Upravljanje informacijskom sigurnošću grada Rovinja-Rovigno

Hrelja, Randi

ISTARSKO VELEUČILIŠTE-

UNIVERSITÀ ISTRIANA DI SCIENZE APPLICATE

Randi Hrelja

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU GRADA ROVINJA-ROVIGNO

Specijalistički završni rad

Pula, 2021.

ISTARSKO VELEUČILIŠTE-

UNIVERSITÀ ISTRIANA DI SCIENZE APPLICATE

Randi Hrelja

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU GRADA ROVINJA-ROVIGNO

Specijalistički završni rad

JMBAG: 0233008259
Studijski smjer: Kreativni menadžment u procesima
Predmet: Poslovni informacijski sustavi
Mentor: Marko Turk, dipl.oec., pred.

Pula, 2021.

Sadržaj

1. UVOD 3
2. INFORMACIJSKA SIGURNOST 5
   2.1. Pojam i povijesni razvoj informacijske sigurnosti 5
   2.2. Aspekti informacijske sigurnosti 7
   2.3. Prijetnje u kontekstu informacijske sigurnosti 9
   2.4. Ranjivost informacijskog sustava 11
   2.5. Napadi na informacijski sustav 12
   2.6. Zaštitne mjere za upravljanje informacijskim sustavom 13
3. ZAKONSKA REGULATIVA I INSTITUCIJE SIGURNOSTI INFORMACIJSKIH SUSTAVA U RH 15
   3.1. Zakoni iz područja informacijske sigurnosti u RH 15
   3.2. Institucije informacijske sigurnosti u RH 18
   3.3. Norme iz područja informacijske sigurnosti u RH 21
4. UTJECAJ UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU NA POSLOVNI KONTINUITET GRADA ROVINJA - ROVIGNO 25
   4.1. Grad Rovinj-Rovigno kao jedinica lokalne samouprave 25
   4.2. Pojam kontinuiteta poslovanja 37
   4.3. Veza između kontinuiteta poslovnih procesa i informacijske sigurnosti 39
   4.4. Odgovor na sigurnosne incidente i mjere zaštite informacijskih resursa u Gradu Rovinju- Rovigno 39
   4.5. Oporavak od havarije 42
5. METODOLOGIJA ISTRAŽIVANJA 44
   5.1. Predmet rada 44
   5.2. Ciljevi rada 44
   5.3. Istraživačka pitanja 44
   5.4. Odabrana metodologija procjene rizika 45
   5.5. Metoda analize proračunskih godina 55
6. PROCJENA RIZIKA ZA GRAD ROVINJ-ROVIGNO 61
   6.1. Karakterizacija sustava 61
   6.2. Identificiranje prijetnji 61
   6.3. Identifikacija ranjivosti 62
   6.4. Analiza kontrola 63
   6.5. Određivanje vjerojatnosti 64

6.6. Analiza utjecaja 64
6.7. Određivanje rizika 65
6.8. Matrica rizika 66
6.9. Preporuka kontrola za umanjivanje rizika 67
6.10. Snimak trenutnog stanja u Gradu Rovinju-Rovigno 67
7. RASPRAVA 72
8. ZAKLJUČAK 74
9. LITERATURA 76
SAŽETAK 81
SUMMARY 81
POPIS TABLICA: 82
POPIS SLIKA: 82

1. UVOD

„Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, te okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tad, ne bih se baš kladio na njega."

(Eugene Spafford)

Informatika omogućuje smanjivanje ili potpuno isključivanje ljudskog rada iz obavljanja velikog broja rutinskih operacija. Čovjekov rad se u današnje vrijeme najviše oslanja na informacijsku tehnologiju bez koje bi suvremeno oblikovani informacijski sustavi bili neefikasni ili neekonomični. Informacije koje se u današnje vrijeme sve više smatraju najvećom imovinom svake organizacije potrebno je prikladno zaštititi kako bi se omogućilo normalno poslovanje.

Okvir ovog rada ističe potrebu upravljanja informacijskom sigurnošću u svrhu zaštite informacija i vlasništva podataka u Gradu Rovinju-Rovigno, koji putem svojih aktivnosti i usluga, unapređuje kvalitetu života i rada svojih građana putem pružanja izvrsne usluge, omogućavanjem participacije u odlučivanju, odgovornim upravljanjem javnim dobrima, protokom informacija te nadasve ljubaznim, efikasnim i transparentnim poslovanjem.

Zahtjev za zaštitom informacija sve je važniji jer u okruženju distribuiranosti poslovne okoline informacije postaju izložene ranjivosti i sve većem broju prijetnji. Bez obzira u kojem se obliku informacija nalazila vrlo je važno prikladno je zaštititi. Informacije mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi elektroničkim putem i sl. Bilo koja od tih oblika informacija, u današnje vrijeme predstavlja najvažniji i najskuplji resurs u poslovanju. Pravovremeno posjedovanje informacija, ispravnost i tajnost informacija omogućuju svakoj organizaciji napredak.

Završni rad prikazuje značajke informacijskih sustava i informacijske sigurnosti te utjecaj upravljanja informacijskom sigurnošću na kontinuitet poslovanja u Gradu Rovinj-Rovigno.

U prvom dijelu rada slijedeći brojnu literaturu i autore, definiran je sam pojam informacijske sigurnosti, govori se o aspektima informacijske sigurnosti, prijetnjama, ranjivostima i napadima koji se sve češće pojavljuju. Također su opisane i definirane zaštitne mjere za sprječavanje neželjenih posljedica. Također, obrađuju se pravni

aspekti upravljanja informacijskom tehnologijom u poslovanju. Razvoj i sve šire korištenje elektroničkih komunikacija dovelo je do novih odnosa kao i potrebe reguliranja prava i obveza kako korisnika tako i davatelja usluga informacijskog društva. Samim time neophodno je došlo do stvaranja raznih institucija u svrhu praćenja i provođenja zakonske regulative sigurnosti informacijskog sustava. Naveden je zakonski okvir Republike Hrvatske vezano za informacijsku sigurnost te su opisane institucije vezane za informacijsku sigurnost u RH. Isto tako se navode temeljne norme ISO/IEC 27001 i ISO/IEC 27002 koje predstavljaju sustav upravljanja i kodeks postupka za upravljanje informacijskom sigurnošću.

U drugom dijelu rada opisuju se rizici na aplikativnom primjeru grada Rovinja – Rovigno. Opisano je ustrojstvo i djelovanje gradske uprave Grada Rovinja-Rovigno te način komuniciranja i korištenja informacijske tehnologije, koje uvelike doprinosi ubrzanju operativnih procesa i optimizaciji troškova. Obrađen je kontinuitet poslovanja, te stvaranje veze između kontinuiteta poslovanja i informacijske sigurnosti. Prezentirane su metode koje se koriste u rješavanju eventualnih nemilih događaja i kako se u slučaju havarije na najbrži mogući način vratiti poslovnom procesu a sve u svrhu dobrog poslovnog ugleda, osiguranja tržišne konkurentnosti i zadovoljavanja propisane zakonske regulative. Nadalje, opisana je metodologija procjene sigurnosnog rizika za Grad Rovinj, postavljena su istraživačka pitanja, navedeni su ciljevi te predmet rada .

U posljednjem dijelu su prezentirani rezultati procjene rizika odabranom metodom, te su temeljem rezultata analize doneseni zaključci koji osiguravaju poslovni kontinuitet grada Rovinja – Rovigno.

2. INFORMACIJSKA SIGURNOST

Informacijska sigurnost koncept je koji se sve više upliće u mnoge aspekte našeg društva, uglavnom kao rezultat gotovo sveprisutnog usvajanja računalne tehnologije. U svakodnevnom životu računala se koriste za poslodavce, za igranje zahtjevnih računalnih igrica, u školama za praćenje nastave, računalima se putem interneta kupuje roba u web trgovinama. Katkad se prijenosna računala koriste u kafićima za provjeru elektroničke pošte, pametnim telefonima se provjerava stanje računa u banci.

Isto tako se pomoću raznih senzora u satovima i cipelama prati zdravlje, a mobitelom se na daljinu upravljaju i nadziru razni kućanske aparati kao što su npr. usisavači ili klima uređaji.

Iako tehnologija danas omogućuje veću produktivnost i pristup mnoštvu informacija samo klikom miša, ona uz to donosi i niz sigurnosnih problema. Ako npr. podaci o sustavima koje koriste poslodavci ili banke postanu izloženi napadaču, posljedice mogu katastrofalne. Ono što se nerijetko može pročitati u medijima ili pogledati na vijestima sve su učestaliji hakerski napadi na velike korporacije, banke a u zadnje vrijeme i na male kućne korisnike čime napadači pokušavaju raznim metodama otuđiti ili iznuditi određenu korist.

U općenitom smislu, sigurnost znači zaštitu naše imovine. To može značiti zaštitu od napadača koji napadaju naše mreže, zaštitu od prirodnih katastrofa zaštitu od prekida napajanja, krađa ili vandalizma.

Krajnji cilj je osigurati imovinu od najvjerojatnijeg oblika napada, u onoj mjeri u kojoj se to razumno može s obzirom na postojeće okruženje.

2.1. Pojam i povijesni razvoj informacijske sigurnosti

Pod pojmom informacijske sigurnosti podrazumijeva se povjerljivost, cjelovitost, raspoloživost, te zaštita i sigurnost podataka u poslovnim procesima informacijskog sustava primjenom mjera i standarda (Nacionalni CERT, Upravljanje kontinuitetom poslovnih procesa, 2010).

Trendovi globalizacije kroz informatičko povezivanje traže od svih zemalja i trgovačkih društava zadovoljenje osnovnih zahtjeva za učinkovito međusobno djelovanje i informacijsku sigurnost.

Ubrzani razvoj informacijskih mreža u posljednjim godinama zahtijevao je od privatnih i državnih organizacija ugradnju učinkovitih mjera informacijske sigurnosti kako bi unaprijedile svoj kredibilitet i konkurentnost na tržištu.

Povijesni razvoj informacijske sigurnosti datira iz 60-ih godina 20. stoljeća kada se krenulo sa primjenom računala, a sigurnost je tada rezultirala fizičkom zaštitom i sigurnošću računala. Računala su u to vrijeme imala relativno visoku cijenu, te se zaštita bazirala na zaštiti od fizičkog uništenja, požara i sl.

Razdoblje primjene tranzistorskih komponenti u kasnijim 60 - im godinama prošlog stoljeća, unaprijedilo je komunikaciju između čovjeka i stroja, omogućilo porast obrade podataka, niže cijene računala, uz sve napredniju informacijsku tehnologiju. Započinje razdoblje takozvane sigurnosti podataka. Broj korisnika informacijske tehnologije se povećava u kvalitativnom i kvantitativnom obliku, što ujedno rezultira pohranjivanjem na nove magnetske medije. Naglasak sa fizičke zaštite računala premješten je na zaštitu i sigurnost podataka i informacija.

Sedamdesetih godina koristi se interaktivni način rada, koji se očituje u obradi u realnom vremenu, uporabom računalnih lozinki, metodom pohranjivanja podataka, informacija i programa na vanjske medije s ciljem zaštite od eventualnog uništenja.

Razdoblje osamdesetih godina prošlog stoljeća donosi novo razdoblje sigurnosti, takozvane sigurnosti informacija. Samim time, naglašava se informacija kao najvažniji, ali i najranjiviji gospodarski resurs. U narednom razdoblju ovisnost o informacijskim tehnologijama nastavlja se povećavati. Osnovna značajka se ne očituje u kvantitativnoj pohrani sve veće količine podataka i informacija na magnetskim i optičkim medijima, nego prerastanje današnjih informacijskih sustava u sustave za pohranu i obradu informacija, odnosno znanja.

Čizmić i dr., (2016, 469-470) tvrde kako apsolutna zaštita sustava i podataka nije moguća. Prvenstveno je riječ o metodama suzbijanja, rješavanja i sprječavanja opasnostima kojima je informacijski sustav izložen.

2.2. Aspekti informacijske sigurnosti

Kako bi se uopće moglo govoriti o aspektima informacijske sigurnosti mora se definirati informacijski sustav. Informacijski sustav je onaj koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju i društvo, tako da budu dostupne i upotrebljive svakome kome su potrebne. To je skup uzajamno povezanih komponenata koje rade zajednički na unosu, obradi, isporuci, pohranjivanju i drugim upravljačkim aktivnostima kojima podatke pretvaraju u informacije namijenjene predviđanju, planiranju, upravljanju, koordinaciji, donošenju odluka i operativnim aktivnostima u organizaciji (Varga i Strugar, 2016, 6 prema Bocij i dr., 2006.).

Osnovni aspekti informacijske sigurnosti odnose se na očuvanje vrijednosti i tajnosti podataka, a očituju se u:

- povjerljivosti podataka,
- integritetu podataka i
- njihovoj raspoloživošću tj. dostupnošću.

Povjerljivost podataka neophodna je u svakom informacijskom sustavu kako bi zaštitila informacije od neželjenog objavljivanja. Time se podrazumijeva tajnost podataka i dostupnost podataka samo ovlaštenim osobama.

Najveća pažnja usmjerena je na identifikaciju i autentikaciju korisnika, a metode koje se primjenjuju u tu svrhu su metoda kontrole pristupa i metoda enkripcije sa neophodnim postojanjem tajnog ključa za dostupnost informacijama.

Tri su osnovna autentikacijska pristupa:

- dokaz znanjem (korisniku se omogućava pristup podacima provjerom nečega što zna samo autorizirani korisnik npr. lozinka),
- dokaz posjedovanjem (svoj identitet korisnik dokazuje predočenjem predmeta kojeg može samo on posjedovati npr. magnetna ili čip kartica sa upisanim važnim podacima u digitalnom obliku) i
- dokaz osobinom (identitet se dokazuje fizičkim osobinama koje nije lako krivotvoriti npr. otisak prsta, zjenica oka ili sl.).

Ovakav pristup autentikacije se temelji na činjenici nemogućnosti izbjegavanja odgovornosti i omogućava povezivanje vjerodostojnosti, tajnosti i identifikacije na

način da korisnik koji je autenticiran ujedno i snosi odgovornost za proces koji je izvršen (Čizmić i dr., 2016, str.545).

Metoda enkripcije omogućuje korisniku da uz poseban tajni ključ pristupi i ima uvid podacima. Istim tim podacima se bez tajnog ključa isto može pristupiti ali oni neće biti razumljivi.

Integritet informacija kao drugi aspekt sigurnosti informacijskog sustava znači zaštititi informacije od neovlaštenog korištenja i očuvanje istih od nenamjernih promjena.

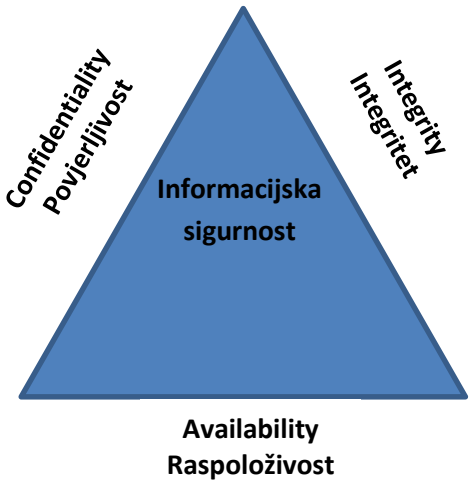
Navedeni aspekt je također moguće očuvati uz primjenu obje gore navedene metode; jednostavna metoda kontrole pristupa i složenija metode enkripcije.

Postojanjem navedenog aspekta osigurava se nemogućnost mijenjanja postojećih podatka i informacija neovlaštenim osobama, a time u konačnici održavanje konzistentnosti podataka i programa.

Raspoloživost znači dostupnost podataka i informacija ovlaštenim korisnicima, a važna karakteristika ovog aspekta je omogućiti uvid korisnicima informacija njenu dostupnost u svakom trenutku bez obzira na vanredne moguće situacije uslijed kojeg se sustav narušava. Dostupnost se može narušiti na nekoliko načina:

- uskraćivanjem usluge u smislu zagušenja, primjerice mrežne opreme ili poslužitelja,
- kroz gubitak sposobnosti procesiranja podataka kao rezultat prirodnih katastrofa kao što su to poplave, požari i potresi i sl.

Sva tri aspekta međusobno su povezana te se prikazuju u osnovnom sigurnosnom trokutu (eng. CIA triad) na Slici 1.



Slika 1 Povezanost triju aspekta informacijske sigurnosti CIA

Izvor: http://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/290-2014.pdf

Prema svemu sudeći kako bi informacijski sustavi bili djelotvorni i sigurni u svome radu moraju zadovoljiti sve navedene aspekte (Andress, 2014, str.15).

2.3. Prijetnje u kontekstu informacijske sigurnosti

Informacijski sustavi su osnova modernog poslovanja, a baziraju se na računalnim mrežama te Internetu kao najvećoj i najpoznatijoj mreži. Raširenim pristupom dolazi do narušavanja poslovnih informacijski sustava, a uzrokuju ih prijetnje koje pokušavaju ugroziti cijeli poslovni sistem. U kontekstu informacijske sigurnosti prijetnja je objekt, osoba ili drugi entitet koji predstavlja stalnu opasnost za imovinu organizacije, a prema Stojaković – Čelustka (2020), prijetnjom možemo nazvati i svaku silu ili sredstvo koja može smanjiti učinkovitost sustava odnosno ograničiti ili onemogućiti ispunjenje cilja.

Da bi se realizirala i rezultirala štetom, prijetnja mora iskoristiti postojeću ranjivost imovine, stoga je potrebno točno utvrditi njihovu razinu i vjerojatnost (mala, srednja, velika).

Postoje različiti izvori i oblici prijetnji sigurnosti informacijskih sustava, a možemo ih podijeliti prema izvoru kao:

- prirodne nepogode (onečišćenja, požar, incidentne situacije, oluja, potres, poplava idr.),
- nenamjerne prijetnje ljudi (nepažnja, nedisciplina, nemar, neznanje, neadekvatna organizacija),
- namjerne prijetnje ljudi (neautorizirani pristup, krađa, maliciozni programi, prisluškivanje, uništenje, razno razaranje),
- oprema (tehnička pogreška opreme, prestanak napajanja, ispadi opreme, prekid komunikacije idr.).

Svi se ti oblici očituju gubitkom povjerljivih informacija, što je u današnjem trendu globalizacije u velikoj mjeri prisutno kao ozbiljni napad na informacijsku infrastrukturu korporacije.

Najčešće su slijedeće prijetnje: hakiranje, neovlaštena korisnička aktivnost, nezaštićeno preuzimanje datoteka s lokalne mreže, trojanski konji i ostale nepredviđene okolnosti.

Kada je riječ o integritetu podataka, njegovo narušavanje može se dogoditi kroz neovlaštene promjene, a prekid rada sustava uzrokuje nedostupnost servisa ili podataka.

Raspoloživost se može narušiti na nekoliko načina. Najčešće je to uskraćivanje usluge zbog gušenja na mrežnoj opremi ili poslužiteljima te nemogućnost procesuiranja podataka zbog prirodnih katastrofa poput potresa ili poplava i sl.

Gledano u globalu najviše prijetnji se odnosi prvenstveno na narušavanje tajnosti informacija što je povezano s povjerljivosti.

Vukelić (2016) je rekao da se osim prema izvoru, prijetnje mogu grupirati i prema slijedećem:

- logička infiltracija,
- komunikacijska infiltracija,
- kvarovi na opremi,
- pogreške radi zaposlenika,
- fizičke prijetnje,

a svaka prijetnja ima obilježja koja daju korisne informacije o samoj prijetnji. To su:

- izvor (unutarnja ili vanjska prijetnja),
- motiv (ostvarivanje financijske dobiti, konkurentske prednosti),

- učestalost pojavljivanja,
- veličina razorne moći.

2.4. Ranjivost informacijskog sustava

„Ranjivost sama po sebi ne nanosi štetu. Možemo je definirati kao stanje ili skup stanja koji može omogućiti nekoj prijetnji da utječe na resurse (primjerice nedostatak mehanizama kontrole pristupa je ranjivost koja bi mogla omogućiti ostvarenje prijetnje neovlaštenog pristupa, što može dovesti do gubitka ili oštećenja resursa).” (Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, 2006.)

Slijedom velike rasprostranjenosti informacijske tehnologije uz ogroman broj korisnika Interneta, dolazi do povećane implementacije elektroničkog poslovanja u svim segmentima društva i gospodarstva te se sve više ulaže u segment komunikacijske zaštite u svrhu informacijske sigurnosti.

Postepeno se razvija i svijest o „nezaštićenosti“ pri pristupanju mreži, čime se ulazi u posve nepoznat, ogroman prostor, koji nazivamo „*cyberspace*“. Riječ je o prostoru koji nije opipljiv na dodir, koji svojim širokim djelovanjem prelazi granice države i kontinenata. Takvim se ishodom sa jedne strane, korisnici informacijskog sustava zbližuju i omogućuju razmjenu podataka u vrlo kratkom vremenu, međutim sa druge strane isti taj sustav rezultira ranjivošću i nemogućnošću da se potpuno zaštiti (Radmilović, 2015, str. 32).

Ranjivost se najčešće povezuje s propustima u programskom kodu, no mogući su i mnogi drugi primjeri, kao što su površno implementirana fizička sigurnost, nedovoljno poznavanje i neprikladan izbor tehnologija i alata, propusti u dizajnu sustava, propusti u implementaciji i održavanju sustava i sl.

S obzirom na prirodu i faze informacijskog sustava razlikujemo tri osnovna tipa ranjivosti (Rittinghouse i Ransome, 2005, 96):

- ako informacijski sustav još nije dizajniran, ispitivanje ranjivosti potrebno je fokusirati na sigurnosnu politiku organizacije, planirane sigurnosne postupke te na razvojnu sigurnosnu analizu proizvoda;
- ako je informacijski sustav u fazi implementacije, identifikacija ranjivosti je proširena i uključuje više specifičnih podataka, kao opis značenja

planirane sigurnosti u dokumentaciji dizajna sigurnosti te rezultate testiranja i ocjene sustava;

- ako je sustav u radu, proces identifikacije ranjivosti treba uključivati analize obilježja informacijskog sustava i sigurnosne kontrole, tehnike i postupke koji se upotrebljavaju u zaštiti sustava.

