SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Tomislav Horvat

ANALIZA SIGURNOSTI I ZAŠTITE INFORMACIJSKO - KOMUNIKACIJSKOG SUSTAVA U KORPORATIVNOM OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2017.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA SIGURNOSTI I ZAŠTITE INFORMACIJSKO-KOMUNIKACIJSKOG SUSTAVA U KORPORATIVNOM OKRUŽENJU

ANALYSIS OF SAFETY AND SECURITY OF INFORMATION AND COMMUNICATION SYSTEM IN A CORPORATE ENVIRONMENT

Mentor: prof. dr. sc. Dragan Peraković

Student: Tomislav Horvat

JMBAG: 0135225986

Zagreb, rujan 2017.

SAŽETAK:

Postoji široki raspon proizvoda i usluga koji su namijenjeni otkrivanju rizika i ranjivosti IK sigurnosti. Nove sigurnosne prijetnje i nove sigurnosne tehnologije za zaštitu, razvijaju se svakodnevno. Pojavom IK (Informacijsko – komunikacijski) sustava značajno se promijenio način poslovanja i oblik komuniciranja čime su se razvili i novi mediji. Radno mjesto više nije fiksno određeno, a informacija je postala ubrzana i pojednostavljena. Razumijevanje brzine tih rješenja i kvalitetne zaštite ključne su za pravovremena ulaganja. Prioriteti, odabir i održavanje metoda sigurnosti i zaštite i dalje su glavna pitanja organizacija koje se suočavaju sa prijetnjama i ranjivostima. Stoga je posebno važno postaviti odgovarajuće mehanizme zaštite IK sustava uz definiranje sigurnosne politike organizacije što je u radu i prikazano.

KLJUČNE RIJEČI: Sigurnost, IK sustav, zaštita, metode zaštite, sigurnosna politika.

ABSTRACT:

There is a wide range of products and services designed to detect the risks and vulnerabilities of IK Security. New security threats and new security technologies for protection are being developed on a daily basis. With the introduction of IK (Information and Communication) systems, the way of business and the form of communication has changed significantly and new media have been developed. The workplace is no longer fixed and the information has become accelerated and simplified. Understanding the velocity of these solutions and their chances for success as they mature is critical for timely investments. Prioritizing, choosing and maintaining security technologies continue to be major issues for enterprises face continuing and newly introduced threats and emerging vulnerabilities. It is therefore particularly important to set up appropriate mechanisms of the IK system protection, defining the security policy of the organization as it is presented in the work.

KEYWORDS: Security, IK system, protection, methods of protection, security policy.

SADRŽAJ

1. Uvod

Posljednjih 20-ak godina dogodile su se značajne tehnološke promjene u sektoru privatne i korporativne sigurnosti, koje su utjecale i na razvoj sigurnosti IK (Informacijsko – komunikacijski) sustava. Negativna posljedica razvoja IK tehnologije je povećanje napada na IK sustave i zlouporaba podataka. Posljedice je moguće smanjiti provedbom sigurnosnih mjera i kvalitetnim strategijskim upravljanjem. Trenutno dostupne metode i načini zaštite IK sustava omogućuju organizacijama konkurentnost. Promjene i prilagodba sigurnosnim zahtjevima su nužne kako bi poslovne organizacije opstale na tržištu.

Ovaj rad daje uvid u prednosti zaštite IK sustava koje organizacija provodi, odnosno mjere, pravila i norme kojih se pridržavaju za sigurnost poslovanja u korporativnom okruženju. Sigurnost i zaštita IK sustava i poslovnog procesa predstavlja logično ulaganje organizacije koja želi sniziti troškove i poboljšati konačne rezultate poslovanja.

