, pa je ne možemo ugraditi u konačni trošak uvođenja ZTA, ali je autor rada smatrao da je ovu komponentnu važno naglasiti.

8. ANALIZA TROŠKOVA I KORISTI

„Kad bi osiguranje podataka tvrtke bilo jednostavno, svaka bi tvrtka imala Zero Trust i ne bismo tako često čuli za povrede podataka“ [61].

8.1 Sumiranje svih troškova

Temeljem svega navedenog u prethodnom poglavlju, sljedeća tablica broj 21. sumira sve kvantificirane troškove sigurnosne inicijative kroz njezino uvođenje i pet godina produkcijskog rada.

Tablica 21 – Ukupni trošak posjedovanja na pet godina – ZTA

SIGURNOSNA INICIJATIVA - UKUPNI TCO				
Rb.	**Projekt**	**Ukupni trošak tehnologije (projekt + 5 godina)**	**Ukupni trošak radnika (projekt + 5 godina)**	**UKUPNI TCO (projekt + 5 godina)**
1	Sustav za upravljanje identitetima	€ 752.086,00	€ 49.547,30	**€ 801.633,30**
2	802.1x	€ 425.290,00	€ 17.710,98	**€ 443.000,98**
3	Vatrozid sljedeće generacije	€ 720.220,00	€ 42.375,98	**€ 762.595,98**
4	Upravljanje privilegiranim pristupom	€ 529.741,00	€ 49.655,96	**€ 579.396,96**
5	UEBA	€1.244.541,00	€ 29.011,25	**€ 1.273.552,25**
6	Sustav za orkestraciju	€ 294.921,00	€ 9.453,10	**€ 304.374,10**
7	EDR	€ 185.173,00	€ 15.863,83	**€ 201.036,83**
8	Višefaktorska autentifikacija	€ 325.454,00	€ 30.858,41	**€ 356.312,41**
9	Segmentacija mreže	€ 498.550,00	€ 31.401,69	**€ 529.951,69**
10	Proxy i reverzni proxy	€ 717.634,00	€ 40.528,82	**€ 758.162,82**
	UKUPNO:	**€ 5.693.610,00**	**€ 316.407,32**	**€ 6.010.017,32**

Nesumnjivo je da je tvrtka izdvojila značajnu količinu sredstava da bi dizajnirala i implementirala koncept moderne mrežne sigurnosti. Iznos od praktično šest milijuna eura za pet godina korištenja ZTA tehnologije predstavlja iznos koji bi bio značajan u bilanci bilo koje organizacije, a pogotovo relativno male državne tvrtke.

Analizom troškova ulaganja i troškova održavanja mogu se uočiti ključni parametri koji su ove iznose gurali prema gore. Broj licenci je uglavnom vezan uz broj radnika (veća tvrtka plaća više), no značajniji je bio inicijalni trošak centralne komponente rješenja, fiksni iznos koji se morao platiti za „prvog“ korisnika svakog pojedinog sustava. U tom smislu, velika tvrtka bi plaćala progresivno manje po svakom novom korisniku, dok bi takvi sustavi bili po radniku

nepodnošljivo skupi za manje tvrtke. Prave koristi ZTA vide se u zaštitama i redukcijom rizika u područjima udaljenog pristupa i sigurnosti trećih strana, dakle u situacijama gdje je veliki broj internih i eksternih udaljenijih korisnika. Tvrtke sa samo par lokacija ili koje takve situacije imaju samo sporadično, odnosno u zanemarivom broju slučajeva neće imati motivacija uvoditi ZTA, ali kod Energenta d.o.o ovo je svakodnevna rutina, pa je ovo također dobro pogođena korist provedene inicijative. Bitno je uočiti da je prilagodljivi dizajn ZTA mreže pogodan za rapidna uvođenja novih servisa dok god se ti servisi uvode koristeći sve sigurnosne postulate sigurne mreže. Tvrtke koje idu u naglu digitalizaciju ili provode određene zakonske ili regulatorne modifikacije poslovnih procesa uvidjet će prednosti ZTA dizajna za daljnje širenje mreže. U ovom slučaju, digitalizacija je krenula paralelno sa sigurnosnom inicijativom, pa mreža nije bila spremna prihvatiti nove servise, ali je tvrtka od prvog dana prihvatila i propisala sigurnosna načela koja su vrijedila za sve ostale servise koji su uvedeni u promatranih pet projektnih godina. Tvrtka je dobila i jednu negativnu pojavu kao rezultat provedbe sigurnosne inicijative u vidu jasnog preopterećenja svojih informatičkih radnika. Ova situacija je nešto što bi tvrtka trebala što prije adresirati kako ne bi kompromitirala svoje ulaganje u ZTA i dovela u pitanje koristi koje je njome dobila.