Zorčec M.(2006) navodi kako bi se uspješno identificirale ranjivosti sustava, potrebno je izvršiti testiranje samog sustava ovisno o kritičnim točkama informacijskog sustava i dostupnim resursima (tehnologija, stručno osoblje za testiranje).

Metode ispitivanja ranjivosti jesu (Vukelić B., 2016, str.17):

- alati za automatsko skeniranje ranjivosti (koriste se metodom koja skenira korisnike mreže na poznate ranjive servise poput FTP protokola, ali ovi alati ne mogu pokazati realne ranjivosti u sklopu okruženja u koje se nalazi informacijski sustav);
- sigurnosni testovi i vrednovanja (testiranje efikasnosti ugrađenih sigurnosnih kontrola u informacijskom sustavu, tako da kontrole zadovoljavaju sigurnosnu politiku i standarde organizacije);
- testiranje upada u sustav (procjena sposobnosti da se informacijski sustav odupre namjernim pokušajima zaobilaženja sigurnosnog sustava);
- popisi ranjivosti drugih organizacija;
- dokumentacija od prethodnih analiza rizika procjenjivanog informacijskog sustava

2.5. Napadi na informacijski sustav

Napadi na informacijski sustav su akcije kojim se ugrožavaju sigurnost informacija. Budući da je današnji život raznoraznim tehnološkim dostignućima sastavljen od primjene komunikacijskih sredstava na tehničkoj razini, informacijski sustav je u neprestanoj obrani i odgovorima na napad.

Razvojem interneta i njegovim velikim utjecajem na ljudski život dolazi se do računalnog kriminaliteta kao najvećeg napada na informacijski sustav. Računalni kriminalitet je posebna kategorija napada, budući da može djelovati na ugrožavanje

informacijskog sustava ne samo korištenjem računala već i oštećenjem samih medija za pohranu.

Računalni kriminalitet obuhvaća kaznena djela kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost tehničke, programske ili podatkovne strukture kompjuterskog sustava ili na tajnost digitalnih podataka (Čizmić, i dr., 2016, 481-500).

2.6. Zaštitne mjere za upravljanje informacijskim sustavom

Gledano sa tri osnovna aspekta informacijske sigurnosti, zaštitne mjere za upravljanje informacijskim sustavom isto obuhvaćaju očuvanje tajnosti podataka, integriteta i raspoloživosti podataka.

Informacijski sustav se može zaštiti na unutarnjoj razini, odnosno kontrolom pomoću računala i na vanjskoj razini, tj. pomoću umreženih sustava.

Prema Čizmiću (2016), zaštita i sigurnost podataka umreženih sustava obuhvaća slijedeće razine:

1) Hardversko-softverska zaštita i sigurnost
2) Fizička i organizacijska zaštita i sigurnost
3) Zakonodavna zaštita i sigurnost
4) Komunikacijska zaštita (kripto zaštita) i informacijska sigurnost .

Hardversko-softverska zaštita i sigurnost temelji se na korištenju uobičajenih hardversko-softverskih mogućnosti sustava i uređaja što omogućuju njihov rad. Hardverska zaštita i sigurnost se uglavnom primjenjuje na zaštitu memorije i telekomunikacija dok se softverska zaštita i sigurnost primjenjuje na zaštiti programskih paketa, datoteka i ulazno/izlaznih jedinica.

Fizička i organizacijska zaštita i sigurnost temelji se na zaštiti cjelokupnog objekta i okoline, njenu primjenu izvršavaju svi djelatnici, te se smatra klasičnom metodom zaštite i sigurnosti (Ždrnja**,** 2010).

Pravna ili zakonodavna zaštita i sigurnost se temelji na izvršavanju zaštite umreženih sustava regulirane zakonskim propisima na razini države i smatra se takozvanom administrativnom kontrolom zaštite. Tu podrazumijevamo kontrolu i organizaciju baze podataka, kontrolu poštovanja propisanih mjera zaštite podataka,

kontrolu i evidenciju pristupa podacima, kontrolu lozinki koje treba periodički mijenjati te kontrolu dokumentacije o sustavu, programima i slično.

Komunikacijska zaštita i sigurnost temelji se na zaštiti podataka koji se kreću komunikacijskim kanalom unutar umreženog sustava. Komunikacijski kanali su najranjiviji dijelovi sustava, pa se zbog toga najveća pozornost pridaje upravo takvom načinu zaštite. U tu svrhu se koriste i hardverska i softverska rješenja, a neke od metoda koje se koriste su kriptografska zaštita, korištenje pametnih kartica, korištenje specijalnih uređaja za promjenu signala (*scrambling*) i drugo.

3. ZAKONSKA REGULATIVA I INSTITUCIJE SIGURNOSTI INFORMACIJSKIH SUSTAVA U RH

Informacijski sustavi se kroz povijest ubrzano i intenzivno razvijaju. Šezdesete godine prošlog stoljeća su obilježile početak pravne regulacije na području zaštite osobnih podataka, sedamdesete su obilježile pravnu zaštitu od gospodarskog računalnog kriminaliteta, osamdesete zaštitu intelektualnog vlasništva, dok su devedesete obilježile stvaranje i uspostavljanje normativnog okvira regulacije elektroničkog trgovanja.

Raširenost korištenja elektroničkih komunikacija dovodi do novih odnosa, a ujedno i potrebu reguliranja prava i obveza korisnika i davatelja usluga informacijskog društva.

3.1. Zakoni iz područja informacijske sigurnosti u RH

Raširenost trenda informacijskog društva, koje je doprinijelo unaprjeđenju kvalitetne komunikacije i oplemenilo razvoj tehnologija, uvodi potrebu analiziranja i zaštite podataka kako sa sigurnosnog tako i sa pravnog aspekta.
Republika Hrvatska, kao članica Europske Unije obavezna je uskladiti svoje zakonodavstvo sa regulativom EU-a pa tako i vezano za zaštitu podataka.

Juran (2014), je navela da je Hrvatski Sabor donositelj pravnih oblika i Zakona vezanih za informacijsku sigurnost te je nabrojala i opisala neke od Zakona donesenih na temu informacijske sigurnosti od kojih su najvažniji:

- Zakon o zaštiti osobnih podataka,
- Zakon o sigurnosno-obavještajnom sustavu RH,
- Zakon o elektroničkoj ispravi,
- Zakon o informatičkoj sigurnosti,
- Zakon o provedbi opće uredbe o zaštiti podataka i drugi.

Na tragu zaštite tajnosti podataka i postavljanja temelja za razvoj zakonodavne regulative i uredbi u području informacijske sigurnosti osnovan je Središnji Državni Ured za e-Hrvatsku (SDUeH), kao tijelo Vlade Republike Hrvatske zaduženo za

koordinaciju povezivanja informacijskih sustava tijela državne uprave jedinstvenom informacijskom-komunikacijskom mrežom te za donošenje tehničkih i normizacijskih pravila uporabe informatičke opreme u tijelima državne uprave (Čizmić i dr., 2016, 683)

Zakon o zaštiti osobnih podataka donio je Hrvatski Sabor u lipnju 2003. godine, a njime se uređuje zaštita osobnih podataka fizičkih osoba te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u RH (Zakon o zaštiti osobnih podataka, 2012).

U lipnju 2006. Hrvatski Sabor donosi *Zakon o sigurnosno-obavještajnom sustavu RH.*

Ovim se Zakonom, radi sustavnog prikupljanja, analize, obrade i ocjene podataka koji su od značaja za nacionalnu sigurnost, u cilju otkrivanja i sprječavanja radnji pojedinaca ili skupina koje su usmjerene protiv opstojnosti, neovisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, nasilnom rušenju ustroja državne vlasti, ugrožavanju Ustavom Republike Hrvatske i zakonima utvrđenih ljudskih prava i temeljnih sloboda te osnova gospodarskog sustava Republike Hrvatske i koji su nužni za donošenje odluka značajnih za ostvarivanje nacionalnih interesa u području nacionalne sigurnosti, osnivaju sigurnosno-obavještajne agencije:

- Sigurnosno - obavještajna agencija (SOA)[1], prikuplja, analizira, obrađuje i ocjenjuje političke i gospodarske podatke, znanstveno-tehnološke i sigurnosne prirode koji se odnose na strane države, organizacije, političke i gospodarske saveze, skupine i osobe, osobito one koji ukazuju na namjere, mogućnosti, prikrivene planove i tajna djelovanja usmjerena na ugrožavanje nacionalne sigurnosti, odnosno podatke koji su od značaja za nacionalnu sigurnost Republike Hrvatske.
- Vojna sigurnosno - obavještajna agencija (VSOA)[2] prikuplja, analizira, obrađuje i ocjenjuje podatke o vojskama i obrambenim sustavima drugih zemalja, o vanjskim pritiscima koji mogu imati utjecaj na obrambenu sigurnost te aktivnostima u inozemstvu koje su usmjerene na ugrožavanje obrambene sigurnosti zemlje.

[1] Više informacija na linku https://www.soa.hr/hr/informacije/faq/
[2] Više informacija na linku https://www.soa.hr/hr/informacije/faq/

Zakon o elektroničkoj ispravi uređuje pravo fizičkih i pravnih osoba na uporabu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku (Juran, 2014, str.29). Elektronička isprava ima istu pravnu snagu kao i isprava na papiru, ako se njena uporaba i promet provode u skladu s odredbama ovoga zakona. Elektronička isprava u procesima prikazivanja sadržaja, kao i u tijeku rukovanja sadržajima ugrađenim u elektroničku ispravu, sadrži obvezno unutarnji i vanjski obrazac prikaza (Zakon o elektroničkoj ispravi, 2005).

- unutarnji obrazac prikaza sastoji se od tehničko-programskog obrasca zapisivanja sadržaja u elektroničkom obliku na medij koji zadržava ili prosljeđuje elektroničku ispravu.
- vanjski obrazac sastoji se od vizualnog i razumljivog prikaza sadržaja elektroničke isprave na zaslonu računalnih ili drugih elektroničkih uređaja, na papiru ili drugom materijalnom predmetu proizvedene (odvojene) iz zapisa u elektroničkom obliku.

Zakon o informacijskoj sigurnosti donesen je u srpnju 2007. godine, a daje nam smjernice o povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Prema Zakonu o informacijskoj sigurnosti (2018) područja informacijske sigurnosti za koja se propisuju mjere i standardi su:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podatka,
- sigurnost informacijskog sustava,
- sigurnost poslovne suradnje.

Zakon o provedbi opće uredbe o zaštiti podataka donesen je u travnju 2018. Ovim Zakonom osigurava se provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka.

3.2. Institucije informacijske sigurnosti u RH

Slijedom donesenih Zakona u svrhu reguliranja informacijske sigurnosti, dolazi do osnivanja institucija koje djeluju u skladu sa donesenim pravilima i Zakonima a one su:

- Nacionalni CERT,
- Zavod za sigurnost informacijskih sustava,
- Ured vijeća za nacionalnu sigurnost,
- Agencija za podršku informacijskim sustavima i informacijskim tehnologijama,
- Agencija za zaštitu osobnih podataka,
- Središnji državni ured za e-Hrvatsku.

Nacionalni CERT[3] (engl. Computer Emergency Response Team) osnovan je u skladu sa Zakonom o informacijskoj sigurnosti Republike Hrvatske 30. listopada 2007. godine. Zadaća Nacionalnog CERT-a je provođenje reaktivnih i proaktivnih mjera kojima se želi podići i očuvati razina sigurnosti informacijskih sustava u Republici Hrvatskoj. Reaktivne mjere prvenstveno čini obrada računalno sigurnosnih incidenata na internetu, tj. očuvanje informacijske sigurnosti u Republici Hrvatskoj.

Pod obradom incidenata podrazumijeva se koordinacija uključenih strana, forenzička analiza, analiza zlonamjernog softvera, mrežnog prometa i logova. Uz reaktivne, u djelovanje Nacionalnog CERT-a spadaju i proaktivne mjere koje podrazumijevaju diseminaciju informacija (vijesti, preporuke, dokumenti, brošure, alati), održavanje predavanja i webinara, sudjelovanje na konferencijama te rad na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj (Nacionalni CERT, 2020).

[3] https://www.cert.hr/onama/ (lipanj 2020.)

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

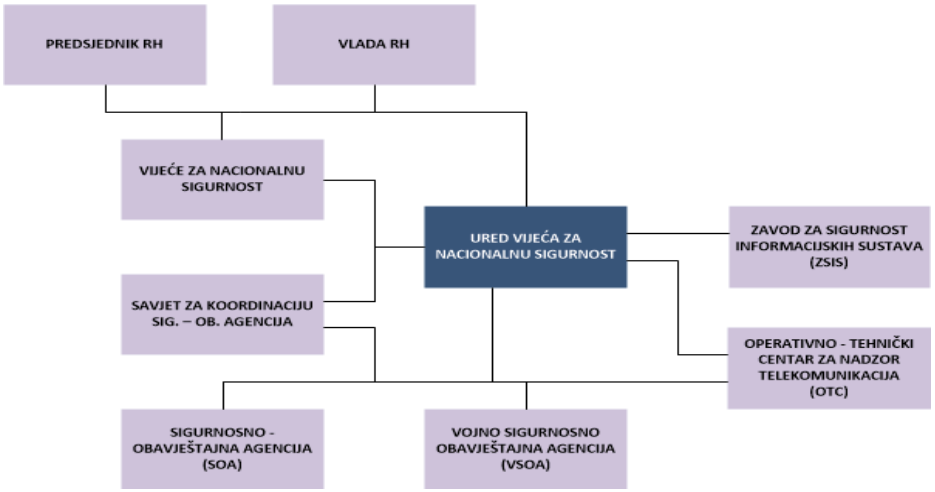
Osim poslova prevencije i odgovora na računalne ugroze informacijskih sustava, Zavod za sigurnost informacijskih sustava zadužen je za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima i njihovo trajno usklađivanje s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.

Djelokrug i zadaće Zavoda za sigurnost informacijskih sustava utvrđeni su Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakonom o informacijskoj sigurnosti te Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti (Zavod za sigurnost informacijskih sustava, 2007).

Ured Vijeća za nacionalnu sigurnost je središnje tijelo sustava domovinske sigurnosti. Pruža administrativnu potporu radu koordinacije za sustav domovinske sigurnosti, sudjeluje u izradi strateških dokumenata iz područja nacionalne sigurnosti i sustava domovinske sigurnosti, kao i u izradi procjene nacionalnih sigurnosnih rizika i određivanju prioriteta u njihovu tretiranju. Isto tako, Ured surađuje i daje potporu nadležnim državnim tijelima, osobito onima čije su obveze određene zakonom kojim se uređuje sigurnosna zaštita kritičnih infrastruktura.

Sastav Vijeća za nacionalnu sigurnost propisan je zakonom kojim se uređuje sigurnosno-obavještajni sustav Republike Hrvatske.

Vijeće za nacionalnu sigurnost razmatra i procjenjuje sigurnosne prijetnje i rizike, pitanja iz djelokruga središnjih tijela državne uprave i drugih državnih tijela koja se odnose na nacionalnu sigurnost te donosi smjernice, odluke i zaključke o načinima zaštite i ostvarivanja interesa nacionalne sigurnosti koji se odnose i na sustav domovinske sigurnosti (Ured Vijeća za nacionalnu sigurnost, 2017).



Slika 2 Ured Vijeća za nacionalnu sigurnost

Izvor: https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

Agencija za podršku informacijskim sustavima informacijskih tehnologijama (APIS IT) je institucija koja pruža strateške, stručne i provedbene usluge javnom sektoru Republike Hrvatske u planiranju, razvoju, podršci i održavanju poslovno-informacijskih sustava po principima umrežene i korisnički usmjerene uprave (Juran, 2014).

Agencija za zaštitu osobnih podataka je pravna osoba, koja samostalno izvršava poslove u nadležnosti Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/18). Tim se Zakonom osigurava provedba Uredbe EU-a 2016/679 Europskog parlamenta i Vijeća od 27.04.2016. o zaštiti pojedinca u vezi s obradom podataka.

Agencija djeluje samostalno i neovisno o izvršnoj i zakonodavnoj vlasti, a neovisnost propisuje Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija 10/ Vijeća Europe) i dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.

Središnji državni ured za e-Hrvatsku (od 2011 g. Ministarstvo uprave) je institucija čije se djelovanje odnosi na informatizaciju unutarnjeg poslovanja državne uprave, međusobnu komunikaciju i interoperabilnost tijela državne uprave elektroničkim putem i modernizaciju poslova javne uprave kroz usluge elektroničke

uprave, stručne poslove koji se odnose na planiranje, uvođenje i primjenu informacijsko-komunikacijske tehnologije.

Ured obavlja poslove koji se odnose na razvitak informacijskog sustava državne uprave, uspostavu tehnološke i sigurnosne informatičke infrastrukture u tijelima državne uprave, racionalizaciju uporabe informatičkih resursa u tijelima državne uprave, povezivanje informacijskih sustava tijela državne uprave kroz jedinstvenu informacijsko - komunikacijsku mrežu, praćenje i koordinaciju projekata iz područja informacijsko - komunikacijske tehnologije u tijelima državne uprave. Ured sudjeluje u donošenju i praćenju provedbe zakona i drugih propisa u području primjene informacijsko - komunikacijske tehnologije u tijelima državne uprave, prati i koordinira razvoj registarskih sustava državne uprave prati razvitak primjene informacijske i komunikacijske tehnologije u sustavima elektroničke uprave, te priprema i prati provedbe Strategije e-Hrvatska 2020 i pripadajućeg Akcijskog plana (Uprava za e-Hrvatsku, 2011).

3.3. Norme iz područja informacijske sigurnosti u RH

Uspostavljanjem sigurnosne politike organizacije uvode određene standarde vezane uz sigurnost informacijskih sustava. Uspostavljeni standardi osiguravaju pridavanje pažnje svim aspektima zaštite nekog informacijskog sustava te ujedno dokazuju kvalitetu uspostavljenih mjera sigurnosti.

Prema Nacionalnom CERT-u mjerodavne institucije za izdavanje ovakvih standarda u području zaštite informacijskih sustava su:

- ISO (International Organization for Standardization) i
- IEC (International Electrotechnical Commission).

Standardi iz ISO/IEC 27000 serije organizacijama pružaju smjernice za konstruiranje, primjenu i provjeru informacijskih sustava čime se osiguravaju aspekti zaštite informacijskog sustava: povjerljivost, integritet i dostupnost informacijskog sadržaja, sustava i procesa unutar organizacije.

Za područje sigurnosti informacijskih sustava najčešće se koriste dva standarda:

- ISO/IEC 27001[4] i
- ISO/IEC 27002[5] (prije 2007. godine poznat kao ISO/IEC 17799:2005).

Pri izradi sigurnosne politike preporuča se upotreba oba standarda.

ISO/IEC 27001 standard, punim imenom „ISO/IEC 27001:2005 Informacijske tehnologije - Tehničke zaštite - Specifikacije za sustav upravljanja informacijskim sustavima“ je standard izrađen 2005. godine, a nastao je na temelju standarda BS 7799 (British Standards).

ISO/IEC 27001 je službena skupina specifikacija na temelju kojih organizacije imaju pravo zatražiti postupak certifikacije, naravno ukoliko su primijenile taj standard na sustav upravljanja sigurnošću informacija. Ovaj standard propisuje zahtjeve za uspostavljanje, provođenje, nadgledanje, ispitivanje, održavanje i poboljšanje sustava za upravljanje sigurnošću informacija. Standard je primjenjiv na sve vrste organizacija (komercijalne, neprofitne, državne institucije, itd.) i sve veličine organizacija, od malih pa do velikih svjetskih organizacija (CARNet CERT, 2009).

Standard se sastoji od 5 dijelova:

1. Sustav za zaštitu informacija
2. Odgovornost rukovodećih ljudi
3. Unutarnje provjere sustava za zaštitu informacija
4. Provjera valjanosti sustava za zaštitu informacija
5. Poboljšanja na sustavu za zaštitu informacija

U standardu su također navedeni ciljevi provjere koje je potrebno ostvariti i provjere koje je potrebno provesti kako bi se ostvarili ti isti ciljevi. Certifikacija je stvar izbora organizacije, ali vrijedi spomenuti, da poslovni partneri ponekad traže da organizacija s kojom surađuju ima certifikat.

ISO/IEC 27002 standard također je nastao na temelju BS 7799 standarda. ISO/IEC 27001 standard definira koje zahtjeve neki sustav za zaštitu informacija mora imati, te za primjerene provjere navodi uporabu ISO/IEC 27002 standarda. ISO/IEC

[4] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[5] https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

27002 jest službeni standard, ali bolje ga je protumačiti kao skup smjernica koje je moguće upotrijebiti (CARNet CERT, 2009).

Carnetov CERT (2009) dijeli ISO/IEC 27002 standard na 12 dijelova:

1. *Procjena rizika* - organizacija mora na temelju zahtjeva odrediti koje su moguće prijetnje informacijskom sustavu.
2. *Sigurnosna politika* - rukovodeći ljudi organizacije bi trebali odrediti skup pravila i zahtjeva kako bi se stekla jasna vizija o dozvoljenim i nedozvoljenim radnjama.
3. *Organizacija informacijske sigurnosti* - rukovodeći ljudi organizacije bi trebali odrediti ljude odgovorne za provođenje primjerene zaštite informacija, kako zaštite od unutarnjih, tako i od vanjskih prijetnji.
4. *Upravljanje imovinom* - organizacija mora biti svjesna koliko su vrijedne informacije koje posjeduje, te znati njima ispravno raspolagati.
5. *Zaštita od zaposlenika* - organizacija mora postaviti i dodijeliti potrebnu razinu pristupa svakom zaposleniku, među zaposlenicima uspostaviti određenu razinu svijesti, te ih primjereno obrazovati.
6. *Fizička zaštita i zaštita od okoline* - vrijedna računalna oprema mora biti fizički zaštićena od zlonamjernih ili nenamjernih oštećenja i gubitaka.
7. *Upravljanje komunikacijama i operacijama* - uspostavljanje sigurnosnih provjera za sustave i mrežnu komunikaciju.
8. *Provjera pristupa* - pristup računalima, mreži i podacima mora biti pod nadzorom kako bi se spriječilo neovlašteno korištenje.
9. *Nabava, razvoj i održavanje informacijskih sustava* - potrebno je odrediti specifikacije opreme koju je potrebno nabaviti, smjer mogućeg razvoja informacijskog sustava, te primjeren način održavanja kako ne bi došlo do gubitka ili oštećenja.
10. *Upravljanje incidentima u informacijskom sustavu* - sigurnosne incidente koji su se dogodili potrebno je odmah prijaviti nadležnoj ustanovi, te voditi računa o upravljanju sustavom ukoliko se sigurnosni incident dogodi.
11. *Upravljanje poslovnim kontinuitetom* - potrebno je provesti analizu utjecaja informacijskog sustava na kontinuirano poslovanje organizacije kako bi se umanjila šteta nastala sigurnosnim incidentom.
12. *Usklađivanje* - informacijski sustav potrebno je uskladiti sa propisanim standardima i zakonima.

Svaki od dijelova sadrži određeni broj glavnih sigurnosnih kategorija, a pod sigurnosnim kategorijama navodi se cilj provjere koji je potrebno ostvariti i provjere koje je moguće primijeniti radi ostvarivanja cilja.

ISO/IEC 27002 sadrži prijedloge ustroja sustava za zaštitu informacija isto kao i sustava provjere. U standardu nije naglašeno koje specifične sigurnosne provjere je potrebno raditi, već samo kako sustav za upravljanje mora funkcionirati jer se od svake organizacije očekuje da provede detaljnu procjenu rizika kako bi se odredile specifične potrebe prije odabira sustava provjere a isto tako je nemoguće nabrojati sve moguće provjere u standardu za opću primjenu (Nacionalni CERT, Sigurnosna politika, 2016).

4. UTJECAJ UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU NA POSLOVNI KONTINUITET GRADA ROVINJA - ROVIGNO

„Na ekranu mi se pojavio natpis da moram platiti 2.000 Eura ako želim vidjeti moje dokumente.“

Ne radi server, ne možemo pokrenuti aplikaciju..

To su samo neki od slučajeva koji su noćna mora svakog informatičara zaduženog za održavanje i sigurnost sustava.

Prvi se odnosi na hakerski napad "*ransomwareom*" tj. "*CryptoLocker*"-om ili crvom koji kriptira datoteke određenog tipa npr. sve tekstualne datoteke (*.doc, *.docx, *.rtf, *.odt, *.txt), slikovne datoteke (*.jpg, *.png, *.eps, *.ai). Korisniku se prikazuje prijetnja da u roku od „x“ dana uplati određeni iznos u kriptovaluti (najčešće bitcoinu) ukoliko ne želi ostati bez podataka.

Drugi je posljedica neobjašnjivog kvara diskova na serveru. Iako je server bio u zaštitnom ormaru, iako se "*RAID*" controler i sam server kasnije ispostavio ispravnim, desilo se to da su oba diska na koje je implementirana tehnika zrcaljenja jednostavno „zaribala“, što je dovelo do potpunog gubitka svih podataka i samog operativnog sistema. Slijedio je mukotrpan noćni rad, kako bi se računalo i server vratili u prvobitno operativno stanje.

Ovi scenariji bi bili pogubni da nije bilo adekvatne sigurnosne kopije podataka kojim su se svi važni dokumenti povratili te se time omogućio kontinuitet poslovanja.

Primjena informacijskih sustava u poslovanju donosi brojne prednosti, ali ga isto tako izlaže potpuno novim opasnostima i neželjenim posljedicama. Rizici primjene informacijskih sustava se nikako ne smiju smatrati rizicima ili problemima koji nisu od velike važnosti za uspješnost poslovanja. Krive procjene tih rizika mogu određeni poslovni subjekt izložiti velikom financijskom gubitku i nenadoknadivoj šteti.

4.1. Grad Rovinj-Rovigno kao jedinica lokalne samouprave

Nakon uspostave samostalne Hrvatske, doneseni su odgovarajući zakoni o lokalnoj samoupravi, među kojima i Zakon o područjima županija, gradova i općina prema kojemu je definirano 419 općina, 70 gradova, 20 jedinica područne (regionalne) samouprave, odnosno županija i Grad Zagreb s položajem i ovlastima grada i županije.

U narednim godinama broj općina i gradova postupno se povećavao, te je na teritoriju Republike Hrvatske ustrojeno sveukupno 428 općina, 127 gradova u koji spada i Grad Rovinj - Rovigno.

Naziv grada, jedinice lokalne samouprave je GRAD ROVINJ-ROVIGNO - CITTÀ DI ROVINJ-ROVIGNO sa sjedištem u zgradi Vijećnice - Municipija na Matteottijevom trgu br. 2 u Rovinju. Grad Rovinj-Rovigno je jedinica lokalne samouprave u sastavu Istarske županije i Republike Hrvatske (Ministarstvo uprave, 2019).

Grad ima svojstvo pravne osobe. Statut Grada Rovinja-Rovigno, osnovni je akt usvojen i donesen na sjednici Gradskog vijeća 7. listopada 1993. godine, kojim se uređuju osnovna pitanja od značaja za grad Rovinj-Rovigno kao jedinice lokalne samouprave.

Prema strategiji razvoja grada za razdoblje 2015-2020 (2015), Grad Rovinj - Rovigno obavlja poslove lokalnog značaja kojima se neposredno ostvaruju potrebe građana, a koji nisu Ustavom ili zakonom dodijeljeni državnim tijelima i to osobito poslove koji se odnose na: uređenje naselja i stanovanje, prostorno i urbanističko planiranje, komunalne djelatnosti, brigu o djeci, socijalnu skrb, primarnu zdravstvenu zaštitu, odgoj i osnovno obrazovanje, kulturu, tjelesnu kulturu i šport, zaštitu potrošača, zaštitu i unapređenje prirodnog okoliša, protupožarnu i civilnu zaštitu, promet na svom području, te ostale poslove sukladno zakonima.

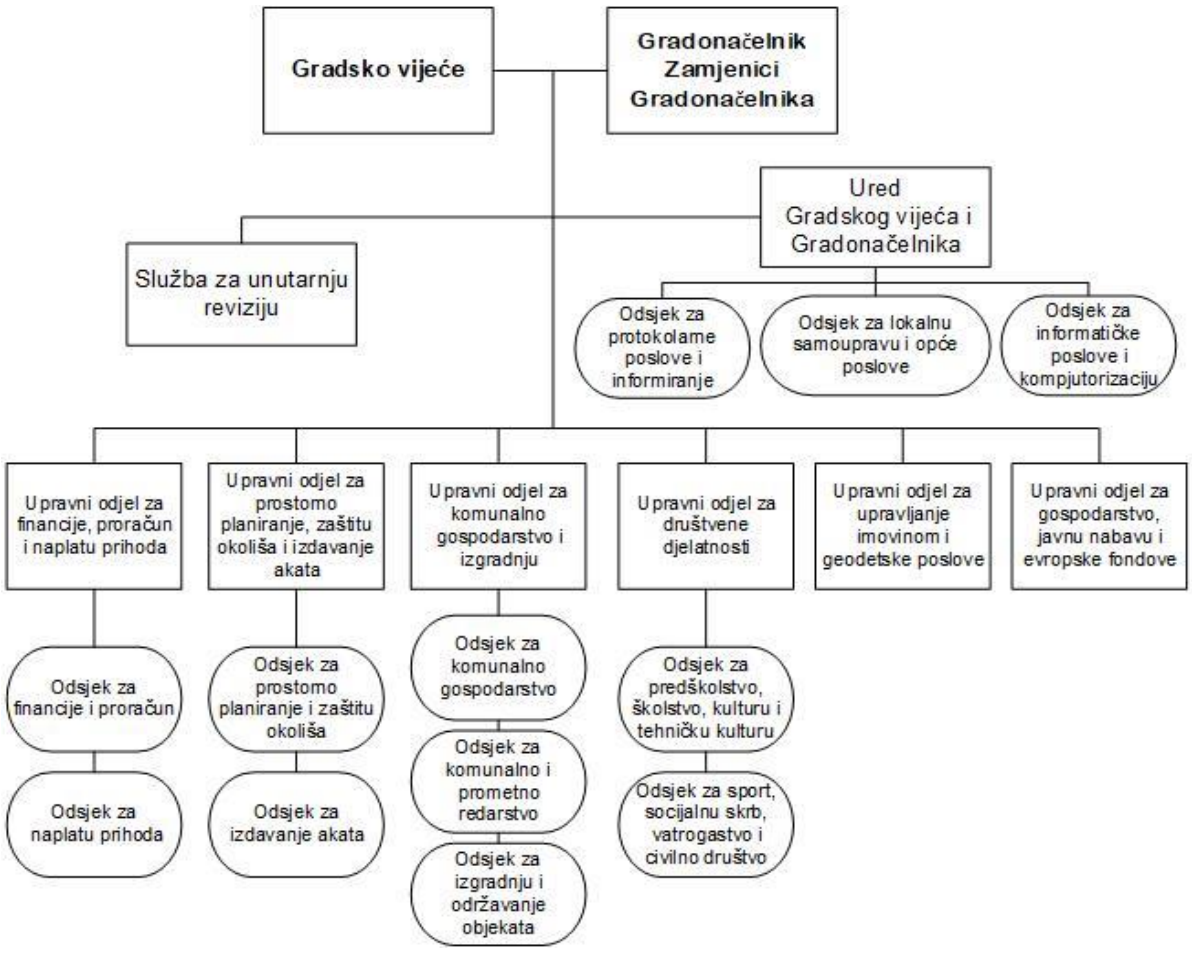
Gradska uprava Grada Rovinja-Rovigno opunomoćena od strane svih svojih građana da kontinuirano putem svojih aktivnosti i usluga unapređuje kvalitetu života i rada u gradu Rovinju svim svojim građanima putem pružanja izvrsne usluge, omogućavanjem participacije u odlučivanju, odgovornim upravljanjem javnim dobrima, protokom informacija te nadasve ljubaznim, efikasnim i transparentnim radom administracije, kako bi Rovinj kao mjesto življenja bio poželjan i siguran grad u kojemu je ugodno raditi i živjeti. Gradska uprava grada Rovinja-Rovigno nastoji uvijek biti u službi svih svojih građana (Gradska obilježja, 2020).

Izvršnu vlast u Gradu Rovinju-Rovigno obavlja gradonačelnik, koji ima svojeg zamjenika, i koji je ujedno pripadnik talijanske nacionalnosti.

Gradonačelnika i zamjenika biraju direktno birači, a mandat im traje 4 godine. Upravne i stručne poslove za potrebe gradonačelnika i Gradskog vijeća iz samoupravnog djelokruga rada, obavljaju gradske službe.

Odlukom o ustrojstvu i djelokrugu poslova ureda i upravnih tijela Grada Rovinja-Rovigno rad gradske uprave organiziran je po sljedećim uredima i službama: (Organizacija gradske uprave, 2020).

- Ured Gradskog vijeća i gradonačelnika;
- Upravni odjel za financije, proračun i naplatu prihoda;
- Upravni odjel za prostorno planiranje, zaštitu okoliša i izdavanje akata;
- Upravni odjel za upravljanje imovinom i geodetske poslove;
- Upravni odjel za društvene djelatnosti;
- Upravni odjel za komunalno gospodarstvo i izgradnju;
- Upravni odjel za gospodarstvo, javnu nabavu i europske fondove.



Slika 2.: Shema gradske uprave Grada Rovinja - Rovigno

Izvor: izradio autor

Gradsko vijeće je predstavničko tijelo građana i tijelo lokalne samouprave koje u okviru svojih prava i dužnosti donosi opće akte propisano zakonom i Statutom grada. Gradsko vijeće broji 15 vijećnika čija je funkcija počasna, mandat vijećnika traje 4 godine, a čiji mandat nije obvezujući i nije opozivi (Gradsko vijeće Grada Rovinja-Rovigno, 2020).

Ured Gradskog vijeća i gradonačelnika obuhvaća sljedeće aktivnosti:

- stručne, pravne, protokolarne, savjetodavne i administrativno-tehničke poslove za potrebe gradonačelnika, Gradskog vijeća, radnih tijela, klubova vijećnika;
- sazivanje i organiziranje sjednica Gradskog vijeća, radnih tijela, kao i izrada zapisnika i čuvanje istih;
- izrada potrebnih nacrta propisa i akata u kojima raspravlja i odlučuje Gradsko vijeće;
- izrada nacrta rješenja i zaključaka koje donosi Gradsko vijeće i njegova radna tijela;
- poslove vezane za informiranje i promidžbu grada, organiziranje tiskovnih konferencija gradonačelnika i drugih dužnosnika grada, priprema priopćenja i izvješća za medije;
- briga o stvaranju afirmativne slike grada, te o akcijama koje grad promiče u kulturnom, turističkom i gospodarskom smislu;
- prikupljanje informacija o gradu i članaka iz tiska;
- poslove vezane za međunarodnu i međugradsku suradnju sa zbratimljenim gradovima i općinama, regijama u Hrvatskoj i inozemstvu;
- pružanje stručne pomoći vijećnicima u izvršavanju njihovih prava i dužnosti, te informiranje istih o pitanjima od značaja za ostvarivanje njihove uloge;
- suradnja i koordinacija sa upravnim odjelima radi pripreme materijala za Gradsko vijeće;
- koordinacija sa upravnim odjelima radi izvršavanja programa i pojedinih zadaća, te radi izrade potrebitih izvješća za gradonačelnika, Gradsko vijeće i druga tijela;
- poslove u vezi s prijemima, upitima i predstavkama građana, te davanje odgovora na iste, davanje informacija o nadležnostima iz djelokruga rada upravnih odjela i ostalih organa i organizacija na području grada;
- prevođenje materijala za službene potrebe grada;
- provođenja informatizacije i izrade Službenog glasnika Grada Rovinja-Rovigno;

- poslove pisarnice i arhive, poslove u svezi radnih odnosa djelatnika gradskih upravnih odjela te prava i obveza lokalnih dužnosnika, kartoteke zaposlenih u upravnim odjelima, portirske službe, nabavke uredskog i ostalog potrošnog materijala te održavanja i čišćenja prostorija te
- te obavljanje drugih srodnih poslova iz ove oblasti i poslova koji su Uredu stavljeni u nadležnost zakonom, pod zakonskim aktima te odlukama gradonačelnika ili Gradskog vijeća.

Unutar Ureda odjela ustrojavaju se odsjeci, kao unutarnje ustrojstvene jedinice i to:

- Odsjek za protokolarne poslove i informiranje,
- Odsjek za lokalnu samoupravu i opće poslove i
- Odsjek za informatičke poslove i kompjutorizaciju obavlja sve poslove vezane uz informatizaciju gradske uprave na način da bude servis informatičkih usluga i tehničko-tehnološke potpore, te organizira bolje informatičko funkcioniranje svih organizacijskih jedinica Gradske uprave. Odsjek sudjeluje i u informatizaciji komunalnih i trgovačkih društava, kao i ustanova kojima je Grad osnivač i vlasnik, u smislu stvaranja integriranog informatičkoga sustava Grada. Odsjek također obavlja poslove planiranja, projektiranja, izgradnje i uspostavljanja informacijskih sustava, geo-informacijskog (GIS) sustava, integracije alfanumeričkih i grafičkih podataka, WEB Portala Grada te sustava on-line usluga. Također se obavljaju poslovi planiranja, nabave i upravljanja informatičko komunikacijske opreme, nadzora nad radom mreže (intranet i internet), osiguravanje sigurnosti i zaštite podataka, te svi drugi srodni poslovi. (Ured Gradskog vijeća i gradonačelnika, 2020).

Slijedom navedenog vidimo da je upravo odsjek za informatičke poslove i kompjutorizaciju zadužen za informacijsku sigurnost grada Rovinja – Rovigno.

Upravni odjel za financije, proračun i naplatu prihoda obavlja poslove određene zakonom, Odlukom o ustrojstvu i djelokrugu poslova ureda i upravnih tijela Grada Rovinja-Rovigno („Službeni glasnik Grada Rovinja-Rovigno“ broj 7/10 i 7/17) i drugim propisima, kao i poslove po nalogu Gradskog vijeća i Gradonačelnika.

Unutar Upravnog odjela ustrojavaju se odsjeci, kao unutarnje ustrojstvene jedinice:

- Odsjek za financije i proračun i
- Odsjek za naplatu prihoda (Upravni odjel za Proračun, gospodarstvo i evropske fondove, 2020).

Upravni odjel za prostorno planiranje, zaštitu okoliša i izdavanje akata obavlja stručne poslove vođenja i pripreme na izradi strateških i provedbenih dokumenata prostornog uređenja u skladu sa Zakonom o prostornom uređenju i gradnji, sl., izdavanje dozvola, obavljanje drugih srodnih poslova iz ove oblasti i poslova koji su upravnom odjelu stavljeni u nadležnost zakonom, pod zakonskim aktima te odlukama gradonačelnika ili gradskog vijeća.

Unutar Odjela ustrojavaju se odsjeci, kao unutarnje ustrojstvene jedinice:

- Odsjek za prostorno planiranje i zaštitu okoliša i
- Odsjek za izdavanje akata (Upravni odjel za prostorno planiranje, zaštitu okoliša i izdavanje akata, 2020).

Upravni odjel za upravljanje imovinom i geodetske poslove obavlja poslove predlaganja mjera za upravljanje i raspolaganje građevinskim zemljištem, općih uvjeta za raspisivanje natječaja za prodaju i davanje u zakup i obavljanje drugih poslova u svezi s građevinskim zemljištem, poslovi u svezi turističkog i ostalog građevinskog zemljišta, vođenje evidencije o građevinskom zemljištu u vlasništvu grada, upravljanje stambenim i poslovnim objektima u vlasništvu grada, izrada kriterija i mjerila za korištenje i namjenu poslovnih prostora, davanje koncesija i koncesijskih odobrenja na pomorskom dobru, priprema i obavljanje svih poslova vezanih za provođenje javnih poziva za prodaju ili davanje u zakup poljoprivrednog zemljišta, obavljanje geodetskih poslova za potrebe gradske uprave, priprema i vođenje sudskih i upravnih postupaka u svezi gradske imovine, obavljanje drugih srodnih poslova iz ove oblasti i poslova koji su upravnom odjelu stavljeni u nadležnost zakonom, pod zakonskim aktima te odlukama gradonačelnika ili Gradskog vijeća (Upravni odjel za upravljanje imovinom i geodetske poslove, 2020).

Upravni odjel za društvene djelatnosti obavlja poslove određene zakonom, Odlukom o ustrojstvu i djelokrugu poslova ureda i upravnih tijela Grada Rovinja-Rovigno

(„Službeni glasnik grada Rovinja“ broj 7/10) i drugim propisima, kao i poslove po nalogu Gradskog vijeća i gradonačelnika (Upravni odjel za društvene djelatnosti, 2020).

Unutar Upravnog odjela ustrojavaju se odsjeci, kao unutarnje ustrojstvene jedinice:

- Odsjek za pred školstvo, školstvo, kulturu i tehničku kulturu i
- Odsjek za sport, socijalnu skrb, vatrogastvo i civilno društvo.

Upravni odjel za komunalno gospodarstvo i izgradnju obavlja poslove određene zakonom, Odlukom o ustrojstvu i djelokrugu poslova ureda i upravnih tijela Grada Rovinja-Rovigno („Službeni glasnik Grada Rovinja – Rovigno“ broj 7/10 i 7/17) i drugim propisima, kao i poslove po nalogu Gradskog vijeća i Gradonačelnika.

Unutar Upravnog odjela ustrojavaju se odsjeci, kao unutarnje ustrojstvene jedinice:

- Odsjek za komunalno gospodarstvo,
- Odsjek za komunalno i prometno redarstvo i
- Odsjek za izgradnju i održavanje objekata. (Upravni odjel za komunalno gospodarstvo i izgradnju, 2020).

Upravni odjel za gospodarstvo, javnu nabavu i europske fondove obavlja poslove predlaganje i izrada elaborata i razvojnih programa, praćenje rada i razvoj poduzetničkog inkubatora, provođenje postupaka javne nabave za potrebe Grada Rovinja-Rovigno, odnosno gradskih upravnih tijela, provođenje projekata financiranih od strane EU, obavljanje drugih poslova koji su upravnom odjelu stavljeni u nadležnost zakonom, pod zakonskim aktima te odlukama gradonačelnika li gradskog vijeća (Upravni odjel za gospodarstvo, javnu nabavu i europske fondove, 2020).

Grad Rovinj obavlja ulogu predstavnika i zaštitnika interesa lokalnog stanovništva (politička dimenzija), te ulogu nositelja/ pružatelja mnogih javnih poslova, od kojih su najvažnije lokalne komunalne službe.

Iz svega navedenog može se zaključiti da Grad Rovinj – Rovigno obavlja poslove od lokalnog značaja kojima se ostvaruju potrebe građana.

Upravljanje i dijeljenje podataka i informacija među odjelima i djelatnicima unutar Grada Rovinja-Rovigno omogućuje se korištenjem informatičke tehnologije i mrežnih alata.