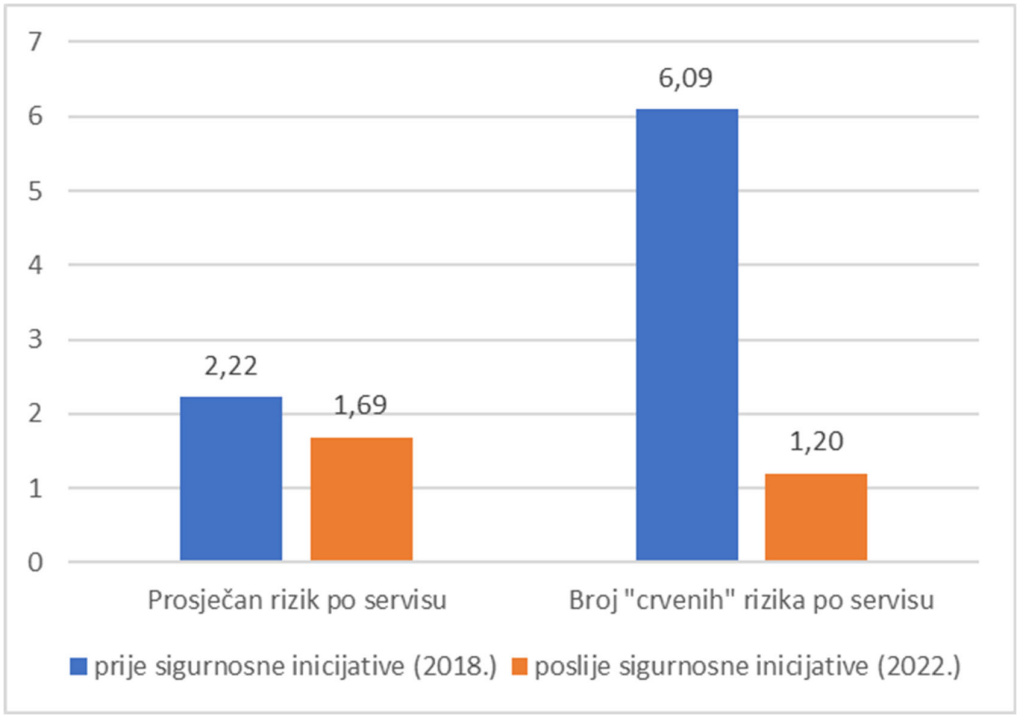
8.2 Sumiranje svih koristi

Koristeći podatke iz tablica i slika u prethodnim poglavljima (tablica 16, slika 8) prikazan je tablični pregled nekoliko ključnih pokazatelja koristi od uvođenja sigurnosne inicijative za Energent d.o.o.. Svih pet parametara prikazano je i grafički, gdje se lako uočavaju pozitivni pomaci za tvrtku.

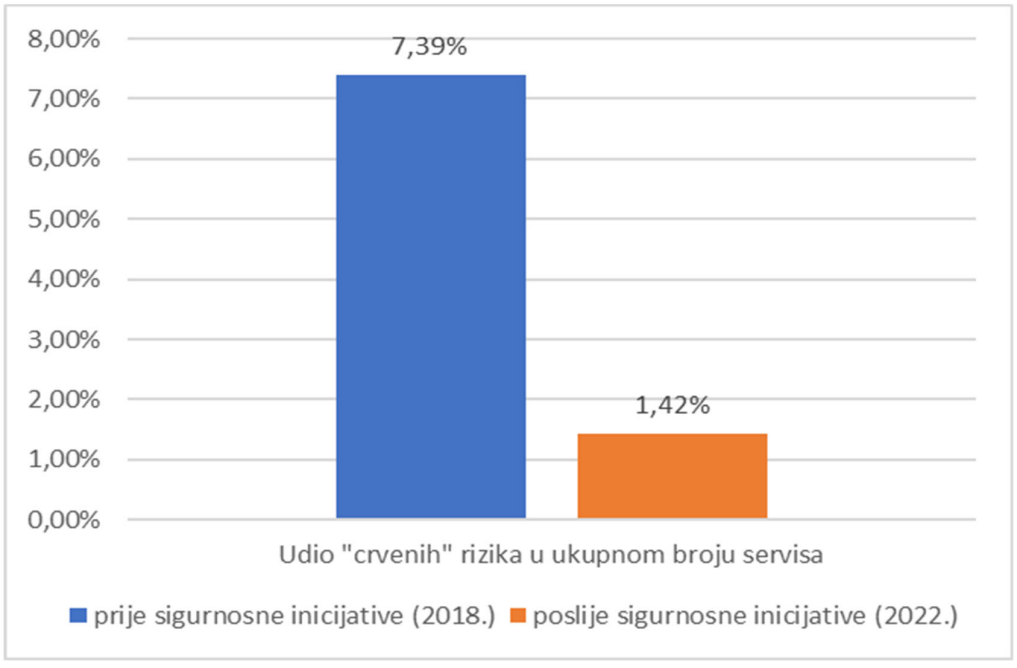
Tablica 22 – Pregled ključnih pet metrika koristi

Rb.	Ključni parametar	prije sigurnosne inicijative (2018.)	poslije sigurnosne inicijative (2022.)
1	Prosječan rizik po servisu	2,22	1,69
2	Broj "crvenih" rizika po servisu	6,09	1,20
3	Udio "crvenih" rizika u ukupnom broju rizika	7,39%	1,42%
4	Prosječna ocjena zrelosti (POZ)	1,0	2,6
5	Broj sigurnosnih tehničkih kontrola	21	31

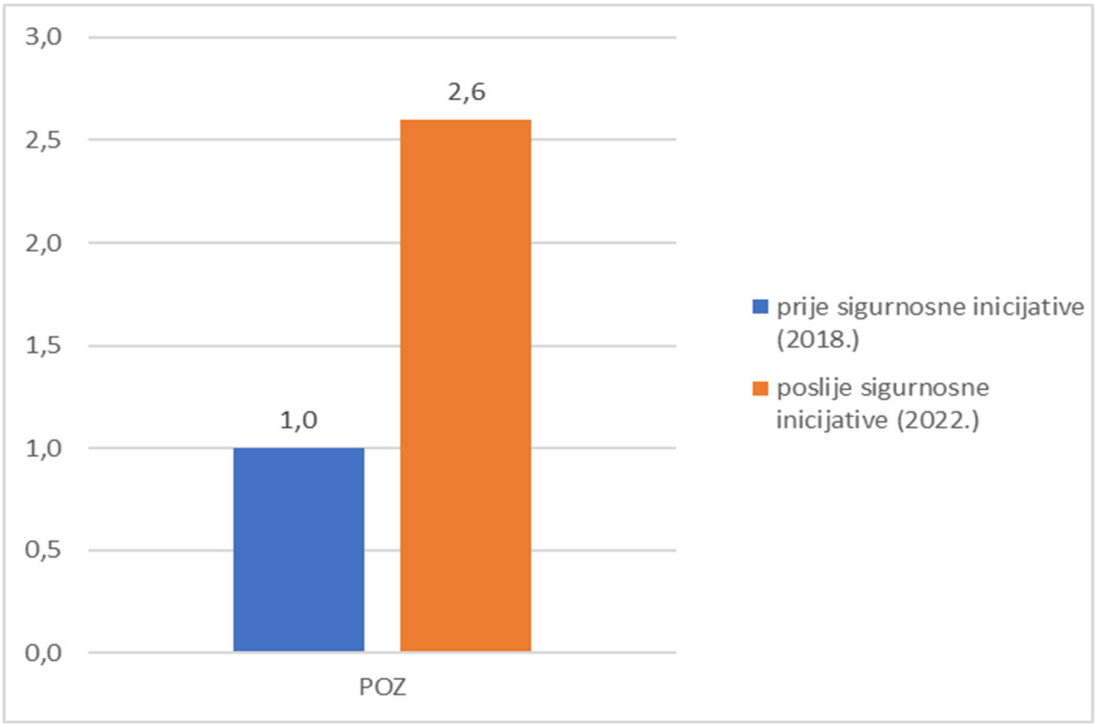
Pet ključnih parametara koristi su „prosječan rizik po servisu“, „broj 'crvenih' rizika po servisu“, „Udio 'crvenih' rizika u ukupnom broju rizika“, „prosječna ocjena zrelosti“ (prema ZTMM), te „broj sigurnosnih tehničkih kontrola“.