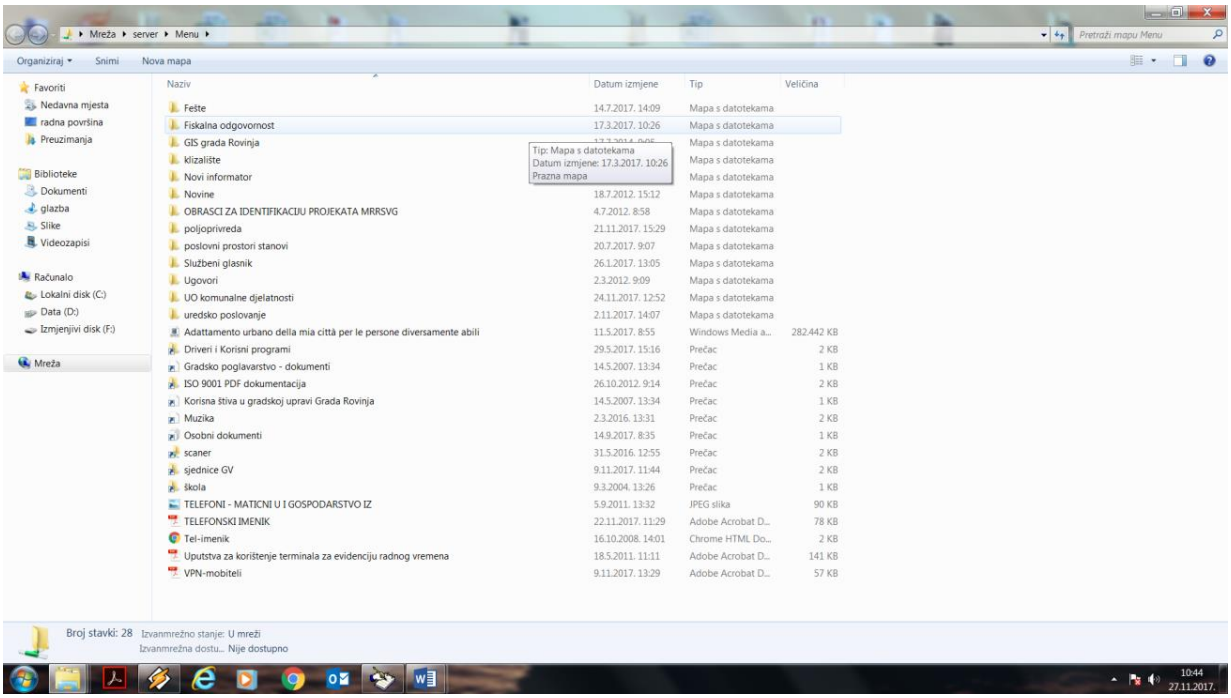
Korištenjem informatičke tehnologije i mrežnih alata omogućuje se komunikacija, suradnja i dijeljenje informacija unutar samog poslovnog subjekta ili između više poslovnih subjekata što omogućuje konkurentsku prednost, produktivnost i brzinu, a samim time i smanjenje troškova. Svaki zaposlenik u gradskoj upravi je svojim računalom, tabletom ili mobitelom spojen na lokalnu mrežu (LAN) koja je vatrozidom dalje spojena na internet. Uspostavljena je zajednička baza ključnih dokumenata i propisa, a klasificiranim se podatcima omogućuje svakom djelatniku uvid u bazu, dijeljenje i preuzimanje sadržaja i pronalazak podataka i informacija u bilo koje vrijeme s obzirom na njegove ovlasti i prava.

Upravljanje podacima i informacijama u Gradu Rovinju - Rovigno odvija se slijedećim načinima:

- kroz gradski portal na lokalnoj mreži Grada Rovinja – Rovigno i web portal Grada Rovinja - Rovigno
- elektroničkom poštom,
- Task Track-om (program za internu komunikaciju) te
- Web GIS portalom Grada Rovinja-Rovigno

Gradski portal Grada Rovinja – Rovigno se nalazi na serveru gradske uprave, sadrži razna izvješća, zakonsku regulativu, sve službene glasnike Grada Rovinja-Rovigno, ugovore, dokumente Ureda Gradonačelnika. Svaki djelatnik gradske uprave ovisno o radnom mjestu odnosno upravnom odjelu u kojem je zaposlen može pristupiti izvještajima relevantnima za njegovo radno mjesto, te isto tako šifriranim pristupom pohranjivati i dijeliti dokumente koji su važni za njegov odjel ili radni tim.

Slika ispod prikazuje gradski portal na lokalnoj mreži

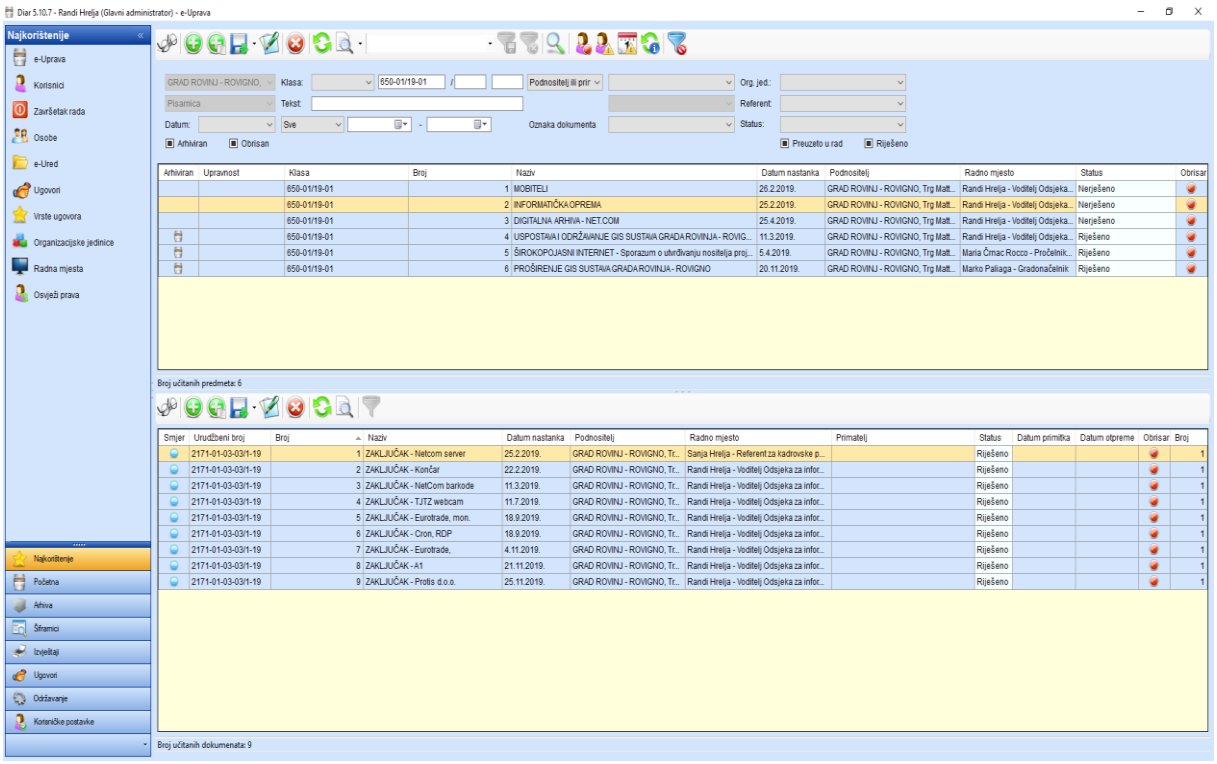


Slika 3 Gradski portal na lokalnoj mreži Grada Rovinja – Rovigno

Izvor: Screenshot – Gradski portal, \\server\menu

Isto tako se putem prečaca pristupa aplikaciji za „Digitalnu arhivu sa djelovodnikom“, čiji screenshot prikazuje slika 4, koja olakšava i ubrzava uredsko poslovanje i kolanje dokumenata. Aplikacija omogućava ubrzano evidentiranje predmeta na mjestu prijema uz mogućnost unosa multimedijalnih priloga. Omogućuje povezanost djelovodnika i arhive, trenutan pristup informacijama uz istovremeni rad više osoba na jednom predmetu. Aplikacijom se efikasno prati status svakog predmeta i kontrolira njihovo rješavanje, omogućuje se brzo pretraživanje dokumenata, štampanje evidencija i statističkih izvješća.

Komunikacija između odjela time postaje efikasnija, a sigurnost uz kontrolu pristupa veća. Na taj način se povećava produktivnost i vrši velika ušteda vremena, novaca čime se podiže razina pružanja usluga građanima. Poseban naglasak je na njenoj jednostavnosti i ergonomiji tako da se operativno ne razlikuje od klasičnog, pisanog načina vođenja arhive s djelovodnikom.



Slika 4 Digitalna arhiva s djelovodnikom

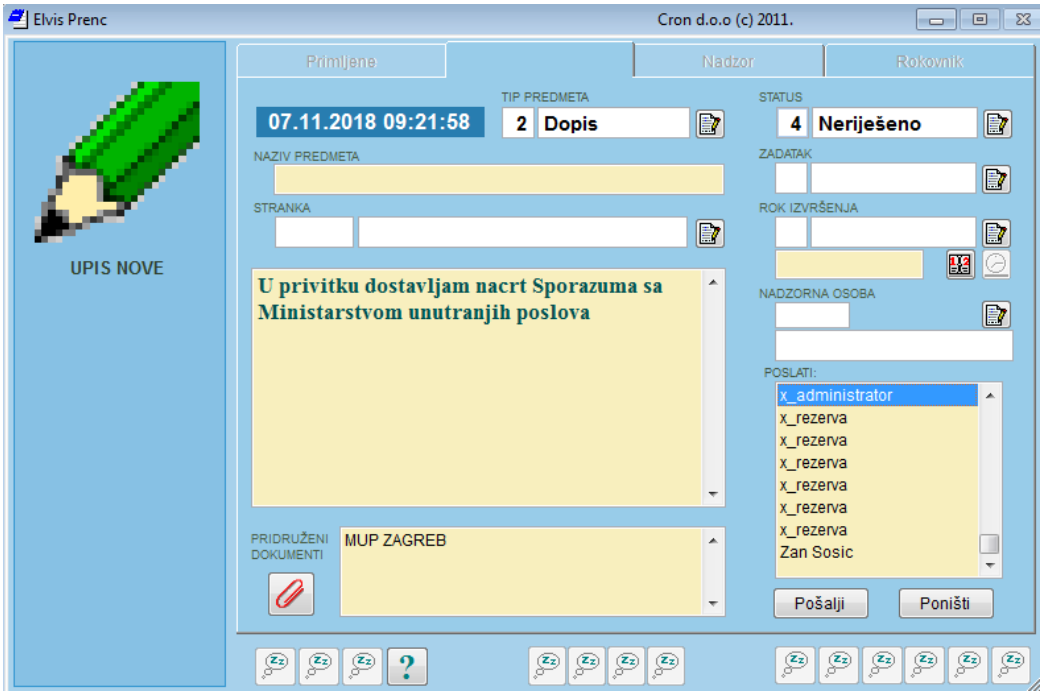
Izvor: Screenshot – Digitalna arhiva sa djelovodnikom

Elektronička pošta je jedan od glavnih načina komunikacije djelatnika gradske uprave sa vanjskim subjektima, a sve više služi i za internu komunikaciju te razmjenu dokumenata među samim djelatnicima. Microsoft Outlook kao mail klijent je sastavni dio Microsoftovog office paketa te se uz osnovnu namjenu slanja elektroničke pošte koristi i kao kalendar i organizator obveza. U današnje vrijeme elektronske komunikacije je vrlo bitno da je korisniku sva elektronička pošta dostupna u svakom trenutku, bilo putem računala ili putem mobitela stoga je baza elektroničke pošte pohranjena na Exchange serveru koji garantira visoki stupanj pouzdanosti.

TaskTrack , slika 5 i slika 6 ispod, je aplikacija namijenjena međusobnoj komunikaciji između djelatnika. Osim interne komunikacije omogućuje razmjenu datoteka, praćenje izvršavanja radnih naloga, slanje radnih materijala te praćenje svih informacija i podataka prilikom obavljanja radnih zadataka. Pokreće se automatski pri startu operativnog sistema računala, a od svakog korisnika se za pokretanje aplikacije zahtijeva upis personalne lozinke čime se otvara aplikacija.

Slika 5 Početna stranica za prijavu aplikacije TaskTrack

Izvor: Screenshot – TaskTrack prijava, \\servergis\razno\notes\tasktrak.exe

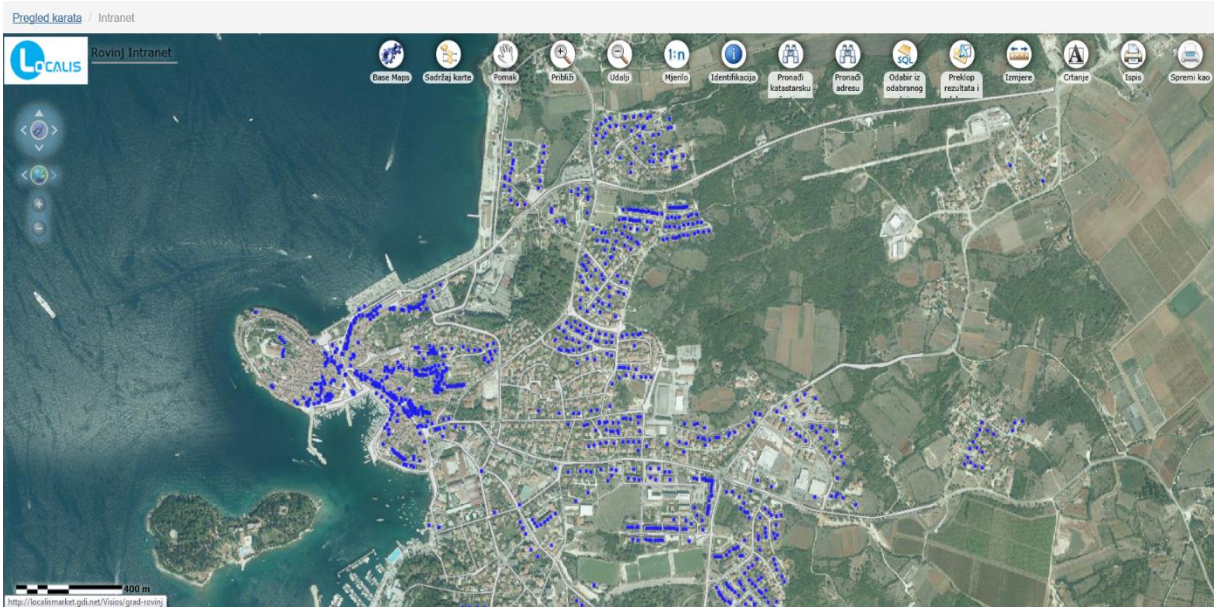


Slika 6 TaskTrack aplikacija

Izvor: Screenshot – TaskTrack aplikacija, \\servergis\razno\notes\tasktrak.exe

Cjelokupnu prostornu infrastrukturu, od baza podataka, do računalnih rješenja Grad Rovinj-Rovigno ima na GDi Cloud platformi. Tu infrastrukturu Grad Rovinj temelji na IaaS („Infrastructure as a Service“, tj. infrastrukture kao servisa). GDi CLOUD računalna usluga omogućuje uz brzi internet dostupnost svih hardverskih i softverskih komponenti potrebnih za nesmetano, kontinuirano funkcioniranje sustava.

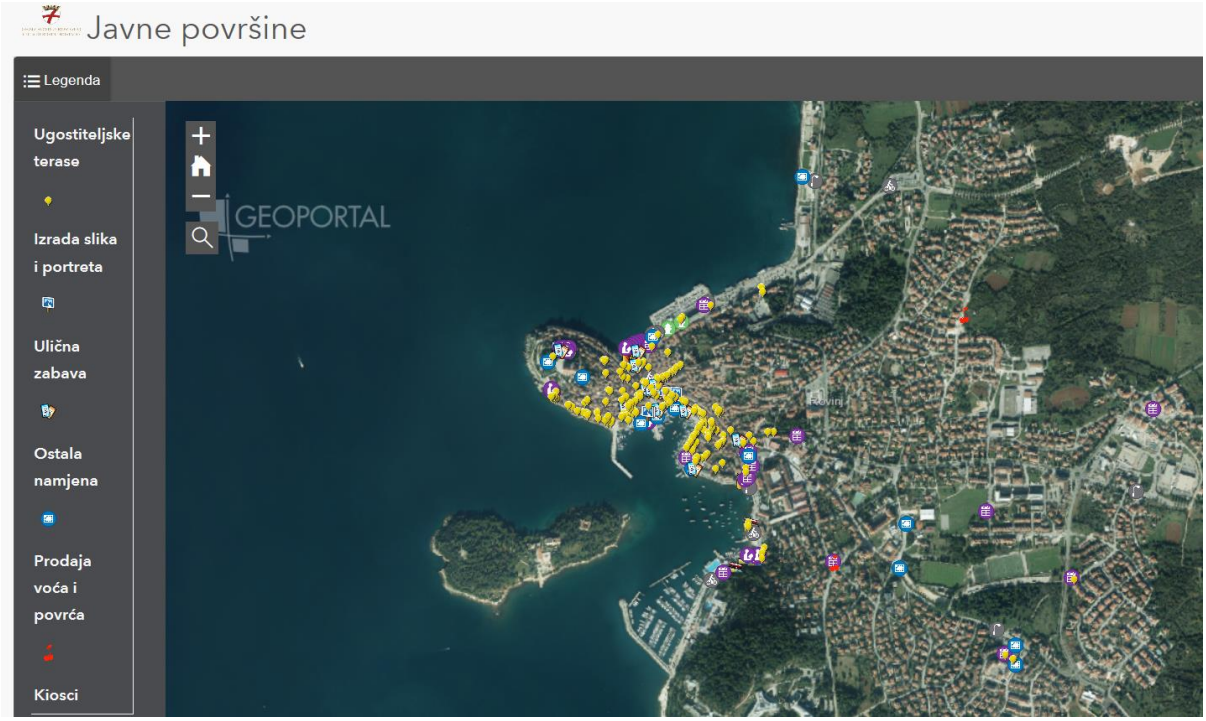
WEB GIS Sustav[6] je osmišljen na način da je Grad nositelj sustava, koji ima pravo održavanja i ažuriranja sustava i podataka koji iz njega nastaju za svoje poslovne procese, dok svi korisnici sustava imaju pravo neograničenog korištenja sustava u pregledu i analizama. Sustav sadrži skupne obrađene podatke od službenih podloga državne geodetske uprave i digitalnog katastara do topološki obrađenih podataka kao što su adresni model ulica i kućnih brojeva i sustava javne rasvjete, kao što je prikazano na slici 7 i 8 dolje. Nadalje, GIS mrežna usluga sadrži ažurirane podatke o nerazvrstanim cestama, bazu imovine poljoprivrednog zemljišta kao i kompletnu bazu javnih površina i nekretnina u vlasništvu Grada Rovinja-Rovigno. Sustav također sadrži rasterske podloge generalno urbanističkog plana Grada i zasebne cjeline naselja Rovinjsko Selo, te ostale prostorne planove svih razina koji se odnose na teritorij jedinice lokalne samouprave Grada Rovinja-Rovigno.



Slika 7 Web GIS Portal Grada Rovinja - Rovigno

Izvor: Screenshot – web GIS Portal Grada

[6] Aplikacija se nalazi na http://localismarket.gdi.net/Visios/grad-rovinj/Intranet



Slika 8 Prikaz izgleda Web GIS Portala Grada Rovinja-Rovigno iz domene podataka o korištenju javnih površina na užem području grada

Izvor: Screenshot – web GIS Portal Grada

Takav način komuniciranja i korištenja informacijske tehnologije uvelike doprinosi ubrzanju operativnih procesa i optimizaciji troškova.

4.2. Pojam kontinuiteta poslovanja

Kontinuitet poslovanja je “strateška i taktička sposobnost organizacije da planira i odgovori na incidente i prekide u poslovanju, kako bi nastavila s poslovnim aktivnostima na nivou koji je prethodno definirala kao prihvatljiv“ (Košutić, 2010).

Osnovna ideja kontinuiteta poslovanja zapravo je zaštititi informacije u slučaju neke veće i neočekivane nezgode (dakle, osigurati dostupnost informacija). Upravljanje kontinuitetom poslovanja predviđa pisanje planova koji određuju na koji način je potrebno postupiti u izvanrednim situacijama (priprema rezervne lokacije, određivanje vremena oporavka, priprema komunikacije u slučaju krize i sl.).

Plan kontinuiteta poslovanja mora se sastojati od: (CERT, Upravljanje kontinuitetom poslovnih procesa, 2010)

1) plana odaziva na incident i

2) plana oporavka

Plan odaziva na incident obično je jedinstven plan koji se odnosi na cijelu organizaciju i opisuje radnje koje se moraju poduzeti odmah nakon pojave havarije – smanjenje posljedica incidenta, komunikacija sa službama za hitne slučajeve, evakuacija zgrade, okupljanje na zbornim mjestima, organizacija transporta na rezervnu lokaciju i sl.

Plan oporavka se obično piše zasebno za svaku kritičnu aktivnost i mora obuhvaćati sljedeće korake (Vukelić, 2016):

- vrijeme i način na koji se komunicira s raznim zainteresiranim stranama (zaposlenicima, dioničarima, klijentima, partnerima, državnim službama, javnim medijima i dr.),
- princip sastavljanja tima,
- provođenje oporavka infrastrukture,
- provjera funkcionalnosti aplikacija i kontrole pristupa,
- provjerava podataka koji nedostaju i utvrđivanje svega što je oštećeno u havariji,
- oporavak podataka i uspostava normalnih aktivnosti.

Neadekvatno planiranje kontinuiteta poslovanja može prouzročiti (Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, 2006):

- gubitak raspoloživosti,
- gubitak reputacije,
- gubitak konkurentskih prednosti,
- gubitak podataka,
- gubitak produktivnosti,
- povećanje operativni troškova,
- povredu ugovornih odnosa,
- povredu važeći propisa,
- financijski gubitak.

4.3. Veza između kontinuiteta poslovnih procesa i informacijske sigurnosti

Na prvi pogled reklo bi se da kontinuitet poslovanja i informacijska sigurnost nemaju zajedničkih veza. No, iz dubljeg promatranja njihove povezanosti proizlazi zaključak da postoje velike poveznice. Naime, informacijska sigurnost se brine o povjerljivosti, integritetu i dostupnosti (raspoloživosti) informacija, dok se kontinuitet poslovanja u prvom redu brine da informacije budu dostupne onima koji ih trebaju.

Suština kontinuiteta poslovanja jest da osigurava kontinuitet ključnih poslovnih procesa u nekoj organizaciji. Kako se svaki poslovni proces bazira na protoku informacija, tako je fokus kontinuiteta poslovanja na dostupnosti, odnosno očuvanju i oporavku vitalnih poslovnih informacija. Sličnosti postoje i u nekim provedbenim dokumentima. Na primjer, svaka metodologija za kontinuitet poslovanja propisuje potrebu procjene rizika, koja se provodi na isti način kao i procjena rizika za informacijsku sigurnost. Dakle, dio dokumentacije će biti zajednički i za kontinuitet poslovanja i informacijsku sigurnost (CERT, Upravljanje kontinuitetom poslovnih procesa, 2010).

4.4. Odgovor na sigurnosne incidente i mjere zaštite informacijskih resursa u Gradu Rovinju- Rovigno

Kao odgovor na sigurnosne incidente gradonačelnik Grada Rovinj-Rovigno je u „Priručniku upravljanja kvalitetom prema ISO 9001“ iz 2018, čiji je referentni dokument Sigurnost informacijskog sustava grada Rovinja-Rovigno, propisao niz mjera, pravila rada i postupanja kojih su se svi zaposlenici dužni pridržavati. Isto tako je za provedbu istih imenovana stručna osoba, voditelj sigurnosti (voditelj odsjeka za informatičke poslove i kompjutorizaciju), koja će voditi brigu o upravljanju, podjeli zaduženja i samom obrazovanju korisnika. Voditelj sigurnosti brine o ukupnoj sigurnosti informacijskog sustava u što je uključena osobna sigurnost, fizička sigurnost, kontrola pristupa, razvoj i održavanje te usklađenost sa zakonskim propisima.

Voditelj odsjeka za informatičke poslove i kompjutorizaciju ima glavnu ulogu vezanu za sigurnost, ispravan rad računala, servera i mrežne opreme. Odgovoran je za:

- nadziranje rada mreže i servisa,

- izradu sigurnosnih kopija na serverima te kontrolu i ispravnost istih,
- dodjeljuje korisnicima dozvole za pristup podacima i poduzima mjere za sprječavanje izmjene podataka od neautoriziranih osoba,
- kontaktira i ugovara proizvođače vanjskih aplikacija i dogovara isporuku novih verzija,
- brine o instalaciji i ispravnom radu antivirusnog programa kao i o konfiguraciji vatrozida koji služi za zaštitu informacijsko komunikacijskog sustava i računala, prema određenim pravilima, od neautorizirane uporabe,
- vrši nabavku računala i aplikacija te instalaciju istih na korisničkom mjestu,
- sudjeluje u razvoju aplikacija, kako bi osigurao da se poštuju pravila iz sigurnosne politike,
- prijavljuje i dokumentira incidente ili pokušaje iznude CERT-u ili MUP-u u svrhu nastojanja da se izbjegnu slične situacije u budućnosti.

Korisnici su osobe koje se u svom radu služe računalima, proizvode dokumente ili unose podatke. Svaki korisnik je upoznat sa pravima i dužnostima i ulogom u poboljšanju sigurnosti sustava. Oni nisu odgovorni za instalaciju i konfiguraciju aplikacija, niti za ispravan i neprekidan rad računala i mreže, za što je zadužen i o tome vodi brigu, voditelj odsjeka za informatičke poslove i kompjutorizaciju. Voditelj vrši upoznavanje neposredno (usmeno, pisano) te putem pisanih obavijesti, elektroničkom poštom, pravilima vidljivim na stranicama korisničke podrške (Intranet).

Pravila nalažu da korisnici ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim normama i pravilima, moraju prijavljivati sigurnosne incidente i bilo kakve nepravilnosti u radu računala, kako bi se isti što prije i bezbolnije riješili.

Vanjske tvrtke se smatraju onima kojima se mora dopustiti pristup opremi, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja itd. Ukoliko se vanjskoj pravnoj osobi prepušta održavanje opreme i aplikacija s povjerljivim podacima, Grad Rovinj-Rovigno sa tom pravnom osobom potpisuje „Sporazum o povjerljivosti i tajnosti podataka“.

Sporazum o povjerljivosti i tajnosti podataka je pravno obvezujući dokument za utvrđivanje uvjeta pod kojima jedna strana (pružatelj informacije) u povjerenju otkriva informacije drugoj osobi (primatelj informacije).

Za fizičku sigurnost opreme odgovoran je gradonačelnik Grada Rovinja-Rovigno, međutim, ta se odgovornost može prenijeti na druge zaposlenike, koji pri tome potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Grad Rovinj-Rovigno ima razrađene procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme (Pravilnik o korištenju inf. opreme u vlasništvu Grada Rovinja-Rovigno). Svaka stavka informatičke opreme ima svoj inventarni broj sa pozicijom koju korisnik zadužuje do njene zamjene, a koja je zavedena u popisu dugotrajne imovine Grada. U slučaju nabavke nove ili dodatne opreme gradonačelnik potpisuje zaključak kojim se odobrava nabavka iste i bez kojeg odjel za Financije, proračun i naplatu prihoda ne može izvršiti plaćanje dobavljaču. Isto tako se prilikom zaduženja prijenosnog računala, mobilnog uređaja ili dlanovnika potpisuje „Izjava o preuzimanju“ koja je ujedno i dokument koji se na porti kontrolira od strane djelatnika zaštitarske službe, a sve u svrhu zaštite imovine od otuđenja.

Portir, odnosno djelatnik zaštitarske službe provjerava da li oprema koja se iznosi ima potrebne prateće dokumente (izjave o preuzimanju, radne naloge za popravak itd.).

Nadzor nad informacijskim sustavom Grada Rovinja-Rovigno smiju obavljati samo osobe koje je gradonačelnik za to ovlastio, poštujući pri tome privatnost i osobnost korisnika i njihovih podataka.

Grad Rovinj-Rovigno zadržava pravo nadzora nad instaliranim aplikacijama i podacima koji su pohranjeni na umreženim računalima, te nad načinom korištenja računala.

Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa,
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident, te
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

U svrhu što uspješnije provedbe sigurnosne politike Grad Rovinj-Rovigno:

- ima postojeći popis računala, pisača i drugih informatičkih uređaja,

- ima postojeću skicu mreže sa ažuriranim novim priključcima,
- ima sve mrežne priključke numerirane na razumljiv i jedinstven način, tako da se svaki priključak može brzo pronaći,
- godišnje radi inventuru kompletne računalne opreme, uključujući mrežne i komunikacijske uređaje,
- ima evidenciju svakog računala, koji se operacijski sustav na njemu koristi, te popisane aplikacije koje su na njemu instalirane,
- ima ažurirani popis softvera koji se koristi na računalima i serverima Grada Rovinj-Rovigno, kako bi se moglo lakše brinuti o licenciranju.

4.5. Oporavak od havarije

Kako bi se u slučaju nezgoda (poput kvarova na sklopovlju, požara, ili ljudskih grešaka) podaci sačuvali, potrebno je redovito izrađivati sigurnosne kopije svih vrijednih informacija, uključujući i konfiguraciju aplikacija. Preporučuje se izraditi više kopija i čuvati ih na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Grad Rovinju-Rovigno je Općim procedurama sustava upravljanja kvalitetom koje su u primjeni od 2015. g. propisao „P-XVII proceduru o načinu izrade sigurnosne kopije dokumenata na serverima“ (backup). Ona se nalazi na serveru među ISO9001 procedurama i dokumentima, a nadležnost i provođenje vrši voditelj odsjeka za informatičke poslove i kompjutorizaciju. Procedura nalaže da se čuvanje sigurnosnih kopija servera (backup servera) vrši u posebnoj prostoriji koja je fizički osigurana tako što je ulaz omogućen samo osoblju sa magnetnom karticom i koja je pod video nadzorom, a sve kako bi se spriječilo otuđenje ili zloupotreba, te kako bi se sačuvala povjerljivost informacija.

Serverima se prema proceduri dnevno, na kraju radnog dana, izrađuje sigurnosna kopija koje se pohranjuju na mrežne diskove *"NAS"* (Network Attached Storage). To su uređaji velikih diskovnih kapaciteta, koji su smješteni jedan u istoj zgadi, a drugi u zgradi koja je na drugoj lokaciji. Pristup mrežnim diskovima zaštićen je lozinkom, koja je pohranjena u vatrootpornom ormaru server sobe. Mrežni diskovi su konfigurirani tako da su diskovi povezani u "*RAID*" (Redundant Array of Independent Disks – polje redundantnih nezavisnih diskova), koje osim veće brzine zapisa i čitanja podataka sa njih, ima svojstvo veće tolerancije na greške u slučaju kvara jednog od

diska, čime se povećava sigurnost izrade i dostupnosti sigurnosne kopije. Procedura također nalaže da se sigurnosna kopija servera za „Financije i knjigovodstvo“, na kojem se obrađuju sve važne financijske transakcije Grada, te na kojem su implementirane aplikacija za plaće, materijalno knjigovodstvo, naplatu komunalnog prihoda i dr. putem VPN veze dodatno dnevno šalje na udaljeni server Cron-a d.o.o., čije su i aplikacije.

Radi osiguranja kontinuiteta poslovanja, svi važni dokumenti vezani za sigurnost informacijskog sustava, kao što su procedure o načinu izrade i vraćanja sigurnosnih kopija, aplikacijske lozinke korisnika te svih servera, lozinke za pristup upravljivim preklopnicima i vatrozidu, čuvaju se u pisanom obliku u vatrootpornom ormaru, kako bi se u slučaju nesreće, a kada bi došlo do zamjene izvršitelja novozaposlenim djelatnikom, moglo brže reagirati.

Voditelj odsjeka za informatičke poslove i kompjutorizaciju je zadužen za provjeru logova servera o pravilnom izvršenju sigurnosnih kopija te samoj ispravnosti istih.

Isto tako se prema proceduri o izradi sigurnosnih kopija, koja je sastavni dio ISO9001 dokumentacije, provjerava upotrebljivost sigurnosnih kopija, čime se osigurava kontinuitet poslovanja i dostupnost podataka informacijskog sustava Grada Rovinja-Rovigno.

5. METODOLOGIJA ISTRAŽIVANJA

5.1. Predmet rada

Predmet rada je sigurnost informacijskih sustava te utjecaj upravljanja informacijskom sigurnošću na kontinuitet poslovanja u Gradu Rovinj-Rovigno kroz procjenu rizika.

Pitanje da li Grad Rovinj ulaže dovoljnu količinu financijskih sredstava u informacijsku sigurnost vlastitog sustava nameće se samo od sebe, te je taj aspekt potrebno sagledati, kako bi se zaokružilo istraživanje o upravljanju informacijskom sigurnošću Grada i pripadajuće mu uprave. Pritom valja uzeti u obzir činjenicu da niti veličina proračunskih sredstava izdvojenih za ulaganja u informatičku opremu, programe i aplikacije, operativne sustave i licence, odnosno za njihovo tekuće održavanje, nije uvijek jamstvo postizanja kvalitetne razine sigurnosti, posebno ukoliko se sredstva troše bez nejasnih i nedefiniranih strategija zaštite informacijskog sustava i smanjivanja razine rizika, kojem je bez prekida danonoćno izložen informacijski sustav.

5.2. Ciljevi rada

Cilj ovog rada je temeljem odabrane NIST-ove metode procjene rizika utvrditi najkritičnije dijelove informacijskog sustava te predložiti mjere za smanjenje rizika na prihvatljivu razinu. Analizom ulaganja proračunskih sredstva u informatičku sigurnost u posljednjih 12 god. odgovoriti će se na pitanje, da li Grad Rovinj-Rovigno ulaže dovoljno u sigurnost informacijskog sustava.

5.3. Istraživačka pitanja

P1: Da li je ustaljena praksa (trenutno stanje) Grada Rovinja-Rovigno upravljanja sigurnošću informacijskog sustava (tehnički i ne tehnički izvori prijetnji) na prihvatljivoj razini u smislu kontinuiteta poslovanja Grada.

P2: Da li Grad Rovinj-Rovigno ulaže dovoljno u sigurnost informacijskog sustava.

5.4. Odabrana metodologija procjene rizika

Metoda koja će se u ovom radu koristiti je NIST (National Institute of Standards and Technology) metoda procjene rizika.

Rizik je po definiciji opasnost ili vjerojatnost da će odgovarajući izvor prijetnji u određenim okolnostima iskoristiti ranjivost ili slabost sustava, čime se posljedično može počiniti neka šteta imovini organizacije. Kad govorimo o rizicima u digitalnom poslovanju onda oni proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije koji su važna podrška odvijanju i unapređenju poslovnih procesa i poslovanja bilo kojeg poslovnog subjekta. Možemo ih predočiti funkcijom koja predstavlja međudjelovanje varijabla poput imovine poslovnog subjekta (materijalna i financijska), prijetnji (incidenti, neželjeni događaji) i ranjivosti (slabost sustava koja predstavlja razinu implementiranih kontrola čiji je cilj spriječiti pojavu neželjenih događaja). Ta se šteta može ogledati u materijalnom i financijskom smislu, a može biti izravna ili neizravna (Dalziel, 2015, 14).

RIZIK = f (imovina, prijetnja, ranjivost)

TIP IMOVINE	RANJIVOST	PRIJETNJA
Hardware	Neredovito održavanje	Tehnički kvar u sustavu
	Nezaključani ormarići	Namjerno uzrokovanje kvara
	Nekontrolirano odbacivanje medija	Krađa medija i dokumenata
Software	Nedovoljno testiranje softwarea	Greška u aplikaciji
	Poznate ranjivosti u softwareu	Iskorištavanje poznatih ranjivosti
	Nedostatak operativnih i sistemskih zapisa	Neovlaštene promjene u sustavu
Mreža	Slabo upravljanje zaporkama	Napadi probijanjem lozinki
	Nekriptirani promet	Prisluškivanje prometa
	Neredundantna oprema	Kvar na mrežnom uređaju
Ljudi	Nedovoljna obučenost ljudi	Greške pri korištenju
	Manjak obučenog kadra	Otkaz djelatnika
Lokacija	Nedostatak agregata ili UPS-ova	Nestanak struje

Tablica 1 Primjer popisa ranjivosti i prijetnji pri procjeni rizika

Izvor: Kako upravljati IT rizicima, http://www.alterinfo.hr/userfiles/media/upravljanje_rizicima.pdf

Procjena sigurnosnog rizika uključuje razmatranje poslovne štete koja može nastati kao rezultat sigurnosnih propusta uzimajući u obzir posljedice gubitaka podataka, cjelovitosti i dostupnosti informacija. Isto tako mora se uzeti u razmatranje i realnu vrijednost da će do tih incidenta i doći uz prevladavajuće prijetnje te trenutačnu implementaciju zaštitnih mehanizma.

„Procjena rizika je proces prepoznavanja, kvantificiranja i razvrstavanja rizika po prioritetima prema kriterijima za prihvaćanje rizika i ciljevima važnim za organizaciju, a sastoji se od dva pod procesa, analize rizika i vrednovanje rizika.” (Vukelić, 2016).

Kako bi se moglo krenuti u procjenu rizika uz prethodno opisane ranjivosti i prijetnje, potrebno je opisati vrijednost imovine čiji gubitak Grad Rovinj-Rovigno može pretrpjeti u slučaju da prijetnja iskoristi ranjivost.

Informacijsku imovinu Grada Rovinja-Rovigno možemo podijeliti na:

- nematerijalnu imovinu (baze podataka, aplikacijski i sistemski software, računalne, komunikacijske i servise za podršku u radu i licence),
- materijalnu imovinu (računala, serveri, komunikacijska oprema te ostala tehnička oprema).

Isto tako, informacijska imovina Grada je osjetljiva poslovna dokumentacija, mediji za pohranu podataka, različite procedure koje su važne za poslovanje pa i samo osoblje.

Hadjina (2016) smatra informacijskom imovinom sva sredstva koja skladište informaciju, prenose informaciju, kreiraju informaciju, koriste informaciju ili su informacija sama za sebe.

Vrijednost informacije se definira tako da djelatnici kroz intervju ističu scenarij koji se može dogoditi kao posljedica utjecaja prijetnji na:

- nedostupnost podataka ili informacija,
- otkrivanje podataka ili informacija,
- slučajnu ili namjernu promjenu informacija ili podataka i
- uništenje podataka ili informacija.

Slijedom navedenog metodologija procjene rizika po NIST –u sastoji se od devet koraka: (Stojaković – Čelustka, 2020).

1. Karakterizacija sustava
2. Identificiranje prijetnji
3. Identificiranje ranjivosti
4. Analiza kontrola
5. Određivanje vjerojatnosti
6. Analiza utjecaja
7. Određivanje rizika
8. Preporuka kontrola
9. Dokumentiranje rezultata

Karakterizacija sustava

U procjeni rizika za neki informacijski sustav prvi korak je definirati cilj poduhvata. U tom koraku identificiraju se granice informacijskog sustava, zajedno sa uređajima i informacijama koji čine sustav. Karakterizacijom informacijskog sustava se utvrđuje cilj procjene rizika, te se daju osnovne informacije (npr. hardver, softver, komunikacijske veze, odgovorno osoblje) za definiranje rizika.

Najprije je potrebno prikupiti informacije o samom sustavu kako bi se dobila slika informacijskog sustava i nacrt granica sustava, a sve to po slijedećem redoslijedu (Stojaković – Čelustka, 2020):

- hardver,
- softver,
- sučelja sustava (npr. interna i vanjska povezanost),
- podaci i informacije,
- osoblje koje održava i koristi informacijski sustav,
- namjena sustava (npr. procesi koje izvršava informacijski sustav),
- kritičnost sustava i podataka (npr. vrijednost i važnost sustava za organizaciju),
- osjetljivost sustava i podataka.

Kako bi se podaci mogli prikupiti koriste se razne tehnike (Rhodes-Ousley,, 2013):

- upitnici,

- intervjui odgovornih osoba,
- pregled dokumentacije te
- uporaba automatskih skenirajućih alata.

Identifikacija prijetnji

Sama prijetnja ne predstavlja rizik kada nema ranjivosti koja se može iskoristiti. U određivanju vjerojatnosti prijetnje potrebno je razmotriti prijetnje, potencijalne ranjivosti i postojeće kontrole. U procjeni prijetnji važno je razmotriti sve potencijalne izvore prijetnji koje mogu prouzročiti štetu u informacijskom sustavu i njegovoj radnoj okolini. Centar Informacijske Sigurnosti (Stojaković – Čeluska) prikazuje prijetnje kao:

- prirodni izvori prijetnji su prirodne nepogode,
- tehnički izvori prijetnji su tehnički kvarovi opreme,
- ljudski izvori prijetnji su:
    - unutarnji - nestručni projektanti informatičkog sustava, neodgovorni vlasnici cjelokupnog i dijelova informacijskog sustava, ovlašteni korisnici koji zlouporabe svoje ovlasti, operatori sustava i usluga koji zlouporabe svoje ovlasti, službenici koji imaju fizički pristup informatičkoj opremi, a koji zlouporabe svoje ovlasti, itd.;
    - vanjski - zlonamjerni pojedinci izvana, kriminalne organizacije, strane obavještajne službe, komercijalne organizacije, terorističke organizacije, itd.

Prikaz prijetnji ili lista potencijalnih izvora prijetnji mora biti prilagođena pojedinoj organizaciji i njenom radnom okruženju (npr. običaji korisnika na računalu). Informacija o prirodnim prijetnjama (npr. poplavama, potresima, olujama), također bi trebala biti lako dostupna.

Identifikacija ranjivosti

Analiza prijetnji nekog informacijskog sustava mora uključiti i analizu ranjivosti u okolini sustava i izradu tablice parova ranjivost/ prijetnja. Cilj ovog koraka je dobiti listu ranjivosti sustava (pogreški ili slabosti), koje bi se mogle iskoristiti od strane određene prijetnje (Stojaković – Čelustka, 2020).

Ranjivost	Prijetnja	Akcija prijetnje
Iz sustava nisu uklonjeni korisnički računi otpuštenih zaposlenika	Otpušteni zaposlenici	Spajanje na mrežu organizacije i pristup povjerljivim podacima organizacije
Računalni centar koristi raspršivače vode za gašenje vatre; ali nema vodootpornih prekrivača za hardver i ostalu opremu	Vatra, nesavjesno osoblje	Uključivanje raspršivača vode u računalnom centru

Tablica 2 Lista ranjivosti i prijetnji

Izvor: Osnove upravljanja rizikom, https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Preporučene metode za identificiranje ranjivosti sustava su upotreba izvora informacija o ranjivostima, sigurnosno testiranje sustava i razvoj liste sigurnosnih provjera. Potrebno je naglasiti da će tipovi ranjivosti koji će se pojaviti, kao i metodologija potrebna da se utvrdi da li ranjivosti postoje, obično ovisiti o prirodi informacijskog sustava i o fazi životnog ciklusa u kojoj se sustav nalazi.

Ako informacijski sustav još nije dizajniran, potraga za ranjivostima bi se trebala usmjeriti na sigurnosne politike organizacije, planirane sigurnosne procedure, definicije zahtjeva na sustav, te sigurnosne analize produkata od strane dobavljača ili graditelja sustava.