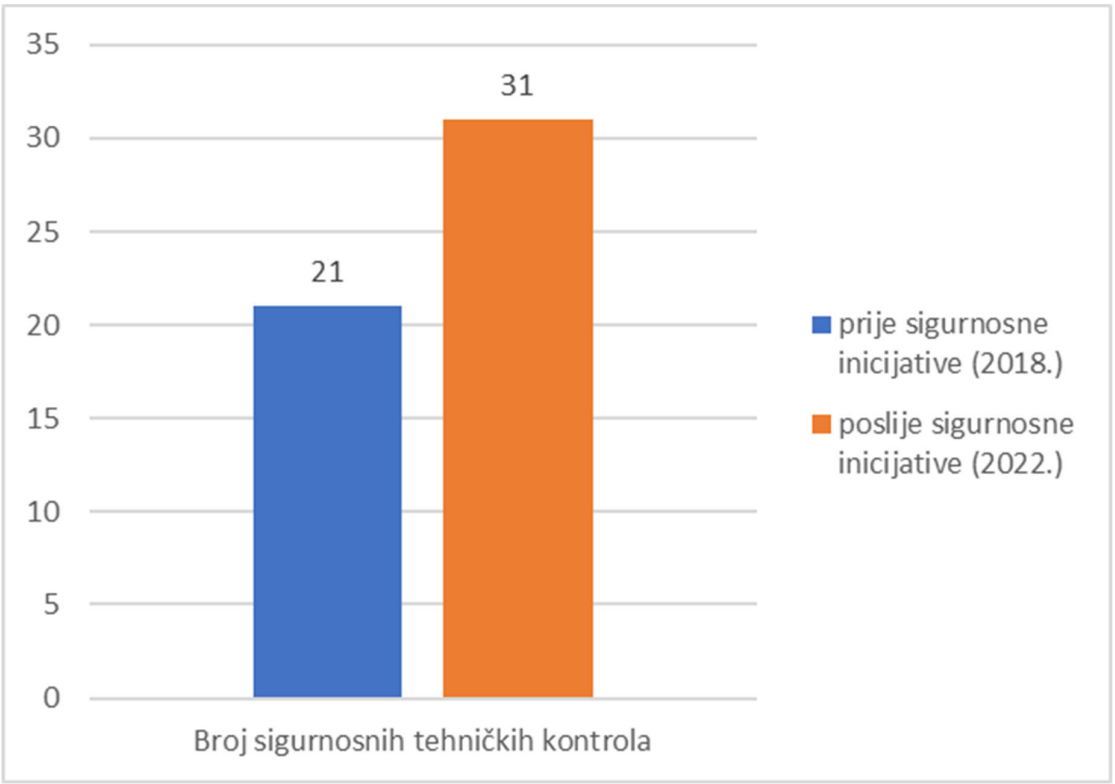
Slika 9 - Pomaci u metrici rizika



Slika 10 - Pomaci u metrici udjela "crvenih" rizika u ukupnom broju rizika



Slika 11 - Pomaci u metrici prosječne ocjene zrelosti



Slika 12 - Pomaci u metrici broja tehničkih kontrola

Ključno je pitanje: da li je šest milijuna eura i pet godina fokusa i truda opravdana cijena za ovaj pomak u profilu rizika tvrtke? Odgovor ovisi o tome kome postavljamo to pitanje.

8.3 Opravdanost ulaganja iz perspektive IT i OT službe

Ljudi koji svakodnevno rade s implementiranim tehničkim kontrolama i koji operativno odgovorni za zaštitu mreže tvrtke svakako imaju bojne koristi od implementirane inicijative, od automatizacije i orkestracije pojedinih procesa, do neusporedivo jače kontrole i vidljivosti nad događajima na mreži. Obzirom da oni ne troše vlastiti novac, njima je sigurnosna inicijativa donijela puno koristi. S druge strane, ocjena o isplativosti je ovdje neodređena jer je deset dodatnih tehničkih kontrola, uz druge servise koji su se pojavili u promatranih pet godina, donijela veliku dodatnu količinu posla koju mora iznijeti čak manji broj radnika nego prije uvođenja sigurnosne inicijative. Isplativost sigurnosne inicijative nije utvrđena na ovom nivou dionika.

Ova ocjena rezultat je razgovora vođenih s radnicima IT i OT službe u prosincu 2022.

8.4 Opravdanost ulaganja iz perspektive uprave tvrtke

Upravljačka struktura tvrtke nema nikakvih premišljanja oko opravdanosti provedbe sigurnosne inicijative prihvaćajući iznos uloženih sredstava kao fer i tržišnu cijenu za očekivane i dobivene koristi. Nema sumnje da je prije pet godina tvrtka vrlo ozbiljno shvatila svoje pravne obveze, te da ulaganje u iznosu ovog reda veličine nije pokrenuto i realizirano kao nešto što će biti komercijalno „isplativo“ ili ne, već kao nešto što jednostavno treba uvesti, i to u procesnom smislu beskompromisno koristeći najbolje tehnologije koje se na tržištu nude. No tvrtka je na početku priče intuitivno ispravno procijenila da će ovako definirana mreža omogućiti ne samo čvrstu platformu za daljnji razvoj svoje mreže i implementaciju novih servisa, dovršetak digitalne transformacije i usklađivanja sa nadolazećim EU direktivama, već toj istoj tvrtki će omogućiti miran san u odnosu na kibernetičke kriminalce na Internetu. Možda taj san nikad više neće biti onako miran kako je to bio slučaj prije deset ili petnaest godina, ali uprava je od svih varijanti „mirnog sna“ sebi omogućila onu najbolju koju novac može kupiti. U tom smislu, ulaganje se u svakom slučaju isplatilo.

Ova ocjena rezultat je razgovora vođenih s članovima uprave tvrtke službe u prosincu 2022.

8.5 Opravdanost ulaganja iz perspektive vlasnika tvrtke

Iz perspektive vlasnika, Republika Hrvatska je relativno brzo dobila čistu situaciju s jednim od ključnih subjekata na energetskoj mapi države, a za novac koji ne predstavlja nikakvu razliku u okviru iznosa s kojima redovno barataju državne financije. Postignuti su rješavanje rizika u smislu ključnih kibernetičkih rizika, dobivena je sigurna platforma za daljnji razvoj i širenje i riješeno je pitanje zakonske usklađenosti kibernetičke sigurnosti prema EU. Isplativost sigurnosne inicijative je za ovog dionika neupitna.

Ova ocjena rezultat je razgovora vođenih s predsjednikom nadzornog odbora tvrtke u prosincu 2022.

9. ZAKLJUČAK

Promjena u načinu na koji radimo i otkuda radimo do kraja je ogolila zastarjeli način razmišljanja o kibernetičkog sigurnosti i dovela u pitanje pojam „sigurne mreže“. Moderna poslovna mreža traži promjenu paradigme što sigurnost uopće jest i kako je postižemo. Jedna od opcija je mreža nultog povjerenja kroz sedam osnovnih principa kako ih je definirao američki NIST Institut, a koji predstavljaju odličnu teoretsku podlogu za razumijevanje i implementaciju koncepta nultog povjerenja u Sjedinjenim Državama i Europskoj Uniji, pogotovo u svjetlu zakonskih inicijativa koje su tamošnje vlade donijele u svrhu podizanja otpornosti tamošnje nacionalne i kritične infrastrukture. U takvoj mreži svaki zahtjev mora biti dinamički potvrđen preko svih dostupnih saznanja o korisniku, uređaju, traženom resursu i svih ostalih okolišnih podataka i povijesno praćenih obrazaca ponašanja u toj mreži, a svaka točka na mreži je sigurnosni resurs nad kojim se provodi kontinuirana analiza rizika i svaka odluka o promjeni bilo čega na mreži je rezultat takve analize. Uvođenje ovog koncepta traži strateško planiranje, promjenu organizacijskog i kulturnog koncepta, povećava opterećenje na tehničko osoblje i zahtijeva ulaganja bitno veća od onih na koje su organizacije navikle.

Energent d.o.o je se odlučio za hitno pokretanje ZTA sigurnosne inicijative kao reakciju na svoju situaciju iz 2017. godine gdje je nedostatak bilo kakve sigurnosne arhitekture mreže dovela do serije incidenata koji su pokazali da se radi pogrešno i da je situacija svaki dan lošija nego prethodni. Iako je sigurnosna inicijativa pokrenuta bez prave analize isplativosti, ovaj rad pokazuje da je četverogodišnji programski iskorak, proveden pod okolnostima intenzivnog rada na paralelnim projektima i u okruženju zagrebačkih zemljotresa i COVID-19 pandemije, rezultirao rješavanjem svih identificiranih ranjivosti, izvanrednim poboljšanjem profila rizika tvrtke i uspostavom jasnog razvojnog okvira i sigurnosnih postulata za daljnji ubrzani razvoj svoje IT i OT mreže. Ono što je ostalo upitno je količina resursa koju je tvrtka odvojila za realizaciju sigurnosne inicijative, te osigurala za održavanje ZTA infrastrukture tijekom prvih pet godina rada pojedinih projekata. Ovo financijsko ulaganje je praćeno količinom utrošenih radnih dana vlastitih radnika usporedivom s radno intenzivnim infrastrukturnim građevinskim projektima kopanja u planinama i polaganja visokotlačnih plinskih cijevi. Ključni faktor u odlučivanju da li je ulaganje na neki način isplativo moglo se naslutiti u odmah u početku iskazanoj snažnoj političkoj volji uprave tvrtke da pokrene ovako financijski opterećujuću, radno intenzivnu i tehnički zahtjevnu inicijativu, a to je jasno iskazana volja da se zakonska obveza kibernetičke zaštite kritične nacionalne infrastrukture ispuni ne samo beskompromisno

u kvalitativnom pogledu, nego da ulaganje postavi temelje za budućnost kibernetičke sigurnosti mreže tvrtke i riješi razvojne nedoumice u kojima se tvrtka često gubila prije pet godina. U tom smislu, tvrtka je za svoj novac dobila sve što je očekivala, ali treba istaknuti da je faktor političke volje za uvođenje ZTA svakako u prvom redu rezultat višegodišnjeg lutanja u tehničkom smislu i iskrene želje za postizanjem zakonskog usklađenja, a puno manje rezultat neke financijske „isplativosti“ sigurnosne inicijative. Bez tog „nekomercijalnog“ motiva, upitno je koji bi faktori mogli motivirati neku drugu tvrtku na uvođenje ZTA od navedenim financijskim uvjetima. Analizirajući ključne parametre koji su doveli do realiziranog budžeta, realno je da bi se na uvođenje ZTA prije odlučila tvrtka s više radnika, više zemljopisno disperziranih lokacija, jakom kulturom rada od kuće i prisutnošću radnika ugovornih partnera na mreži tvrtke, te tvrtka koja pred sobom ima poslovnu potrebu snažnog širenja svoje mreže i rapidnim uvođenjem novih servisa, poglavito kao posljedicu provedbe digitalne transformacije. Dodatno, ZTA bi mogla biti odličan izbor za tvrtku kojoj je sigurna i fleksibilna mreža izvor prihoda, npr. telekom tvrtki.

Isplativost cijele ove sigurnosne inicijative teško je dokaziva klasičnim „novac za korist“ načinom usporedbe jer sigurnost kao takva teško može imati cijenu, pa odgovor na ovo pitanje ovisi o tome kojem dioniku se postavlja ovo pitanje. Upravi i vlasniku tvrtke isplativost je neupitna jer je sigurnosna inicijativa riješila osnovni problem iz perspektive tih dionika (zakonska usklađenost kibernetičke sigurnosti prema EU pravilima), dok su na operativnom nivou stvari ipak neizvjesnije jer informatičari IT i OT službe podnose puno veće radno opterećenje nego ranije, no ovo je nešto što se na nivou uprave tvrtke može relativno jednostavno riješiti dodatnim zapošljavanjem.