Ako je informacijski sustav u fazi primjene, identifikacija ranjivosti treba se proširiti uključujući više specifičnih informacija, kao što su planirana sigurnosna svojstva sustava opisana u dokumentaciji, te rezultati certifikacije i procjene sustava.

Ako je informacijski sustav u radnoj fazi, proces identificiranja ranjivosti bi trebao uključiti analizu sigurnosnih svojstava sustava i sigurnosne kontrole, tehničke i proceduralne, koje se koriste za zaštitu sustava (Stojaković – Čelustka, 2020).

Autorica navodi izvore informacija o ranjivostima te metode za testiranje sustava:

- dokumentacija od prethodnih analiza rizika procjenjivanog informacijskog sustava,
- izvještaji kontrolnih pregleda (audita) sustava, izvještaji o anomalijama sustava, izvještaji sigurnosnih pregleda, te izvještaji testiranja i procjene sustava,
- liste ranjivosti,
- sigurnosna upozorenja,
- upozorenja dobavljača,
- specijalizirane mailing liste,
- sigurnosne analize softvera sustava.

Metode koje se koriste za testiranje sustava mogu se upotrijebiti da se efikasno identificiraju ranjivosti sustava, ovisno o kritičnosti sustava i raspoloživih resursa, a mogu biti:

- automatizirani alati za skeniranje ranjivosti,
- sigurnosni test i procjena (ST&A),
- penetracijsko testiranje.

Analiza kontrola

Cilj ovog koraka je analizirati kontrole koje su primijenjene ili su planirane za primjenu u organizaciji da bi smanjile ili uklonile vjerojatnost da prijetnja iskoristi ranjivost sustava. Sigurnosne kontrole obuhvaćaju upotrebu tehničkih i netehničkih metoda.

Tehničke kontrole su zaštitni alati koji su ugrađeni u računalni *hardver*, *softver* ili *firmware* (npr. mehanizmi za kontrolu pristupa, mehanizmi za identifikaciju i autentikaciju, enkripcijske metode, aplikacije za otkrivanje neželjenog upada).

Netehničke kontrole su kontrole upravljanja i radne kontrole, kao što su sigurnosne politike, radne procedure, te sigurnost osoblja, fizička sigurnost i sigurnost okoliša.

Stojaković – Čelustka, (2020) je uz navedeno, tehničke i netehničke kontrole klasificirala na preventivne i aktivne:

- Preventivne kontrole sprečavaju pokušaje prekršaja sigurnosne politike i uključuju kontrole kao što su kontrola pristupa, enkripcija i autentikacija.
- Aktivne kontrole upozoravaju na prekršaje sigurnosne politike i sadrže kontrole kao što su nadzorna praćenja (eng. audit trails), metode otkrivanja upada i kontrolne sume (eng. checksums).

Određivanje vjerojatnosti rizika

Prema autorici Stojaković – Čelustka, (2020), vjerojatnost rizika označava mogućnost da se iskoristi ranjivost od strane prijetnje. Tri su faktora koja se moraju uzeti u obzir prilikom klasifikacije vjerojatnosti:

- motivacija i mogućnosti prijetnje,
- priroda ranjivosti,
- postojanje i učinkovitost tekućih kontrola.

Nivo vjerojatnosti	**Definicija vjerojatnosti**
Visoki	Prijetnja je visoko motivirana i ima dovoljno mogućnosti za realizaciju, a kontrole koje bi trebale spriječiti iskorištavanje ranjivosti su neefektivne.
Srednji	Prijetnja je motivirana i ima mogućnosti za realizaciju, ali postoje kontrole koje mogu spriječiti uspješno izvođenje prijetnje.
Nizak	Prijetnja nije motivirana ili nema dovoljno mogućnosti za realizaciju, ili postoje kontrole koje mogu spriječiti iskorištavanje ranjivosti

Tablica 3 Određivanje nivoa vjerojatnosti rizika

Izvor: Osnove upravljanja rizikom, https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Analiza utjecaja

Analiza utjecaja se očituje u uspješnom iskorištavanju ranjivosti s obzirom na čimbenike koje uzrokuju prijeteće signale u rušenju postavljenog sustava. Preliminarno, je prije svake radnje vršenja analize potrebno odrediti što je svrha

sustava, kakvu vrijednosnu važnost sustav ima u organizaciji, te odrediti koliko je sam sustav i njegovi podaci osjetljiv i samim time ugrožen.

Nakon analize pristupa se mjerenju utjecaja i to, kvantitativnom metodom i kvalitativnom metodom, uz postojanje prednosti i nedostataka obiju metoda, a prikaz veličine i definicije utjecaja dan je u Tablici 4 ispod.

Veličina utjecaja	Definicija utjecaja
Visoka	Iskorištenje ranjivosti može (1) rezultirati u visokim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskom smrću ili teškim ozljeđivanjem.
Srednja	Iskorištenje ranjivosti može (1) rezultirati u znatnim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskim ozljeđivanjem.
Niska	Iskorištenje ranjivosti može (1) rezultirati u troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno utjecati na poslovanje organizacije, njenu reputaciju ili interes

Tablica 4 Pojmovi definicije nivoa utjecaja

Izvor: Osnove upravljanja rizikom, https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Kvantitativan pristup mjerenja utjecaja rezultira u prikazu prihodovnih gubitaka, rješavanje popravaka sustava i mjerenju veličine angažmana za uspješno rješavanje potencijalne prijetnje, a ima prednost mogućnosti izmjere veličine utjecaja. S druge strane nedostatak je da može doći do nejasnih brojčanih podataka koji se tada moraju interpretirati opisno.

Kvalitativni pristup mjerenja utjecaja rezultira u nemogućnosti prikaza mjernim jedinicama, već je moguć prikazom opisa tj. opisujemo rezultat pojmom visokog, srednjeg ili niskog nivoa utjecaja.

Prednost kvalitativne analize utjecaja je u tome da ona odmah grupira rizik i unaprijed evidentira područja koja bi mogla dovesti do neželjenih posljedica, te kreće u rješavanje istih zbog uvida u sam proces sustava. Međutim, kako se tom analizom ne vrše mjerenja koja bi se prikazala brojčanim podacima, nije moguće napraviti analizu troškova, što rezultira nedostatkom. (Stojaković – Čelustka, 2020).

Određivanje rizika

Odrediti rizik znači procijeniti veličinu rizika za informacijski sustav, a može se prikazati kao funkcija:

- vjerojatnosti određene prijetnje da iskoristi određenu ranjivost,
- veličine utjecaja ako je prijetnja uspješno iskoristila ranjivost,
- prikladnosti planiranih ili postojećih sigurnosnih kontrola za smanjenje ili eliminiranje rizika.

Vjerojatnost prijetnje	**Utjecaj**		
	Niski (10)	**Srednji (50)**	**Visoki (100)**
Visoka (1.0)	Niski 10 X 1.0 = 10	Srednji 50 X 1.0 = 50	Visoki 100 X 1.0 =100
Srednja (0.5)	Niski 10 X 0.5 = 5	Srednji 50 X 0.5 = 25	Srednji 100 X 0.5 = 50
Niska (0.1)	Niski 10 X 0.1 = 1	Niski 50 X 0.1 = 5	Niski 100 X 0.1 = 10

Tablica 5 Vjerojatnost i utjecaj prijetnje

Izvor: Osnove upravljanja rizikom, https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Nivo rizika	**Opis rizika i potrebne akcije**
Visoki	Ako je neka pojava procijenjena kao visoki rizik, postoji jaka potreba za korektivnim mjerama. Postojeći sustav može nastaviti s radom, ali plan korektivnih akcija mora se ostvariti što je prije moguće.
Srednji	Ako je neka pojava procijenjena kao srednji rizik, potrebne su korektivne akcije i mora se razviti plan da se te akcije ostvare u razumnom vremenu.
Nizak	Ako je neka pojava procijenjena kao nizak rizik, mora se odlučiti da li su potrebne korektivne akcije ili se rizik može prihvatiti.

Tablica 6 Nivo rizika i potrebne akcije

Izvor: Osnove upravljanja rizikom, https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

Preporuka kontrola

Svrha preporuke je umanjiti veličinu rizika za sustav i omogućiti da se njegovi podaci sačuvaju i zaštite na što prihvatljiviji način. Preporuka kontrola definira proces procjene rizika i usmjeravanje prema njegovom ublažavanju. Cijeli proces je potkrijepljen i evidentiran preporučenim procedurama i sigurnosnim kontrolama.

Dokumentiranje rezultata

Rezultati procjene rizika (identificirane prijetnje i ranjivosti, procijenjeni rizik i preporučene kontrole) dokumentiraju se popratnim izvještajima.

Preventivne radne kontrole

Svaka poslovna organizacija u svom djelovanju nalaže postojanost preventivnih radnih kontrola, čime se umanjuje nastanak štetnih utjecaja i omogućava brže rješavanje istih ukoliko do njih dođe.
Preventivna radna kontrola je potkrijepljena u svakoj radnoj sredini donesenim pravilnicima i procedurama kojima se nalažu (Stojaković – Čelustka, 2020):

- kontrola pristupa podatkovnim medijima i odbacivanja tih medija (npr. kontrola fizičkog pristupa, demagnetizacijske metode),
- ograničenje vanjske distribucije podataka (npr. upotreba oznaka),
- kontrola računalnih virusa,
- sigurnosna kontrola računalnog prostora (npr. zaštitni čuvari, ulazne procedure za posjetioce, elektronički bedževi, biometrijska kontrola pristupa, upravljanje i distribucija lokota i ključeva, zapreka i ograda),
- sigurni ormari za ožičenje, preklopnike i kablove,
- mogućnosti izrade sigurnosnih kopija (npr. procedure za redovnu sigurnosnu kopiju podataka i sustava, pričuvni logovi koji čuvaju sve promjene u bazama podataka i koji se mogu iskoristiti za oporavak),
- procedure i sigurnost za pohranjivanje izvan radnog prostora,
- zaštita laptopa, osobnih računala (PC-a), radnih stanica,

- zaštita informatičke opreme od vatre (npr. zahtjevi i procedure za upotrebu aparata za gašenje vatre, vodootpornih pokrivača, suhi raspršivački sustavi, halonsko gašenje vatre),
- izvor električnog napajanja za hitne slučajeve (npr. zahtjevi za neprekidno napajanje, interni generatori),
- kontrola vlažnosti i temperature računalnih prostorija (npr. uređaji za klimatizaciju, sustavi za grijanje).

5.5. Metoda analize proračunskih godina

Analiza je provedena na razdoblje od posljednjih 12 proračunskih godina tj. između 2009. i 2020 godine.

Odluka o odabiru godina je donesena na temelju detaljne analize troškova po evidentiranim stavkama iz knjigovodstvenih kartica u navedenom razdoblju prema kojoj kapitalni i tekući rashodi za informatiku niti u jednoj pojedinoj godini nisu pokazali značajnije razine odstupanja ukupnih rashoda u odnosu na iste u godinama koje su kasnije odabrane kao predmet ovog istraživanja. Pritom je kao kriterij uzeto odstupanje ukupnih rashoda u „ostalim“ godinama do najviše +/- 10% u odnosu na promatrane godine odnosno činjenica da li su u određenoj godini koja nije odabrana ukupni rashodi za informatiku viši za preko 10% od ukupnih rashoda u godini sa najvišim rashodima (2017.) odnosno da li su niži za više od 10% od ukupnih rashoda u godini sa najmanjim rashodima (2014.). Obzirom da niti jedna od promatranih godina u navedenom rasponu godina (2009.-2020.) nije izašla iz okvira postavljenog po datom kriteriju, za istraživanje su odabrane godine u pravilnim trogodišnjim razmacima odnosno konkretno 2011., 2014., 2017. te 2020.godina.

Dodatni argument zbog kojeg su za istraživanje odabrane navedene godine je taj, da one predstavljaju pune godine političkih mandata (2009.-2013.godine i 2013.-2017.godine) i to sa dva različita gradonačelnika, čime je uzorak dodatno obogaćen različitošću situacija. Iako je takva različitost zasigurno vidljivija i izrazitija, a možemo reći čak i karakteristična za podatke koji se odnose na konkretna ulaganja u „vidljivu“ komunalnu infrastrukturu, čime se nastoje „dobiti slijedeći izbori“.

Za lakše snalaženje u logici financijskih pravila utrošaka proračunskih sredstava potrebno je ukazati na određena pravila. Svaki utrošak u proračunu podložan je prethodnoj provjeri razine dotadašnjeg iskorištenja odnosno slobodnih planiranih sredstava na namjenskoj stavci (stavka organizacijske i programske klasifikacije je detaljnije razrađena po logici ekonomske klasifikacije odnosno „kontnog“ ili, preciznije rečeno, računskog plana proračunskog računovodstva kao najvažnijeg iako ne jedinog kriterija). Ta pravila su zakonski i prema pravilima struke uokvirena odredbama zakonskih i podzakonskih propisa koji reguliraju proračunsko računovodstvo i financije općenito. Ovdje su posebno važne sa općenitijeg aspekta odredbe Zakona o proračunu, dok je sa detaljnijeg tehničkog aspekta neophodno pridržavati se odredbi Pravilnika o proračunskom računovodstvu i računskom planu. S obzirom na mogućnost višekratnih izmjena plana proračuna (tzv.rebalansa), možemo slobodno reći da je glavninu troškova koji prvobitno čak i nisu bili planirani odnosno ukalkulirani prilikom izrade i donošenja proračuna krajem prethodne kalendarske godine, tehnički moguće izvršiti u trenutku nastajanja ukoliko je to u skladu s financijskim mogućnostima i situacijom u kojoj se proračun određene lokalne jedinice nalazi sa aspekta mogućnosti raspolaganja prenesenim viškom, trenutne likvidnosti te urednog izvršavanja preuzetih i dospjelih tekućih obveza prema dobavljačima i partnerima.

Iz toga možemo zaključiti da je proračunsko (ne)trošenje strogo stvar političkog prioriteta, trenutnih potreba ali i ukazanih prilika, često i u situacijama koje prethodno, prilikom izrade proračuna, nije bilo moguće predvidjeti u realnom obujmu ili uopće tim više što postoji i povezanost sa dinamikom ostvarivanja prihoda gdje ponekad, kao u slučaju prošlogodišnje neočekivane pojave epidemije koronavirusa, dolazi do apsolutnog podbacivanja ostvarivanja planiranih prihoda i nužnog redimenzioniranja izvršenja planiranih programa, pa makar to bilo i privremenog karaktera. U takvim slučajevima nastoji se zbog jasnih načela političkog marketinga reducirati potrebe onog što se ne smatra nužnim, a informatička sigurnost sustava kao dugoročan koncept koji je direktno bitan samo za radni proces i dugoročnu zaštitu podataka je, nažalost, blizu tog poimanja.

proračunska godina	licence	tekuće održavanje softwarea	tekuće i investicijsko održavanje informatičkih postrojenja i opreme	ulaganja u računala i računalnu opremu	ulaganja u video sustav kontrole kretanja	računalni programi	UKUPNO
2011.	69.878,40	161.785,25	7.612,52	23.326,79	14.600,10	165.023,19	**442.226,25**
2014.	23.470,39	310.700,00	9.681,20	76.182,90	0,00	0,00	**420.034,49**
2017.	86.840,13	435.080,63	1.000,00	56.984,77	54.450,57	228.687,50	**863.043,60**
2020.	30.081,26	582.317,95	4.280,25	98.952,60	0,00	104.362,50	**819.994,56**
UKUPNO	**210.270,18**	**1.489.883,83**	**22.573,97**	**255.447,06**	**69.050,67**	**498.073,19**	**2.545.298,90**

Tablica 7 Ukupni rashodi Proračuna Grada Rovinja-Rovigno u informatiku u godinama 2011., 2014., 2017. i 2020.

Izvor: Glavna knjiga Proračuna Grada Rovinja-Rovigno – analitičke kartice ekonomske klasifikacije

Za kvalitetniju analizu pokazatelja iz tablice 7 iznad, treba reći da su ovdje prikazani kompletni rashodi za informatičke potrebe gradske uprave od čega tek oko 8,5% predstavlja rashode za informacijsku sigurnost (tablica 9). Ovo je napomenuto posebno radi činjenice što više od 75% troškova na ukupne informatičke potrebe kumulativno spada na dvije kategorije troškova: tekuće održavanje programa i ulaganje u računalne programe koji tek indirektno i u prilično malom postotku sudjeluju u rashodima za informacijsku sigurnost te stoga nisu ušli u kategoriju navedenih rashoda.

Kod tekućeg održavanja programa (na koje u ukupnim rashodima za informatičke potrebe u promatranom razdoblju otpada čak 58,53%) prevladavaju rashodi bazirani na ugovornim odnosima sa specijaliziranim tvrtkama za slijedeće namjene: održavanje i dopune web-stranice, održavanje web-kamere, održavanje sustava IIS (informacijskog sustava za vođenje računovodstva, porezne evidencije tj. pdv-a, platnog prometa, blagajne, saldakonti, komunalnog gospodarstva itd.), održavanje sustava Wage / Wagh (informacijskog sustava za vođenje i obračun plaća i naknada), održavanje Baze imovine, održavanje digitalne arhive, održavanje Registra ugovora, održavanje sustava radnih naloga, korištenje sustava „e-računi“, održavanje aplikacije „Smart Rovinj“.

Rashodi za ulaganje u računalne programe obuhvaćaju nabavku i instalaciju programa kao i njihove dogradnje i dorade za omogućavanje redovnog funkcioniranja: IIS, Data Collectora, programa za vođenje dugotrajne imovine, programa evidencije poljoprivrednog zemljišta, programa za izračunavanje zateznih kamata, programa za vođenje evidencije stanova u otplati, raznih programa za potrebe vođenja komunalnog gospodarstva, Wage / Wagh, programa pisarnice te AutoCad-a itd.

Rashodi za nabavu računalne opreme obuhvaćaju nabavu računala, pisača, monitora, prijenosnih računala, dodatne memorije te Windows operativnog sustava koji se u posljednjih desetak i više godina redovito nabavlja uz nova računala. Od navedenog obujma nabave opreme, izdvojena je upravo nabavka računala sa operativnim sustavom kao rashod koji izravno utječu na povećanje informacijske sigurnosti. Razlog za to jest činjenica da nova računala imaju bolje tehničke karakteristike i performanse te, zajedno s najnovijim inačicama operativnog sistema podržavaju i najnovije inačice antivirusnog programa, čime se podiže razina informatičke sigurnosti i smanjuju rizici na razini uprave. Ovi rashodi sudjeluju u promatranom razdoblju sa svega 10,04% udjela ukupnih informatičkih rashoda na razini gradske uprave.

Rashodi za licence obuhvaćaju nabavke licenci bilo da se radi o fiksnim nabavkama kao kapitalnim ulaganjima odnosno ulaganjima u dugotrajnu imovinu ili da je riječ o vrsti tekućih rashoda za licence koje su vremenski limitirane i produžavaju se na razdoblje od godine dana. Na te rashode otpada 8,26% od ukupnih rashoda za informatičke potrebe.

Iz tablice 7 možemo zaključiti da je jedina skupina rashoda koji bilježi konstantan rast u promatranom razdoblju upravo ona koja se odnosi na tekuće održavanje programa. Ugovorni odnosi sa specijaliziranim kućama koji osiguravaju funkcioniranje raznih programa i aplikacija ali i službene web-platforme u nezanemarivom obujmu može navesti na lažan zaključak da je time osigurana visoka razina funkcionalnosti sustava odnosno svih njegovih programsko-aplikativnih dijelova. To je samo dio istine o potrebama informacijske sigurnosti i informatičkim standardima koji bi morali pratiti razinu dostignutu od strane drugih segmenata razvoja Grada od kojih možemo izdvojiti npr. stanje komunalne infrastrukture, stanje kulturnih i predškolskih standarda, praćenje socijalnih potreba ekonomski ugroženog stanovništva itd.

proračunska godina	ostvareni prihodi	rashodi za informacijsku sigurnost					
		licence (antivirusi i vatrozid)	održavanje i popravci u sustavu (servera i slično)	ulaganja u računala računalnu opremu (PC) i operativne sustave (Windows)	ulaganja u video sustav kontrole kretanja	UKUPNO	% izdvojenih sredstava u ostvarnim prihodima
2011.	105.964.425,59	8.440,78	0,00	23.326,79	14.600,10	**46.367,67**	0,04
2014.	142.597.776,97	9.059,50	1.710,00	29.288,00	0,00	**40.057,50**	0,03
2017.	141.955.219,32	9.059,50	0,00	34.954,25	54.450,57	**98.464,32**	0,07
2020.	112.609.737,10	16.517,50	0,00	26.176,25	0,00	**42.693,75**	0,04
UKUPNO	**503.127.158,98**	**43.077,28**	**1.710,00**	**113.745,29**	**69.050,67**	**227.583,24**	**0,05**

Tablica 8 Prihodi Proračuna Grada Rovinja-Rovigno i rashodi za informacijsku sigurnost u godinama 2011., 2014., 2017. i 2020.

Izvor: Glavna knjiga Proračuna Grada Rovinja-Rovigno – analitičke kartice ekonomske klasifikacije

proračunska godina	ukupni rashodi u informatiku	rashodi za informacijsku sigurnost	% izdvojenih sredstava za informacijsku sigurnost u ukupnim rashodima za informatiku
2011.	442.226,25	46.367,67	10,49
2014.	420.034,49	40.057,50	9,54
2017.	863.043,60	98.464,32	11,41
2020.	819.994,56	42.693,75	5,21
UKUPNO	**2.545.298,90**	**227.583,24**	**8,94**

Tablica 9 Udio rashoda za informacijsku sigurnost u ukupnim rashodima za informatiku Proračuna Grada Rovinja-Rovigno u godinama 2011., 2014., 2017. i 2020.