10. POPIS LITERATURE

[1] Wikipedia, »Ransomware,« Wikipedia, 21 prosinac 2022. [Mrežno]. Available: https://en.wikipedia.org/wiki/Ransomware. [Pokušaj pristupa 21 prosinac 2022].

[2] Check Point, »"How the Evolution of Ransomware Has Changed the Threat Landscape",« svibnja 2022. [Mrežno]. Available: https://blog.checkpoint.com/2022/05/11/how-the-evolution-of-ransomware-changed-the-threat-landscape/. [Pokušaj pristupa 3. listopada 2022.].

[3] M. Miliard, »"Hospital Ransomware Attack Leads To Fatality After Causing Delay In Care",« rujna 2020.. [Mrežno]. Available: https://www.healthcareitnews.com/news/hospital-ransomware-attack-leads-fatality-after-causing-delay-care. [Pokušaj pristupa 18. listopada 2022].

[4] J. A. Lewis, »"Cyber War and Ukraine",« lipnja 2022. [Mrežno]. Available: https://www.csis.org/analysis/cyber-war-and-ukraine. [Pokušaj pristupa 2. studenog 2022.].

[5] S. Rose et al, »"Zero Trust Architecture",« 2020.. [Mrežno]. Available: https://doi.org/10.6028/NIST.SP.800-207. [Pokušaj pristupa 4. studenog 2022.].

[6] HNB, »Glavni makroekonomski indikatori,« HNB, 30. prosinca 2022.. [Mrežno]. Available: https://www.hnb.hr/statistika/glavni-makroekonomski-indikatori. [Pokušaj pristupa 6. siječnja 2023.].

[7] Lider/HINA, »Inflacija dosegnula najvišu razinu do kada DZS vodi podatke,« Lidermedia, 16. prosinca 2022.. [Mrežno]. Available: https://lidermedia.hr/biznis-i-politika/inflacija-dosegnula-najvisu-razinu-do-kada-dzs-vodi-podatke-147383. [Pokušaj pristupa 6. siječnja 2023.].

[8] Ministarstvo financija, »"Smjernice za upravljanje rizicima u poslovanju institucija javnog sektora",« svibnja 2017.. [Mrežno]. Available: https://mfin.gov.hr/UserDocsImages//dokumenti/sredisnja-harmonizacija/fin-

upravljanje-kontrole/upravljanje-rizicima//Smjernice%20za%20upravljanje%20rizicima%20u%20poslovanju%20institucija%20javnog%20sektora.pdf. [Pokušaj pristupa 23. svibnja 2022.].

[9] BSI Group, »BS 7799-3:2017 Information security management systems - Guidelines for information security risk management,« BSI Group, 31. listopada 2017.. [Mrežno]. Available: https://knowledge.bsigroup.com/products/information-security-management-systems-guidelines-for-information-security-risk-management-1/standard. [Pokušaj pristupa 9. siječnja 2023.].

[10] NIST, »SP 800-30 Rev. 1 Guide for Conducting Risk Assessments,« NIST, rujna 2012.. [Mrežno]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. [Pokušaj pristupa 9. siječnja 2023.].

[11] Zavod za sigurnost informacijskih sustava, »"Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama ZKS-a i provođenje ocjene sukladnosti",« 2019.. [Mrežno]. Available: https://www.zsis.hr/UserDocsImages/Okvir_dobrih_praksi-v1.pdf. [Pokušaj pristupa 13. lipnja 2022.].

[12] Vlada Republike Hrvatske, »"Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga",« srpnja 2018.. [Mrežno]. Available: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html. [Pokušaj pristupa 23. srpnja 2022.].

[13] Deloitte, »Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga,« [Mrežno]. Available: https://www2.deloitte.com/hr/hr/pages/audit/articles/kiberneticka-sigurnost.html. [Pokušaj pristupa 12. siječnja 2023.].

[14] K. Yasar, »Information Security Management System (ISMS),« TechTarget, [Mrežno]. Available:

https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS. [Pokušaj pristupa 6. siječnja 2023.].

[15] European Comission, »"Prijedlog direktive Europskog Parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148",« 16. prosinca 2020.. [Mrežno]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0023.02/DOC_1&format=PDF. [Pokušaj pristupa 21. studenog 2022.].

[16] M. Berman, »Risk Assessments 101: The Role of Probability & Impact in Measuring Risk,« N Contracts, 20. kolovoza 2018.. [Mrežno]. Available: https://www.ncontracts.com/nsight-blog/risk-assessments-101-the-role-of-probability-impact-in-measuring-risk. [Pokušaj pristupa 4. siječnja 2023.].

[17] B. Cole, »Risk assessment,« TechTarget, [Mrežno]. Available: https://www.techtarget.com/searchsecurity/definition/risk-assessment. [Pokušaj pristupa 4. siječnja 2023.].

[18] NIST, »Computer Security Resurce Center,« NIST, [Mrežno]. Available: https://csrc.nist.gov/. [Pokušaj pristupa 4. siječnja 2023.].

[19] U. P. Jonathan Copley, »Assessing and Managing IT Operational and Service Delivery Risk,« ISACA, 1. rujna 2014.. [Mrežno]. Available: https://www.isaca.org/resources/isaca-journal/past-issues/2014/assessing-and-managing-it-operational-and-service-delivery-risk#:~:text=IT%20operations%20and%20service%20delivery%20risk%20is%20the%20risk%20associated,disaster%20recovery%20(DR)%20provisions. [Pokušaj pristupa 4. siječnja 2023.].

[20] ManageEngine, »An extensive guide to building an IT service catalog,« Zoho Corp., 2023. [Mrežno]. Available: https://www.manageengine.com/products/service-desk/itil/what-is-service-catalog.html#what-is-service-catalog. [Pokušaj pristupa 4. siječnja 2023.].

[21] P. A. Networks, »What is IT Asset Inventory?,« Palo Alto Networks, [Mrežno]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-it-asset-inventory. [Pokušaj pristupa 6. siječnja 2023.].

[22] Stanford University, »Office of the Chief Risk Officer,« Stanford University, 2023.. [Mrežno]. Available: https://ocro.stanford.edu/erm/key-definitions/definition-risk-owner#:~:text=Risk%20Owner%3A%20The%20individual%20who,his%2Fher%20risk%20management%20efforts.. [Pokušaj pristupa 9. siječnja 2023.].

[23] M. K. Pratt, »Risk Profile,« TechTarget, [Mrežno]. Available: https://www.techtarget.com/searchsecurity/definition/risk-profile. [Pokušaj pristupa 6. siječnja 2023.].

[24] Lucidchart, »What are your ERD needs?,« Lucidchart, [Mrežno]. Available: https://www.lucidchart.com/pages/er-diagrams. [Pokušaj pristupa 12. siječnja 2023.].

[25] J. Rabelo, »Primary Key,« Techopedia, 14. kolovoza 2020.. [Mrežno]. Available: https://www.techopedia.com/definition/5547/primary-key. [Pokušaj pristupa 12. siječnja 2023.].

[26] Wikipedia, »Cost-benefit analysis,« Wikipedia, 23. studeni 2022.. [Mrežno]. Available: https://en.wikipedia.org/wiki/Cost%E2%80%93benefit_analysis. [Pokušaj pristupa 4. siječnja 2023.].

[27] Wikipedia, »Corrective and preventive action,« Wikipedia, 7. kolovoza 2022.. [Mrežno]. Available: https://en.wikipedia.org/w/index.php?title=Corrective_and_preventive_action&action=history. [Pokušaj pristupa 4. siječnja 2023.].

[28] T. Asana, »What is technical debt? How to pay it off (with examples),« Asana, 10. srpnja 2022.. [Mrežno]. Available: https://asana.com/resources/technical-debt. [Pokušaj pristupa 4. siječnja 2023,].

[29] »Upravljanje sigurnosnim rizicima - materijalna i nematerijalna imovina, prijetnje sigurnosti i ranjivost, klasifikacija informacija,« Fakultet

elektrotehnike i računarstva, Sveučilište u Zagrebu, [Mrežno]. Available: https://www.fer.unizg.hr/predmet/usr/materijali#%23!p_rep_111973!_-154553. [Pokušaj pristupa 4. siječnja 2023.].

[30] Hrvatski sabor, »"Zakon o provedbi Opće uredbe o zaštiti podataka",« svibnja 2018.. [Mrežno]. Available: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html. [Pokušaj pristupa 09. studenog 2022.].

[31] G. Antolović, »Alati za konceptualno modeliranje podataka,« 2016.. [Mrežno]. Available: https://repozitorij.unipu.hr/islandora/object/unipu%3A580/datastream/PDF/view. [Pokušaj pristupa 11. siječnja 2023.].

[32] T. Roosevelt, »"Goodreads - Theodore Roosevelt Quotes",« 2022.. [Mrežno]. Available: https://www.goodreads.com/quotes/312751-nothing-in-the-world-is-worth-having-or-worth-doing. [Pokušaj pristupa 22. studenog 2022.].

[33] J. Garbis i J. Chapman, Zero Trust Security – An Enterprise Guide, New York: Apress media, 2021..

[34] J. Kindervag, »"No More Chewy Centers: Introducing the Zero Trust Model of Information Security",« rujna 2010.. [Mrežno]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf. [Pokušaj pristupa 20. studenog 2022.].

[35] S. Gittlen i L. Fitzgibbons, »"What is Zero Trust? Ultimate Guide to the Network Security Model",« 2021.. [Mrežno]. Available: https://media.techtarget.com/digitalguide/images/Misc/EA-Marketing/Eguides/What_is_Zero_Trust_Ultimate_Guide_to_the_Network_Security_Model.pdf. [Pokušaj pristupa 12. studenog 2022.].

[36] Cloud Security Alliance, »"Toward a Zero Trust Architecture",« 2021.. [Mrežno]. Available: https://cloudsecurityalliance.org/research/artifacts/. [Pokušaj pristupa 21. listopada 2022.].

[37] C. von Clausewitz, "On War", London: OUP Oxford, 2008..

[38] National Security Agency, »"Embracing a Zero Trust Security Model",« 2021.. [Mrežno]. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF. [Pokušaj pristupa 7. studenog 2022.].

[39] Backblaze, »"The Complete Guide To Ransomware",« 2021.. [Mrežno]. Available: https://f001.backblazeb2.com/file/backblaze-b2-collateral/Ebook_Complete_Guide_Ransomware.pdf?__hstc=4958124.bff00d2632d0bd296f6f21bde6496029.1669140826128.1669140826128.1669140826128.1. [Pokušaj pristupa 22. studenog 2022.].

[40] National Cyber Security Centre, »"Zero Trust Architecture Design Principles",« 2021.. [Mrežno]. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture. [Pokušaj pristupa 2. listopada 2022.].

[41] R. Badhwar, "The CISO Guide to Zero Trust Security", Wroclaw: Amazon Fullfilment, 2022..

[42] Executive Office of the President of USA, »"Executive Order 14028 (document number 2021-10460)",« 17. svibnja 2021.. [Mrežno]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity. [Pokušaj pristupa 8. studenog 2022.].

[43] R. Rammig, »"Cyber Security in Zeiten von Cyber Crime - International Standards and Regulation",« Siemens AG, 2021.. [Mrežno]. Available: https://www.ost-ausschuss.de/sites/default/files/eventdocs/Regulation-Standardization%2C Dr. Ralf Rammig.pdf. [Pokušaj pristupa 8. studenog 2022.].

[44] NSA Cybersecurity Technical Report, »"Network Infrastructure Security Guidance, ver 1.0",« ožujka 2022.. [Mrežno]. Available: https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF. [Pokušaj pristupa 8. studenog 2022.].

[45] US Department of Defense, »"DoDAF Architecture Framework",« kolovoza 2010.. [Mrežno]. Available: https://dodcio.defense.gov/library/dod-architecture-framework/. [Pokušaj pristupa 8. studenog 2022.].

[46] Hrvatski sabor, »"Zakon o kritičnim infrastrukturama",« 10. svibnja 2013.. [Mrežno]. Available: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html. [Pokušaj pristupa 7. studenog 2022.].

[47] DNV, »"The Cyber Priority - The State of Cyber Security in the Energy Sector",« 2021.. [Mrežno]. Available: https://brandcentral.dnv.com/fr/gallery/10651/files/original/e45ef6c8-fb14-4b0c-98f3-caa889584cd9.pdf?_ga=2.78778516.1699903737.1668010285-758950938.1668010285. [Pokušaj pristupa 09. studenog 2022.].