Izvor: Glavna knjiga Proračuna Grada Rovinja-Rovigno – analitičke kartice ekonomske klasifikacije

Tablice 8 i 9 gore prikazuju obujam realnog utrošaka za sigurnost informacijskog sustava Grada. U svojoj ukupnosti ti rashodi sudjeluju tek sa 8,59% u ukupnim rashodima za informatiku. U tom su udjelu sadržani i rashodi za ulaganja u video-sustav kontrole kretanja koji ustvari ne predstavljaju pravi i tipičan informatički rashod. Ipak se radi o sustavu koji omogućuje fizički nadzor u drugoj zgradi gdje je smješten manji broj djelatnika gradske uprave i gdje nema porte ali su u toj zgradi smješteni serveri pa su stoga obuhvaćeni i kao informatički rashodi i kao rashodi za informacijsku sigurnost (sa značajnim udjelom od 31,60% u ukupnim informacijskim rashodima).

Podatak o postotku izdvajanja sredstava (u rasponu od 0,03%-0,06%) u odnosu na ukupno ostvarene proračunske prihode vrlo jasno pokazuje razinu prioriteta informacijske sigurnosti koja nije karakteristična samo za Grad Rovinj-Rovigno već i za cijeli sustav javne uprave u Republici Hrvatskoj koji ovom problemu, osim časnim i rijetkim izuzecima, ne pristupa studiozno i ne razmišlja strateški. Trenutni prioriteti društva čine to da su politički prioriteti društva oni koji donose trenutačan rezultat odnosno proizvode trenutni efekt dok se ulaganja u segmente isključivo „dugoročnih“ razvoja društva među kojima su obrazovanje i znanost, a u koje zasigurno spada i informacijska sigurnost javne uprave zasad u drugom planu.

6. PROCJENA RIZIKA ZA GRAD ROVINJ-ROVIGNO

6.1. Karakterizacija sustava

Naziv opreme	Proizvođač	Model	HDD	Memorija
Server 1	IBM	PowerEdge	2x70GB	8GB
Server 2	DELL	PowerEdge SC 1430	2x500GB	16GB
Server 3	IBM	ThinkServer TD200x	2x250GB	8GB
Server 4	DELL	PowerEdge T30	2x1TB	32GB
Vatrozid	Fortinet	FortiGate 100E	x	x
Upravljivi preklopnici	HP	2510G	x	x
Upravljivi preklopnici	HP	1920G	x	x
Upravljivi preklopnici	HP	1920G	x	x
Upravljivi preklopnici	HP	1920G	x	x
Upravljivi preklopnici	Cisco	Catalyst 3750	x	x
Upravljivi preklopnici	Cisco	Catalyst 3750	x	x
Printeri mrežni	Xerox	Workcentre	x	x
Stolna računala	Razni	x	x	x
Prijenosna računala	Razni	x	x	x
Video nadzor	Axxonnext	x	x	x
Protuprovalni sustav	Securit	x	x	x
Sustav vatrodojave	Securit	x	x	x

Tablica 10 Karakterizacija sustava

Izvor: Izradio autor

6.2. Identificiranje prijetnji

Izvor prijetnje	Opis prijetnje	Karakteristika prijetnje
prirodni izvori prijetnji		
Poplava	Poplava u zgradi	Nemogućnost funkcioniranja Grada, mogućnost gubitaka podataka, softvera, licenci, sigurnosnih kopija
Požar	Požar u zgradi	Nemogućnost funkcioniranja Grada, mogućnost gubitaka podataka, softvera, licenci, sigurnosnih kopija
Potres	Potres	Nemogućnost funkcioniranja Grada, mogućnost gubitaka podataka, softvera, licenci, sigurnosnih kopija

tehnički izvori prijetnji		
Komunikacija	Zastoj vanjskih komunikacija	Nemogućnost komunikacije sa izdvojenim lokacijama, nemogućnost upotrebe e-maila, nemogućnost korištenja web aplikacija
Opskrba električnom energijom	Prekid opskrbe električnom energijom	Nemogućnost funkcioniranja Grada
Pohrana	Kvar diskova	Nemogućnost pristupa i greške prilikom pristupa disku
ljudski izvori prijetnji		
Nenamjerna prijetnja	Mogućnost kompromitiranja sigurnosti sustava od strane nestručnih i/ili neodgovornih korisnika informatičkog sustava	Mogućnost gubitaka podataka, odavanje službenih podataka i sl.
Namjerna prijetnja	Mogućnost kompromitiranja sigurnosti sustava od strane zlonamjernih pojedinaca izvana, pojedinaca iznutra, kriminalnih organizacija, strane obavještajnih službi, komercijalnih organizacija, terorističkih organizacija	Mogućnost gubitaka podataka, mogućnost financijskih gubitaka, mogućnost zastoja u poslovanju, ucjena, sabotaža

Tablica 11 Identificiranje prijetnji

Izvor: Izradio autor

6.3. Identifikacija ranjivosti

Ranjivost	Prijetnja	Akcija prijetnje
Iz sustava nisu uklonjeni korisnički računi otpuštenih zaposlenika	Otpušteni zaposlenici	Spajanje na mrežu Grada i pristup povjerljivim podacima
Računalni centar koristi raspršivače vode za gašenje vatre; ali nema vodootpornih prekrivača za hardver i ostalu opremu	Vatra, nesavjesno osoblje	Uključivanje raspršivača vode u računalnom centru

Tablica 12 Identificiranje ranjivosti

Izvor: Izradio autor

6.4. Analiza kontrola

Kratki naziv (Scoreboard)	Opis kontrola
Netehničke kontrole	
Pravilnik o izradi sigurnosnih kopija	Pravilnik o izradi sigurnosnih kopija servera i ispravnosti istih.
Mjere i pravila rada	Dokument opisuje postupanja kojih su se svi zaposlenici dužni pridržavati.
Odluka o imenovanju voditelja sigurnosti	Opisuje zadaće voditelja sigurnosti (voditelj odsjeka za informatičke poslove i kompjutorizaciju), koji će voditi brigu o upravljanju, podjeli zaduženja i samom obrazovanju korisnika. Voditelj sigurnosti brine o ukupnoj sigurnosti informacijskog sustava u što je uključena osobna sigurnost, fizička sigurnost, kontrola pristupa, razvoj i održavanje te usklađenost sa zakonskim propisima.
Obuka zaposlenika	Obuka zaposlenika koji koriste računala i prijenosna računala o potencijalnim prijetnjama i opasnostima
Tehničke kontrole	
Bilježenje pristupa (log) uređajima i aplikacijama	Aplikacije i računalni sustavi spremaju podatke o pristupima (logove) istima. Provode se periodične kontrole pristupa aplikacijama i računalnim sustavima u svrhu kontrole prava pristupa pojedincima.
Pristup dopušten samo prema potrebi	Pristup spremljenim logovima aplikacija i računalnim sustavima samo uz odobrenje najvišeg managementa i sveden je na minimum
Fizička kontrola	Fizička kontrola ulaza zaposlenika magnetnom karticom, zaštitar, sustav video nadzora, protuprovalni sustav sa dojavom u zaštitarsku tvrtku.
Zapisi o sigurnosnim kopijama	Da li se vode zapisi o izradi sigurnosnih kopija?
Osobni korisnički podatci	Da li su svakom zaposleniku dodijeljeni zasebni korisnički podaci za pristup aplikacijama i računalima?
Automatsko zaključavanje	Da li se računalo automatski zaključa u slučaju neaktivnosti korisnika?
Antivirusni program	Da li je na računalima instalirana najnovija inačica antivirusnog programa?
Periodična promjena lozinki	Da li se vrši periodična promjena lozinki?
Sustav vatrodojave	Dojava vatrogasnoj postrojbi Rovinj
Kvar uređaja – tvrdi disk u serveru	Da li se vodi računa o životnom vijeku tvrdih diskova?

Tablica 13 Analiza kontrola

Izvor: Izradio autor

6.5. Određivanje vjerojatnosti

Razina vjerojatnosti	Definicija vjerojatnosti
Visoki	Prijetnja ima visoku mogućnost za realizaciju, a kontrole koje bi trebale spriječiti iskorištavanje ranjivosti su neefektivne.
Srednji	Prijetnja ima srednju mogućnost za realizaciju, ali postoje kontrole koje mogu spriječiti uspješno izvođenje prijetnje.
Nizak	Prijetnja ima nisku mogućnost za realizaciju, ili postoje kontrole koje mogu spriječiti iskorištavanje ranjivosti

Tablica 14 Određivanje vjerojatnosti

Izvor: Izradio autor

6.6. Analiza utjecaja

Veličina utjecaja	Definicija utjecaja
Visoka	Iskorištenje ranjivosti može (1) rezultirati u visokim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskom smrću ili teškim ozljeđivanjem.
Srednja	Iskorištenje ranjivosti može (1) rezultirati u znatnim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskim ozljeđivanjem.
Niska	Iskorištenje ranjivosti može (1) rezultirati u troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno utjecati na poslovanje organizacije, njenu reputaciju ili interes

Tablica 15 Analiza utjecaja

Izvor: Izradio autor

6.7. Određivanje rizika

Vjerojatnost prijetnje	Utjecaj		
	Niski (10)	**Srednji (50)**	**Visoki (100)**
Visoka (1.0)	Niski 10 X 1.0 = 10	Srednji 50 X 1.0 = 50	Visoki 100 X 1.0 =100
Srednja (0.5)	Niski 10 X 0.5 = 5	Srednji 50 X 0.5 = 25	Srednji 100 X 0.5 = 50
Niska (0.1)	Niski 10 X 0.1 = 1	Niski 50 X 0.1 = 5	Niski 100 X 0.1 = 10

Tablica 16 Određivanje rizika

Izvor: Izradio autor

Nivo rizika	Opis rizika i potrebne akcije
Visoki	Ako je neka pojava procijenjena kao visoki rizik, postoji jaka potreba za korektivnim mjerama. Postojeći sustav može nastaviti s radom, ali plan korektivnih akcija mora se ostvariti što je prije moguće.
Srednji	Ako je neka pojava procijenjena kao srednji rizik, potrebne su korektivne akcije i mora se razviti plan da se te akcije ostvare u razumnom vremenu.
Nizak	Ako je neka pojava procijenjena kao nizak rizik, mora se odlučiti da li su potrebne korektivne akcije ili se rizik može prihvatiti.

Tablica 17 Opis rizika i potrebne akcije

Izvor: Izradio autor

6.8. Matrica rizika

Tablica 18 Matrica rizika

Kontrole/oprema	Netehničke kontrole							Tehničke kontrole						
	Pravilnik od izradi sigurnosnih kopija	Mjere i pravila rada	Odluka o imenovanju voditelja sigurnosti	Obuka zaposlenika	Bilježenje pristupa (log) uređajima i aplikacijama	Pristup dopušten samo prema potrebi	Fizička kontrola	Zapisi o sigurnosnim kopijama	Osobni korisnički podatci	Automatsko zaključavanje	Antivirusni program	Periodična promjena lozinki	Sustav vatrodojave	Kvar uređaja – tvrdi disk u serveru
Server 1	10	X	10	X	10	10	10	10	10	X	10	10	10	50
Server 2	10	X	10	X	10	10	10	10	10	X	10	10	10	50
Server 3	10	X	10	X	10	10	10	10	10	X	10	10	10	50
Server 4	10	X	10	X	10	10	10	10	10	X	10	10	10	50
Video nadzor	X	X	10	X	10	10	10	X	10	X	X	X	10	X
Vatrozid	X	X	10	X	10	10	10	X	10	X	X	X	10	X
Upravljivi preklopnici	X	X	10	X	10	10	10	X	10	1	X	X	10	X
Upravljivi preklopnici	X	X	10	X	10	10	10	X	10	1	X	X	10	X
Upravljivi preklopnici	X	X	10	X	10	10	10	X	10	1	X	X	10	X
Upravljivi preklopnici	X	X	10	X	10	10	10	X	10	1	X	X	10	X
Upravljivi preklopnici	X	X	10	X	10	10	10	X	10	1	X	X	10	X
Pisači - mrežni	X	X	5	X	1	1	1	X	1	X	X	X	1	X
Stolna računala	X	50	5	50	1	1	1	X	1	1	10	10	1	X
Prijenosna računala	X	50	5	50	1	1	1	X	1	1	10	10	1	X

Temeljem gore prikazane matice rizika (Tablica 18) odrediti će se i analizirati sigurnosni rizici za kontinuitet poslovanja Grada Rovinja. Razina rizika rezultat je umnoška razine vjerojatnosti (Tablica 14) i veličine utjecaja (Tablica 15) za svaku definiranu sigurnosnu kontrolu iz Tablice 13. Za određivanje razine rizika koristi će se matrica 3x3 sa vrijednostima: niska, srednja i visoka (Tablica 16). Rizici ocijenjeni kao srednji i visoki zahtijevaju daljnju obradu. Opisi rizika i potrebne akcije dane su u Tablici 17.

Analizom matrice rizika dolazi se do zaključka da su slijedeći izvori rizika ocijenjeni kao srednji rizik, odnosno da je na njih potrebno korektivno djelovati:

- Kvar tvrdih diskova servera 1, 2, 3 i 4;
- *Mjere i pravila rada* za korisnike stolnih i prijenosnih računala i
- Razina edukacije korisnika stolnih i prijenosnih računala.

Kao rezultat postupka procjene rizika donijeti će se preporučene sigurnosne mjere.

6.9. Preporuka kontrola za umanjivanje rizika

1) Predlaže se ažuriranje postojećeg dokumenta *Mjere i pravila rada* s obzirom na novonastale prijetnje barem jednom godišnje. Za implementaciju mjere nisu potrebna financijska sredstva.
2) Predlaže se češća edukacija djelatnika koji rade sa osobnim ili prijenosnim računalima u svrhu smanjenja rizika pojave neželjenih posljedica. Za implementaciju mjere nisu potrebna financijska sredstva.
3) Predlaže se zamjena tvrdih diskova kojima je životni vijek pri isteku koristeći podatak o MTBF (prosječno vrijeme prije kvara) koje je mjera pouzdanosti proizvoda ili komponente tijekom očekivanog vijeka trajanja.

Obzirom da za provedbu predloženih mjera 1) i 2) nisu potrebni financijski resursi, te provedba ne zahtijeva veći angažman vremenskih i ljudskih resursa, u nastavku će se detaljno obraditi samo mjera 3) koja je najkritičnija za osiguranje kontinuiteta poslovanja Grada.

6.10. Snimak trenutnog stanja u Gradu Rovinju-Rovigno

Za potrebu analize trenutnog stanja uzet je kao primjer „server za financije i knjigovodstvo“ koji je ujedno i najkritičniji server u Gradu pošto se na njemu izvršavaju sve knjigovodstvene aplikacije, plaće, materijalno knjigovodstvo, aplikacija za naplatu komunalnog prihoda, baza sklopljenih ugovora i dr. Server je nabavljen 2010. godine,

pokreće ga Windows Server 2008 R2 operativni sustav te je radi kvalitetnijeg i stabilnijeg napajanja spojen na APC „Smart“ neprekidno napajanje koje omogućuje cca. 40 min rada u slučaju izostanka mrežnog napona. Konfiguracija servera je slijedeća:

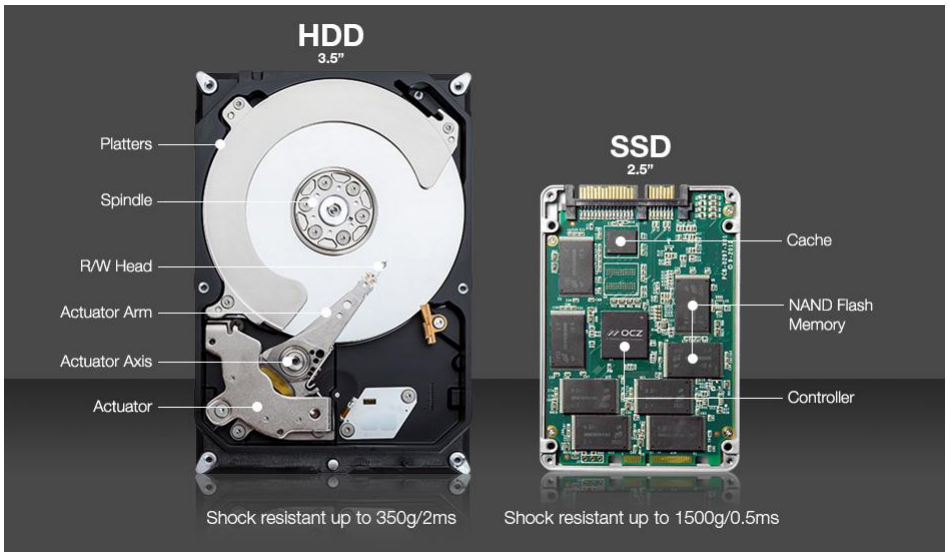
- Model: IBM ThinkServer TD200x
- Procesor Xenon E 5520 2,27GHz, 4 jezgre,
- Radna memorija: 8GB Ram-a,
- Redundantno napajanje,
- Disk: 2 x IBM xSeries, 146Gb, 15k rpm, 6Gb SAS, koji su 2018.g. zamijenjeni Samsung SSD 860 Pro, 256GB

Najkritičniji dio servera i općenito svakog PC-a su zasigurno HDD-ovi ili tvrdi diskovi na kojem su osim operativnog sistema i svih radnih aplikacija pohranjeni i svi podaci i baze podataka.

Tipični tvrdi diskovi koriste namagnetizirane rotirajuće ploče za čuvanje podataka (vizualno slični CD mediju). Takozvana glava lebdi iznad rotirajućih ploča i na taj način čita i upisuje podatke (slično gramofonu). Što se brže diskovi rotiraju performanse tvrdog diska rastu. Druga stavka koja utječe na brzinu samog tvrdog diska je njegova fizička veličina. Ona se mjeri u inčima, odnosno mjeri se dijagonala samog uređaja, pa su standardne dimenzije 2,5'' ili 3,5''. Jednostavno što je fizički veći HDD više ima prostora za rotirajuće ploče koje pri istoj brzini rotacije imaju veću kutnu brzinu, samim time i veću brzinu pisanja i čitanja.

Solid State Drive ili skraćeno SSD nova je generacija tvrdog diska bez pokretnih dijelova. Podaci se čuvaju u čipovima fleš memorije (eng. flash memory chips). Dakle tehnologija je slična kao na fleš momorijama (USB stick-ovima) ali su čipovi drugog tipa i puno su brži. O samoj implementaciji chipova ovisi i brzina diska i njegov vijek trajanja, pa su danas već u upotrebi nekoliko različitih vrsta SSD diskova, a napredak u tehnologiji nastavlja se ubrzanim tempom. Općenito, SSD diskovi se temelje na četiri različite NAND ćelijske tehnologije (Što je solid state disk – SSD, 2019):

- *SLC (Single Level Cell)* - jedan bit po ćeliji,
- *MLC (Multi-Level Cell)* - dva bita po ćeliji,
- *TLC (Triple Level Cell)* - tri bita po ćeliji,
- *QLC (Quad Level Cell)* - četiri bita po ćeliji



Slika 9 Fizička usporedba HDD-a i SSD-a

Izvor: https://shop.times.hr/zamijenite-svoj-tvrdi-disk-hdd-iz-prijenosnog-racunala-sa-ssd-diskom-i-znatno-ubrzajte-rad-sada-vec-sporijeg-prijenosnika.html (pristupio, 9.2020.)

Iz samog opisa dvaju modela tvrdih diskova i slike 9, da se zaključiti kako nova generacija tvrdih diskova (SSD) ima nebrojene prednosti, a neke od njih su:

- SSD je 25 do 100 puta brži od tipičnog tvrdog diska,
- Niska potrošnja energije - nema pokretnih dijelova i ne zahtijeva mehanički rad da bi postao operativan,
- Izdržljiviji je na padove i udarce od magnetnih tvrdih diskova jer nema pokretnih ili mehaničkih dijelova;
- Bez buke tijekom rada - odsutnost rotirajućeg metalnog diska za pohranu podataka i pokretne ruke za čitanje čini ga potpuno mirnim za vrijeme rada;
- Kompaktniji i lakši od tvrdih diskova.

Nedostatci SSD-a pred tipičnim magnetnim diskovima su veća cijena i manji kapacitet međutim ubrzanim razvojem tehnologije cijena sve više pada a i kapaciteti diskova rastu.

Stavka koju treba također uzeti u obzir je životni vijek ili trajnost diskova koja ovisi o mnogo faktora, a najviše o samom opterećenju diska. Što disk više radi trebao bi kraće trajati. MTBF (prosječno vrijeme prije kvara) je mjera pouzdanosti proizvoda

ili komponente tijekom očekivanog vijeka trajanja. Mnogi proizvođači se hvale svojim proizvodima pa je u „šumi“ brojnih modela vrlo teško izabrati pravi.

Obično se radi pouzdanosti izabiru diskovi poznatih i provjerenih proizvođača pa je tako Grad Rovinj-Rovigno za svoj server koristio serverske diskove renomiranog proizvođača IBM "xSeries " koji su nakon 8 godina zamijenjeni isto tako pouzdanim Samsung SSD 860 Pro, 256GB čije je prosječno vrijeme prije kvara 5 godina.

Procjena razine rizika na sigurnost podataka uslijed kvara njegovih diskova. U obzir je uzeto da je sigurnosna kopija dostupna i ispravna te da popravak ne vrši „outsourcing“ tvrtka već se on vrši od strane djelatnika odsjeka za informatičke poslove i kompjutorizaciju.