[48] M. Battista, »"PESTLE analysis",« 6. prosinca 2021.. [Mrežno]. Available: https://www.cipd.co.uk/knowledge/strategy/organisational-development/pestle-analysis-factsheet#gref. [Pokušaj pristupa 9. studenog 2022.].

[49] B. R. Methodology, »PESTLE Analysis,« Business Reasearch Methodology, [Mrežno]. Available: https://research-methodology.net/theory/strategy/7137-2/. [Pokušaj pristupa 4. siječnja 2023.].

[50] Hrvatski sabor, »"Zakon o tržištu plina",« veljače 2018.. [Mrežno]. Available: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_02_18_372.html. [Pokušaj pristupa 9. studenog 2022.].

[51] European Comission, »"EU Cybersecurity Strategy",« 16. prosinca 2020.. [Mrežno]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [Pokušaj pristupa 16. studenog 2022.].

[52] European Comission, »"Prijedlog Direktive Europskog Parlamenta i Vijeća o otpornosti kritičnih subjekata",« 16. prosinca 2020.. [Mrežno]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-

b27b-01aa75ed71a1.0023.02/DOC_1&format=PDF. [Pokušaj pristupa 21. studenog 2022.].

[53] F. M. Vidori, »"The EU Cybersecurity Strategy and the NIS 2 Directive",« siječnja 2021.. [Mrežno]. Available: https://www.lighthouseeurope.com/_files/ugd/ae0383_937ef6fea3214c8ea6e576bf35a4ca32.pdf?index=true. [Pokušaj pristupa 21. studenog 2022.].

[54] KPMG Advisory, »"Security Risk Assessment Methodology Summary",« Gas Infrastructure Europe, Brussels, 2014..

[55] ISO, »ISO/IEC 27001 and related standards - Information security management,« ISO, 2023.. [Mrežno]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Pokušaj pristupa 11. siječnja 2023.].

[56] A. Glossop, »Risk management strategy definition,« Ideagen, 23. travnja 2021.. [Mrežno]. Available: https://www.ideagen.com/thought-leadership/blog/what-is-a-risk-management-strategy. [Pokušaj pristupa 11. siječnja 2023.].

[57] CISA, »Zero Trust Maturity Model, pre-draft version 1.0,« CISA, lipnja 2021.. [Mrežno]. Available: https://www.cisa.gov/zero-trust-maturity-model. [Pokušaj pristupa 13. siječnja 2023.].

[58] Reciprocity, »"What Is Inherent Risk",« 24. ožujka 2022.. [Mrežno]. Available: https://reciprocity.com/resources/what-is-inherent-risk/. [Pokušaj pristupa 22. studenog 2022.].

[59] C. Cunningham i J. Pollard, »"The Eight Business And Security Benefits Of Zero Trust",« 1. studenog 2017.. [Mrežno]. Available: https://advance.biz-tech-insights.com/whitepaper/Forrester-Report-The-Eight-Business-And-Security-Benefits-Of-Zero-Trust.pdf. [Pokušaj pristupa 22. studenog 2022.].

[60] M. Lynd, »"Implementing zero Trust From CISO-s Perspective",« 27. srpnja 2022.. [Mrežno]. Available: https://www.linkedin.com/pulse/implementing-zero-trust-from-cisos-perspective-full-analysis-lynd/?trk=pulse-article. [Pokušaj pristupa 22. studenog 2022.].

[61] J. Carder, »"The Benefits And Barriers When Implementing A Zero Trust Model",« 10. lipnja 2020.. [Mrežno]. Available: https://www.forbes.com/sites/forbestechcouncil/2020/06/10/the-benefits-and-barriers-when-implementing-a-zero-trust-model/?sh=732ed3874cdc. [Pokušaj pristupa 22. studenog 2022.].

PRILOG 1 - POPIS OZNAKA I KRATICA

AD	engl. Active Directory (imenički servis)
BYOD	engl. Bring Your Own Device (donesi svoje vlastito računalo)
CER	engl. Critical Entities Resilience (otpornost kritičnih subjekata)
CI	engl. Configuration Item (konfiguracija jedinica)
CISA	engl. Cybersecurity and Infrastructure Security Agency (Agencija za kibernetičku i infrastrukturnu sigurnost)
CISO	engl. Chief Information Security Officer (rukovoditelj informacijske sigurnosti)
EDR	engl. Endpoint Detection and Response (klijentsko otkrivanje i odgovor na prijetnje)
ERD	engl. entity-relationship diagram (dijagram entiteti-veze)
EU	engl. European Union (Europska Unija)
GIE	engl. Gas Infrastructure Europe (europska udruga svih operatera transporta plina)
HERA	Hrvatska energetska regulatorna agencija
HZMO	Hrvatski zavod za mirovinsko osiguranje
HZZO	Hrvatski zavod za zdravstveno osiguranje
ICT	engl. Information and Communication Technology (informacijske i komunikacijske tehnologije)
IDS	engl. Intrusion Detection System (sustav za otkrivanje upada)
IoT	engl. Internet of Things (Internet stvari)
IP	engl. Internet Protocol (Internet protokol)
IPS	engl. Intrusion Prevention System (sustav za sprječavanje upada)
ISMS	engl. Information Security Management System (sustav upravljanja informacijskom sigurnošću)

ISO	engl. International Organization for Standardization (Međunarodna organizacija za norme)
IT	engl. Information Technology (informacijska tehnologija)
ITIL	engl. Information Technology Infrastructure Library (biblioteka najboljih praksi za upravljanje IT uslugama)
LAN	engl. Local Area Network (lokalna mreža)
NIS	engl. Network and Information Systems (mrežni i informacijski sustavi)
NIS 2	engl. Network and Information Systems 2 (nova verzija NIS direktive)
NIST	engl. National Institute of Standards and Technology (Nacionalni institut za standarde i tehnologiju)
NSA	engl. National Security Agency (američka Nacionalna sigurnosna agencija)
OT	engl. Operational Technology (operativna tehnologija)
PAM	engl. Privileged Access Management (upravljanje privilegiranim pristupom)
POZ	prosječna ocjena zrelosti (za CISA ZTMM)
SaaS	engl. Software-as-a-Service (softver kao usluga)
SCADA	engl. supervisory control and data acquisition (sustav za upravljanje industrijskim procesima i prikupljanje podataka)
SOA	Sigurnosno-obavještajna agencija
SOC	engl. Security Operation Centre (sigurnosni operacijski centar)
SSS	srednja stručna sprema
TCO	engl. Total Cost of Ownership (ukupan trošak vlasništva)
UEBA	engl. User and Entity Behavior Analytics (analitika ponašanja korisnika i uređaja na mreži)
VSS	visoka stručna sprema
ZSIS	Zavod za sigurnost informacijskih sustava
ZTA	engl. Zero Trust architecture (mrežna arhitektura nultog povjerenja)
ZTMM	engl. Zero Trust Maturity Model (Model Zrelosti Nultog Povjerenja)