Direktni gubici nastali zamjenom oba diska uslijed tehničkog kvara

Varijanta 1. Iznenadni kvar dvaju HDD istovremeno (vrlo mala vjerojatnost, vrlo mali rizik, velika šteta)

Cijena SSD diska (2 kom.)	3.800 kn (2018.g.)
Cijena popravka (10h, zanemariva)	
Nedostupnost servera 1-2 dana	

Varijanta 2. Iznenadni kvar jednog HDD (srednja vjerojatnost, vrlo mali rizik, mala šteta)

Cijena SSD diska (1 kom.)	1.900 kn (2018.g.)
Cijena popravka (1h, zanemariva)	
Nedostupnost servera - nema	

Varijanta 3. Planirana zamjena HDD (planirani trošak)

Cijena SSD diska (2 kom.)	3.800 kn (2018.g.)
Cijena zamjene (1h, zanemariva)	
Nedostupnost servera - nema	

Indirektni gubici nastali uslijed tehničkog kvara servera

U slučaju nedostupnosti servera za financije i knjigovodstvo direktno je pogođen Odjel za financije, proračun i naplatu prihoda koji broji 10 djelatnika. Uzimajući u obzir da je prosječna cijena jednog radnog sata djelatnika u tom odjelu 50 kn možemo izračunati cijenu rada servera po danu a to je 4.000,00 kn.

Cijena rada servera po danu = cijena radnog sata × broj djelatnika × 8

Ono što nismo uzeli u kalkulaciju je da taj server koriste i drugi odjeli u Gradu za razne izvještaje, pohranu ugovora te se indirektno koristi za plaćanje računa dobavljačima. Nedostupnost servera za ostale odjele i zaposlenike ne donosi značajni financijski gubitak ali posljedično donosi nepovjerenje i narušavanje poslovnog ugleda naspram dobavljačima i građanima.

7. RASPRAVA

Provedena je analiza na konkretnom primjeru korištenja servera za potrebe Odjela za financije, proračun i naplatu prihoda kao najkritičnijeg komadića poslovne sfere, odnosno kakav utjecaj na informacijsku sigurnost ima eventualna nastala šteta.

Sam utjecaj rješavanja eventualne nastale štete pripisuje se isključivo internom djelovanju Odjela za informatičke poslove i kompjutorizaciju i njenom rješavanju potrebnog zadatka zaštite. Njegova ingerencija je pratiti korištenje opreme i na vrijeme planirati nabavku te po potrebi mijenjati opremu potrebnu za pravilno izvršavanje informacijskih potreba što posljedično donosi siguran informacijski sustav i nepostojanje znatnih ugrožavanja informacijske sigurnosti što dokazuju do sada neevidentirani sigurnosni incidenti.

Varijanta 1 pokazuje kako je u najgorem slučaju, kada bi hipotetski uzeli u obzir da oba diska servera istovremeno zakažu, šteta najveća a sukladno tome i rizik gubitaka podataka najveći. Pošto bi takav događaj bio po pretpostavci iznenadan (neplaniran) moralo bi se pristupiti nabavci diskova te kompletnoj ponovnoj instalaciji servera, što bi potrajalo do 2 dana što rezultira velikim gubitkom u radu. Šteta bi bila još veća ukoliko bi se ispostavilo da je i sigurnosna kopija neispravna. Tada bi se svi podaci morali ručno unositi što bi trajalo mjesecima. Vjerojatnost takvog događaja je ipak jako mala jer je sama konfiguracija RAID 1 polja (zrcaljenje) vrlo sigurna.

Varijanta 2 pokazuje iznenadan kvar jednog od dva diska u RAID 1 polju. Kada se takav kvar dogodi, ukoliko se na vrijeme detektira, šteta je relativno mala a samim time i rizik od gubitka podataka isto mali. U tom slučaju server nastavlja sa svojim radom a nabavkom novog diska i njegovom zamjenom podaci se dupliciraju na novi disk Vidimo da je cijena štete samo cijena koštanja novog diska.

Treća varijanta prikazuje troškove kad se planira zamjena diskova radi dotrajalosti. Tu je ponovno trošak samo cijena diskova i sati rada djelatnika iz odjela za informatičke poslove i kompjutorizaciju kojemu je to ionako u opisu poslova.

Navedenim primjerom dokazujemo da se pravovremenom zamjenom diskova na serveru postiže to da je server „siguran“ i rizik gubitaka podataka a samim time šteta vrlo male.

Edukacijom djelatnika u samoj instituciji, njihovim odgovornim ponašanjem u skladu sa normama, te redovitim praćenjem i korištenjem alata neophodnih za poslovni

proces, svakako se utječe na nesmetan rad i osiguranje pozitivne egzistencije svakog poslovnog okruženja.

Vezano za ulaganje proračunskih sredstva u informacijsku sigurnost smatram da bi u situaciji koja je potpuno u rukama lokalnih jedinica, državna vlast mogla zakonskim rješenjima „natjerati“ lokalnu upravu na obvezu izdvajanja sredstava u određenom postotku od ostvarenih prihoda po uzoru na propisanu obvezu izdvajanja za Gradsko društvo Crvenog križa (za rad i djelovanje Službe traženja te za javne ovlasti i redovnu djelatnost društva) ili vatrogastva (konkretno za Područnu vatrogasnu zajednicu Grada). Naime, malo je vjerojatno da će u bliskoj budućnosti porasti politička svijest na način da će gradovi, općine i županije odnosno odgovorne osobe u istima, uz pomoć i na poticaj informatičkih stručnjaka koji su u njima zaposleni, pokrenuti strategije razvoja informacijskih sustava koji bi jamčili povećanu razinu upravljanja informacijskom sigurnošću.

U praksi bi na razini Grada valjalo najprije postaviti ciljeve i strategije razvoja informacijskog sustava njegove sigurnosti odnosno smanjivanje razine izloženosti vanjskim rizicima. Internim aktima bi trebalo standardizirati pojam „upravljanja informacijskom sigurnošću“ što bi bilo jamstvo obveznog izdvajanja sredstava u obimu za koji prilikom planiranja proračuna postoji procjena da je značajan i dovoljan u određenoj proračunskoj godini, a u skladu sa donesenim ciljevima i strategijom. Time bi se u drugi plan, barem što se tiče ovog segmenta informacijsko-tehničkog razvoja, stavio pristup „gašenja požara“ koji je toliko svojstven za funkcioniranje javne uprave na gotovo svakom području koje ima u svojoj nadležnosti.

8. ZAKLJUČAK

U današnje vrijeme velikog tehnološkog napretka, sve češćih cyber napada, kada sve veću ulogu ima i zaštita osobnih podataka, prikupljanje i širenje privatnih podataka zahtjeva zaštitu od bilo kojeg oblika neautoriziranog pristupa.

Informacije i podaci smatraju se vrlo vrijednom imovinom svake organizacije a kako bi se omogućilo normalno poslovanje, te informacije je potrebno prikladno zaštititi. Zahtjev za zaštitom informacija sve je važniji jer u okruženju distribuiranosti poslovne okoline informacije postaju izložene ranjivosti i većem broju prijetnji. Informacije mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektroničkim putem i sl. ali bez obzira u kojem se obliku informacija nalazila vrlo ju je važno prikladno zaštititi jer upravo tajnost informacija, ispravnost i pravovremeno posjedovanje daju organizaciji moć ka napretku i konkurentnost na tržištu.

Postoje brojne sigurnosne prijetnje s kojim se organizacije suočavaju a neke od njih su računalne prijevare, špijunaža, sabotaža, vandalizam, požar, poplava i slično. Sve prisutnije su štete nanesene organizaciji u obliku zlođudnog koda, računalnog hakiranja i uskraćivanja usluge. Internet kao mreža svih mreža nudi povezanost javnih i privatnih računalnih mreža i dijeljenje informacija među njima.

Gotovo sveprisutno usvajanje računalne tehnologije u svakodnevnom životu gdje se računala koriste za poslodavce, za igranje kod kuće, u školama, gdje se putem interneta kupuje roba u web trgovinama, provjerava elektronička pošta u kafićima, pametnim se telefonima provjerava stanje računa u banci donosi i niz sigurnosnih problema.

Iako tehnologija danas omogućuje veću produktivnost i pristup mnoštvu informacija samo klikom miša, ona uz to donosi i učestale hakerske napade koji pokušavaju otuđiti ili iznuditi raznim metodama određenu korist.

Cilj informacijske sigurnosti svakako je zaštititi informacije od velikog broja prijetnji u svrhu smanjenja poslovnih rizika, osiguranja poslovnog kontinuiteta te u konačnici povećanja broja poslovnih prilika i povrat investicija.

U Hrvatskoj postoji veliki broj procedura, metoda, pravila i zakona vezano za informacijsku sigurnost pa se u svoj toj „gomili“ ponekad i teško snaći i pravilno postupati. Isto tako slijedom donesenih Zakona u svrhu reguliranja informacijske sigurnosti osnovane su nacionalne institucije kao što su Nacionalni CERT, Zavod za

sigurnost informacijskih sustava, Ured vijeća za nacionalnu sigurnost, Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, Agencija za zaštitu osobnih podataka i Središnji državni ured za e-Hrvatsku.

Uz navedene zakone i institucije djeluju i određene norme i standardi od kojih su najpoznatiji ISO/IEC 27001 i ISO/IEC 27002 koji sadrže prijedloge ustroja sustava za zaštitu informacija kao i sustava provjere. Pri izradi sigurnosne politike preporuča se upotreba oba standarda.

Fizička zaštita igra važnu ulogu u zaštiti informacijskog sustava grada Rovinja-Rovigno. Tu se prvenstveno misli na zaštitu od otuđenja opreme koje je spriječeno video nadzorom i portirom koji kontrolira ulaz u objekte, te magnetnim karticama čime se kontrolira ulaz na određena mjesta koja su bitna za sigurnost.

Osim hakerskih napada, virusa, raznih pokušaja iznude od strane napadača upotrebom sofisticiranih kripto virusa i sl. najviše ugroza informacijske sigurnosti čine upravo sami zaposlenici koji namjerno ili nenamjerno čine postupke ili propuste koji dovode do toga da informacije „cure“ sa mjesta gdje bi trebale biti na mjesto gdje one ne bi trebale biti. Stoga je vrlo bitno da su zaposlenici educirani, upoznati sa procedurama i pravilima informacijske sigurnosti, te da poštuju zakonsku regulativu kako ne bi ugrozili informacijski sustav. Veliku ulogu vezano za upravljanje sigurnošću informacijskog sustava u gradu Rovinju-Rovigno ima voditelj odsjeka za informatičke poslove i kompjutorizaciju. On brine o edukaciji zaposlenika, dodjeli lozinki te pazi da se iste redovito mijenjaju, dodjeljuje prava pristupa zaposlenicima kako bi se sačuvala povjerljivost, integritet i dostupnost važnih podataka. Isto tako brine o izradi i kontroli sigurnosnih kopija servera, brine o ažurnosti aplikacija, operativnih sistema zaposleničkih računala, nadogradnjama antivirusnih alata te brine o konfiguraciji vatrozida čime se sprječava neautorizirani upad na lokalnu mrežu grada. Voditelj isto tako nadzire rad mreže i servisa, sudjeluje u razvoju aplikacija, nabavci računala i informatičke opreme te prijavljuje i dokumentira incidente ili pokušaje iznude CERT-u ili Mup-u a sve u svrhu izbjegavanja sličnih situacija u budućnosti.

9. LITERATURA

[1.] Andress J., *The Basics of Information Security. Understanding the Fundamentals of Infosec in Theory and Practice-Elsevier Inc,* Syngress, 2014

[2.] CARNet CERT: *Upravljanje kontinuitetom poslovnih procesa*, https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-15-307.pdf (pristupio 09.2020)

[3.] CARNet CERT: *Sigurnosna politika*, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf

[4.] Čizmić I., Boban M., Zlatović D. : *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*, str. 469-470, Split 2016.

[5.] Dalziel, Henry - *Infosec Management Fundamentals-Elsevier*, Syngress (2015)

[6.] Gradska obilježja, <http://www.rovinj-rovigno.hr/o-rovinju/gradska-obiljezja-grb-zastava-statut/>, (pristupio 07.2020.)

[7.] Gradsko vijeće Grada Rovinj-Rovigno, https://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradsko-vijece/ (pristupio 07.2020)

[8.] Hadjina N., *Zaštita i Sigurnost Informacijskih Sustava*, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2009

[9.] Juran A.: „Sigurnost informacijskih sustava", Pomorski fakultet u Rijeci, Sveučilište u Rijeci, Preuzeto 20.5.2020. s http://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/290-2014.pdf

[10.] Košutić D.: " *Disaster recovery vs. kontinuitet poslovanja*", 27001 Academy, http://advisera.com/27001academy/hr/blog/2010/11/04/disaster-recovery-vs-kontinuitet-poslovanja/

[11.] Ministarstvo uprave, <https://uprava.gov.hr/o-ministarstvu/ustrojstvo/uprava-za-politicki-sustav-i-organizaciju-uprave/lokalna-i-podrucna-regionalna-samouprava/842>, (02.2019.)

[12.] Nacionalni CERT, https://gov.hr/moja-uprava/pravna-drzava-i-sigurnost/sigurnost-na-internetu/nacionalni-cert/1913 (pristupio 09.2020)

[13.] Nacionalni CERT, Upravljanje Kontinuitetom poslovnih procesa, 2010, https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-15-307.pdf, (pristupio, 09.2020)

[14.] Organizacija gradske uprave, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/>, (pristupio 07.2020.)

[15.] Radmilović Ž., *Zbornik radova 4. Međunarodne znanstveno-stručne konferencije 2015*, Ministarstvo unutarnjih poslova Republike Hrvatske/ Ministry of the Interior of the Republic of Croatia Policijska akademija/ Police Academy str. 32

[16.] Rittinghouse J., James F. Ransome, *Business Continuity and Disaster Recovery for InfoSec Managers*-Digital Press, 2005

[17.] Rhodes-Ousley, M.: *Information Security: The Complete Reference*, Second Edi, The McGraw-Hill, 2013

[18.] Nacionalni CERT, Sigurnosna politika, 2016, https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf, (pristupio 08.2020).

[19.] Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, https://itrevizija.ba/wp-content/materijal/zakoni/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf (pristupio 08.2020.)

[20.] Statut Grada Rovinja-Rovigno, <http://www.rovinj-rovigno.hr/wp-content/uploads/2016/11/statut_hr.pdf>, (pristupio 07.2020.)

[21.] Stojaković-Čelustka S.: Osnove upravljanja rizikom informacijskog sustava, http://www.cis. r/files/celuska-Osnove_upravljanja_rizikom.pdf (pristupio 08.2020.)

[22.] Strategija razvoja Grada Rovinja – Rovigno za razdoblje 2015 – 2020 https://www.rovinj-rovigno.hr/wp-content/uploads/2016/11/STRATEGIJA-GRADA-ROVINJA-FINALNA-VERZIJA.pdf (pristupio, 5.2020.)

[23.] Što je solid state disk – SSD, https://www.datasector.hr/hr/blog/sto-je-solid-state-disk-ssd/12 (pristupio 09.2020.)

[24.] Uprava za e-Hrvatsku, https://uprava.gov.hr/o-ministarstvu/ustrojstvo/4-uprava-za-e-hrvatsku-1080/1080, (pristupio 07.2020.).

[25.] Upravni odjel za društvene djelatnosti, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjel-za-drustvene-djelatnosti/>, (pristupio 07.2020.)

[26.] Upravni odjel za gospodarstvo, javnu nabavu i evropske fondove, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjel-za-gospodarstvo-javnu-nabavu-i-europske-fondove-obavlja-sljedece-poslove/>, (pristupio 07.2020.)

[27.] Upravni odjel za komunalno gospodarstvo i izgradnju, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjela-za-komunalne-djelatnosti-i-opce-poslove/ >, (pristupio 07.2020.)

[28.] Upravni odjel za proračun, gospodarstvo i evropske fondove, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjel-za-proracun-gospodarstvo-i-europske-fondove/>, (pristupio 07.2020.)

[29.] Upravni odjel za prostorno planiranje zaštitu okoliša i izdavanje akata, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjel-za-prostorno-planiranje-zastitu-okolisa-i-izdavanje-akata/ >, (pristupio 07.2020.)

[30.] Upravni odjel za upravljanje imovinom i geodetske polove, <http://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/upravni-odjel-za-upravljanje-imovinom/ >, (pristupio 07.2020.)

[31.] Ured Gradskog vijeća i gradonačelnika, https://www.rovinj-rovigno.hr/gradska-uprava-i-organizacija/gradska-uprava/ured-gradskog-vijeca-i-gradonacelnika/ (pristupio 07.2020.)

[32.] Varga M., Strugar I.: Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb, 2016.

[33.] Vukelić B., Sigurnost informacijskih sustava – Skripta, Veleučilište u Rijeci, Rijeka 2016.

[34.] Zakon o elektroničkoj ispravi, https://narodne-novine.nn.hr/clanci/sluzbeni/2005_12_150_2898.html (pristupio 07.2020.)

[35.] Zakon o informacijskoj sigurnosti, https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html (pristupio 07.2020.)

[36.] Zakon o provedbi opće uredbe o zaštiti osobnih podataka, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html (pristupio 07.2020.)

[37.] Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, https://www.morh.hr/wp-content/uploads/2017/10/zakon-o-sigurnosno-obavjestajnom-nn79-06.pdf?x11742 (pristupio 07.2020.)

[38.] Zakon o sustavu domovinske sigurnosti, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2489.html, (pristupio 07.2020.)

[39.] Zakon o zaštiti osobnih podataka, https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html, (pristupio 07.2020.)

[40.] Zavod za sigurnost informacijskih sustava, https://www.zsis.hr/default.aspx?id=13, (pristupio 7.2020.)

[41.] Zorčec M.: „Upravljanje sigurnosnim rizicima”, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, (pristupio 5.2020.) s http://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/290-2014.pdf

[42.] Ždrnja, B., Antoliš, K.: *Sigurnost informacijskih sustava*, Algebra, Zagreb, 2010.

SAŽETAK

U ovom završnom radu predstavljeno je upravljanje informacijskom sigurnošću na primjeru javne uprave, lokalne samouprave Grada Rovinja – Rovigno.
Upravljanje informacijskom sigurnošću se ujedno i smatra najvažnijom normom za sustave upravljanja sigurnosti informacija. Provođenjem navedene norme, podiže se razina sigurnosti i sprječava nastajanje neželjenih ishoda i eventualnih gubitaka na poslovnom planu.
Uvodi se zaštita od prijetnji koje katkad rezultiraju ozbiljnim napadom na informacijsku infrastrukturu grada Rovinja-Rovigno.
Stoga je svakako neizbježno i obavezno širiti svijest pojedinca o zaštiti informacijskog sustava i uvođenje normi upravljanja informacijskom sigurnošću.
Opća umreženost te sveprisutnost informacijske i komunikacijske tehnologije u svim segmentima društva nameće potrebu jakih i jasnih zahtjeva na sigurnost, koje postižemo uvođenjem određenih sigurnosnih normi i pravila u poslovanju, a koje svakako kasnije utječu na kontinuitet poslovanja.

Ključne riječi: informacijska sigurnost, zaštita od prijetnji, napadi na informacijski sustav, kontinuitet poslovanja

SUMMARY

In this final paper the management of information security is presented using the example of public government and local self-governing body of the city of Rovinj-Rovigno.
The management of information security is also considered to be the most important norm of the whole information security management system. By implementing the mentioned norm, the level of security is also being raised as well as the prevention of undesirable outcomes or eventual losses in the business plan.
The protection against wide variety of threats, that are considered to be a serious danger to the IT infrastructure of city of Rovinj-Rovigno, is introduced.
Therefore, it is necessary and obligatory to spread the awareness to each individual about protecting the IT system and implementing the norms of information security management.
The general networking and the omnipresence of information and communicational technologies in all the segments of our society implies that we need strong and clear demands for security which is being achieved by implementing the safety norms and rules in the management and which certainly later affect business continuity.

Key words: information security, protection against threats, threats to the information systems, business continuity

POPIS TABLICA:

Tablica 1 Primjer popisa ranjivosti i prijetnji pri procjeni rizika 45
Tablica 2 Lista ranjivosti i prijetnji 49
Tablica 3 Određivanje nivoa vjerojatnosti rizika 51
Tablica 4 Pojmovi definicije nivoa utjecaja 52
Tablica 5 Vjerojatnost i utjecaj prijetnje 53
Tablica 6 Nivo rizika i potrebne akcije 53
Tablica 7 Ukupni rashodi Proračuna Grada Rovinja-Rovigno u informatiku u godinama 2011., 2014., 2017. i 2020. 57
Tablica 8 Prihodi Proračuna Grada Rovinja-Rovigno i rashodi za informacijsku sigurnost u godinama 2011., 2014., 2017. i 2020. 59
Tablica 9 Udio rashoda za informacijsku sigurnost u ukupnim rashodima za informatiku Proračuna Grada Rovinja-Rovigno u godinama 2011., 2014., 2017. i 2020. 59
Tablica 10 Karakterizacija sustava 61
Tablica 11 Identificiranje prijetnji 62
Tablica 12 Identificiranje ranjivosti 62
Tablica 13 Analiza kontrola 63
Tablica 14 Određivanje vjerojatnosti 64
Tablica 15 Analiza utjecaja 64
Tablica 16 Određivanje rizika 65
Tablica 17 Opis rizika i potrebne akcije 65
Tablica 18 Matrica rizika 66

POPIS SLIKA:

Slika 1 Povezanost triju aspekta informacijske sigurnosti CIA 9
Slika 3.: Shema gradske uprave Grada Rovinja - Rovigno 27
Slika 4 Gradski portal na lokalnoj mreži Grada Rovinja – Rovigno 33
Slika 5 Digitalna arhiva s djelovodnikom 34
Slika 6 Početna stranica za prijavu aplikacije TaskTrack 35
Slika 7 TaskTrack aplikacija 35
Slika 8 Web GIS Portal Grada Rovinja - Rovigno 36
Slika 9 Prikaz izgleda Web GIS Portala Grada Rovinja-Rovigno iz domene podataka o korištenju javnih površina na užem području grada 37
Slika 10 Fizička usporedba HDD-a i SSD-a 69