PRILOG 2 – POPIS TABLICA

PRILOG 3 – POPIS SLIKA

PRILOG 4 – STRUKTURIRANI UPITNIK ZA PRIKUPLJANJE PODATAKA

Procijenite pojedinačne utroške uvođenja sljedećih tehnologija:

- Sustav za upravljanje identitetima
- 802.1x
- Vatrozid sljedeće generacije
- Upravljanje privilegiranim pristupom
- UEBA
- Sustav za orkestraciju
- EDR
- Višefaktorska autentifikacija
- Segmentacija mreže
- Proxy i reverzni proxy

u IT/OT dio mreže tvrtke po kategorijama troška.

a. Izravni jednokratni trošak projekta uvođenja svake pojedinačne tehnologije u poslovne procesa IT/OT segmenta tvrtke
b. Godišnji trošak usluge održavanja licenci, usluga vanjskih ugovornih partnera, hardvera, operativnih sustava, virtualizacijskih licenci i drugih izravnih troškova na nivou prvih godina od dana ulaska tehnologije u produkcijski rad

a. i b. UPISATI: trošak u eurima bez PDV-a

c. Izravni jednokratni utrošak radnih čovjek-dana radnika tvrtke tijekom projekata uvođenja tehnologije u poslovne procesa (sudjelovanje na projektu, edukacija, prikupljanje podataka, integracijske pripreme, revizija dokumentacije)
d. Godišnji utrošak radnih čovjek-dana radnika tvrtke na nivou prvih pet godina od dana ulaska tehnologije u produkcijski rad
    i. *Help desk* aktivnosti
    ii. Pregledi logova
    iii. SOC aktivnosti
    iv. Primjena funkcionalnih i sigurnosnih zakrpi
    v. Upravljane incidentima unutar i izvanrednog vremena

c. i d. UPISATI: ukupni broj radnih čovjek-dana

NAPOMENA: podaci se upisuju samo u žuto označena polja!

UPITNIK - IT/OT OKRUŽENJE					
Rb.	**Projekt**	**Vrijednost projekta**	**Trošak održavanja godina 1**	**Trošak održavanja godina 2**	**Trošak održavanja godina 3**
1	Sustav za upravljanje identitetima				
2	802.1x				
3	Vatrozid slijedeće generacije				
4	Upravljanje privilegiranim pristupom				
5	UEBA				
6	Sustav za orkestraciju				
7	EDR				
8	Višefaktorska autentifikacija				
9	Segmentacija mreže				
10	Proxy i reverzni proxy				
		€ -	**€ -**	**€ -**	**€ -**

UPITNIK - IT/OT OKRUŽENJE			
Rb.	**Projekt**	**Trošak održavanja godina 4**	**Trošak održavanja godina 5**
1	Sustav za upravljanje identitetima		
2	802.1x		
3	Vatrozid slijedeće generacije		
4	Upravljanje privilegiranim pristupom		
5	UEBA		
6	Sustav za orkestraciju		
7	EDR		
8	Višefaktorska autentifikacija		
9	Segmentacija mreže		
10	Proxy i reverzni proxy		
		€ -	**€ -**

UPITNIK - IT/OT OKRUŽENJE								
Rb.	**PROJEKT**	**Količina vlastitih čovjek/dana - PROJEKT**	**Količina vlastitih čovjek/dana ODRŽAVANJE godina 1**	**Količina vlastitih čovjek/dana ODRŽAVANJE godina 2**	**Količina vlastitih čovjek/dana ODRŽAVANJE godina 3**	**Količina vlastitih čovjek/dana ODRŽAVANJE godina 4**	**Količina vlastitih čovjek/dana ODRŽAVANJE godina 5**	**UKUPNA količina vlastitih čovjek/dana**
1	Sustav za upravljanje identitetima							**0,00**
2	802.1x							**0,00**
3	Vatrozid slijedeće generacije							**0,00**
4	Upravljanje privilegiranim pristupom							**0,00**
5	UEBA							**0,00**
6	Sustav za orkestraciju							**0,00**
7	EDR							**0,00**
8	Višefaktorska autentikacija							**0,00**
9	Segmentacija mreže							**0,00**
10	Proxy i reverzni proxy							**0,00**
		0,00	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**

11. ŽIVOTOPIS AUTORA

Goran Kapić rođen je 1973. godine u Zagrebu. Diplomirao je 1997. godine na FER-u u Zagrebu, smjer Telekomunikacije i informatika, te je završio postdiplomske tečajeve na poslovnim školama *Global Development Learning Network (by the World Bank) & KDI School of Public Policy*, te *Henley Business School, University of Reading*. Tijekom 25 godina karijere radio je na više pozicija u poslovnoj informatici i korporativnoj sigurnosti u raznim rukovodećim rolama, a danas radi kao CISO i pomoćnik predsjednika uprave za kibernetiku sigurnost u tvrtki državnom operatoru energetske kritične infrastrukture. Nositelj je dvadesetak stručnih certifikata iz područja kibernetičke i informacijske sigurnosti, te ITIL najboljih praksi.

12. BIOGRAPHY

Goran Kapić was born in 1973 in Zagreb. He graduated in 1997 from FER in Zagreb, majoring in Telecommunications and Informatics, and completed postgraduate courses at the *Global Development Learning Network (by the World Bank) & KDI School of Public Policy*, and *Henley Business School, University of Reading*. During his 25-year career, he has worked in several positions in business IT departments and corporate security in various management roles, and today he works as CISO and assistant to the president of the board for cyber security in a state-owned operator of critical energy infrastructure. He holds twenty professional certificates in the field of cyber and information security, as well as ITIL best practices.