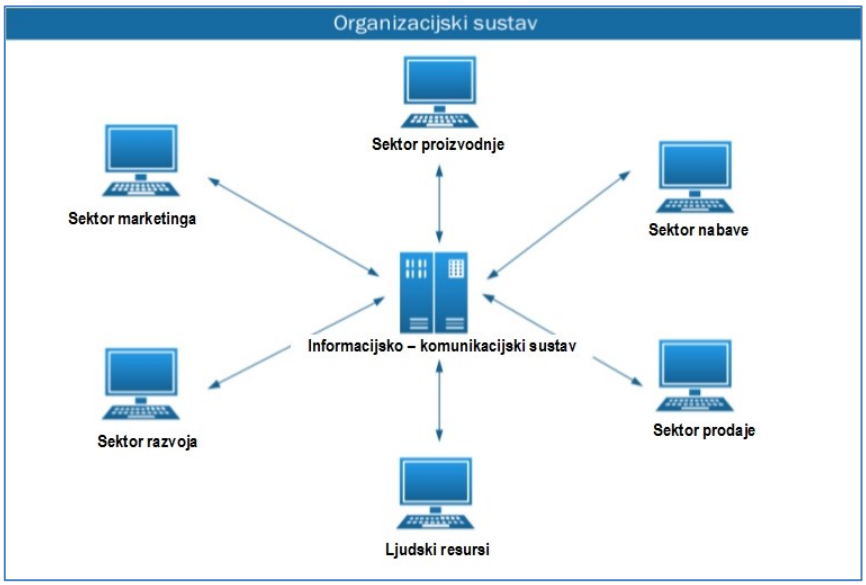
Diplomski rad se sastoji od sedam metodoloških cjelina uključujući uvod i zaključak. U uvodnom poglavlju definiran je problem i predmet istraživanja diplomskog rada, gdje se prikazuju i pojašnjavaju metodologije rada. Drugo poglavlje rada odgovara na pitanje zašto je potrebno obratiti pozornost na sigurnost IK sustava unutar korporativnog okruženja. Također u njemu se definiraju osnovni pojmovi, te sigurnosna svojstva koja daju veliki značaj za daljnju provedbu sigurnosti u korporativnom okruženju. Uz to prikazani su osnovni modeli sigurnosti i zaštite IK sustava, te sredstva koja se primjenjuju za zaštitu IK sustava. Treće poglavlje daje pozornost na sigurnosnom aspektu poslovanja i načinu korporativnog upravljanja, te prikazuje ovisnost korporativnog okruženja o IK sustavu. Isto tako u njemu se prikazuje arhitektura sigurnosnog sustava, te se opisuje ISMS (Informacijski sustav upravljanja sigurnošću), kao temeljni koncept sustava upravljanja poslovanjem.

Za praćenje standardizacije, te pravilnog načina implementacije IK sustava unutar korporativnog okruženja, potrebno je konstantno pratiti standarde, zakone i smjernice opisane u poglavlju četiri. Sve to zajedno sačinjava sigurnosnu politiku koja se provodi unutar korporativnog okruženja i predstavlja primarni okvir za razvoj sigurnosti i zaštitnih mehanizama IK sustava u poslovanju. Unutar petog poglavlja dan je primjer realnog poslovnog subjekta, unutar kojeg je definiran model sigurnosti IK sustava u korporativnom okruženju. Uz prikazani model definirana su pojedina sredstva zaštite korištene unutar organizacije, normativni okvir i sigurnosna politika organizacije.

Preporuke sigurnosti i metode zaštite IK sustava prikazuje se u poglavlju šest koje opisuje usporedbu suvremenih metoda sigurnosti i zaštite IK sustava u odnosu na realni poslovni subjekt. Sedmo poglavlje ujedno je i zaključno poglavlje, u kojemu će biti prikazane spoznaje i zaključci izvedeni iz prethodne analize stručne literature, znanstvenih članaka, prethodnih istraživanja slične tematike i navedenog primjera realnog poslovnog subjekta.

2. Sigurnost i zaštita informacijsko – komunikacijskog sustava

Sigurnost IK (Informacijsko – komunikacijski) sustava obuhvaća primjenu mjera za zaštitu podataka koji se obrađuju, pohranjuju ili prenose, od gubitka povjerljivosti, cjelovitosti i raspoloživosti [1]. Uloga IK sustava prikazana slikom 1 prikazuje različite fizičke elemente organizacije kroz koju se omogućava razmjena informacija/podataka između elemenata organizacije, ali isto tako pruža mogućnost komunikacije sa okolinom. Temeljni cilj IK sustava je pravovremeno dostaviti informaciju na unaprijed definiran način uz što manje troškove.



Slika 1. IK sustav kao podsustav organizacijskog sustava.

Izvor: **[1]**

IK sigurnost je zaštita cjelovitog IK sustava u kojem kolaju različite informacije, stoga pristup pravoj informaciji u pravo vrijeme predstavlja poslovni uspjeh. U sljedećim potpoglavljima raspisuju se osnovni pojmovi vezani za sigurnost IK sustava, te svojstva IK sustava koja su neophodna za definiranje zaštitnih mjera. Također za zaštitu IK sustava, koriste se određeni modeli koji su u nastavku opisani.

2.1. Temeljna načela sigurnosti i zaštite informacijsko – komunikacijskog sustava

Pojam sigurnosti IK sustava u ovom radu obrađuje se na način kakav je danas prihvaćen u razvijenim zemljama svijeta i koji osigurava sukladnost s konceptom IK sigurnosti NATO-a i EU. Sigurnosni IK sustav obuhvaća ljude, procese, organizaciju i tehnologiju. Također se sastoji od uravnoteženog skupa sigurnosnih mjera koje su podijeljene kroz sigurnost provjere zaposlenika, fizičku sigurnost, sigurnost podataka, sigurnost informacija i mrežne komunikacije. Prije opisa i objašnjenja sigurnosnih mjera, standarda, smjernica i mogućnosti

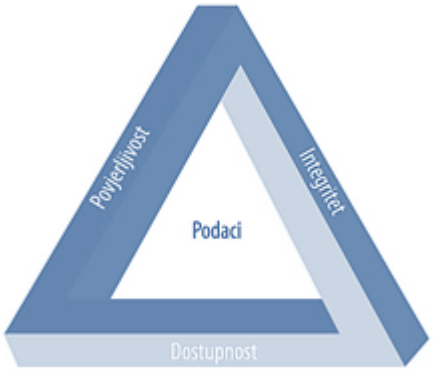
zaštite korporativnog IK sustava potrebno je definirati osnovne pojmove koji se koriste u radu [2], [3], [4]:

- Sigurnost je poslovni proces, usmjeren na smanjenje rizika ili vjerojatnosti nastajanja štete.
- IK sustav je svaki sustav kojim se prikupljaju, pohranjuju, čuvaju, obrađuju, prikazuju, dohvaćaju i isporučuju informacije.
- Korisnici IK sustav su sve pravne i fizičke osobe koje (zaposlenici subjekta, vanjski suradnici, klijenti) sudjeluju u procesima obrade podataka.
- Sigurnost IK sustav je područje IK sigurnosti u okviru kojeg se utvrđuju mjere i standardi IK sigurnosti, te zaštite cjelovitosti i raspoloživosti IK sustava.
- Sigurnost poslovne suradnje je područje IK sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe.
- Zaštita je skup mjera za očuvanje sigurnosti.
- Nadzor je provjera da li je sustav zaštite učinkovit.
- Ovlaštenje je pravo postupanja u zadanim okvirima.
- IK infrastruktura obuhvaća svu infrastrukturu koja utječe na temeljna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili pohranjuju.
- Vlasnici IK infrastrukture odgovorni su za planiranje i implementaciju organizacijskih i tehničkih mjera s važećim propisima IK sigurnosti.
- Pravo pristupa i korištenja IK resursa određuje se isključivo po načelu poslovne potrebe («*need to know*»).
- Sigurnosna akreditacija se odnosi na provjeru niza propisanih mjera i metoda implementiranih u obliku organizacijskih i tehničkih kontrola u poslovne procese određene pravne osobe ili državnog tijela.
- Sigurnosno akreditacijsko tijelo je neovisna pravna osoba, koja vrši provjeru sposobnosti pravnih osoba za provođenje procesa IK sigurnosti u okviru vlastitog poslovnog procesa.
- Sigurnosni certifikat: se odnosi na korištenje pojedinih tržišnih proizvoda u propisanim uvjetima s ciljem sustavne realizacije projekata IK infrastrukture.

2.1.1. Sigurnosna svojstva informacijsko – komunikacijskog sustava

Uz terminologiju važno je spomenuti sigurnosna svojstva IK sustava, koja su neophodna za definiranje zaštitnih mjera, te određenih modela zaštite (Slika 2). Povjerljivost unutar IK sustava podrazumijeva zaštitu sadržaja, informacija ili podataka od bilo kakvog nenamjernog ili namjernog otkrivanja neovlaštenim osobama. Kroz svojstvo integriteta se osigurava konzistentnost podataka i onemogućava bilo koje nedozvoljene promjene sadržaja. Dostupnost se odnosi na sve relevantne informacije, raspoložive unaprijed dozvoljenim entitetima, uz vremensko ograničenje [5]. Osim navedenih temeljnih sigurnosnih svojstva koji

su usko vezani uz implementaciju kontrola, isto tako važne su i sigurnosne kontrole kao što su: autentifikacija, autorizacija, identifikacija, zaštita i mogućnosti praćenja.



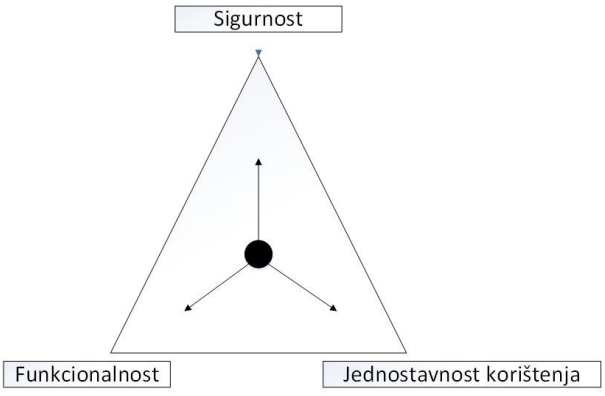
Slika 2. Odnos između povjerljivosti, cjelovitosti i raspoloživosti.

Izvor: **[5]**

Autentifikacija se odnosi na dokazivanje identiteta korisnika, dok se kroz proces identifikacije podrazumijeva predstavljanje entiteta kroz sustav. Pristup pojedinom resursu IK sustava se odobrava ili zabranjuje kroz proces autorizacije. Mogućnost praćenja osigurava praćenje i nadzor akcija unutar sustava, dok pojam zaštite govori sam za sebe [5].

2.1.2. Trijada sigurnosti podataka

Prilikom uspostave željene razine sigurnosti i pri odabiru sigurnosnih metoda potrebno je razmotriti trijadu: Sigurnost / funkcionalnost / jednostavnost korištenja (*Security / Functionality / EaseofUse*) prikazanu slikaom 3.



Slika 3. Trijada Sigurnost/Funkcionalnost/Jednostavnost.

Izvor: **[6]**

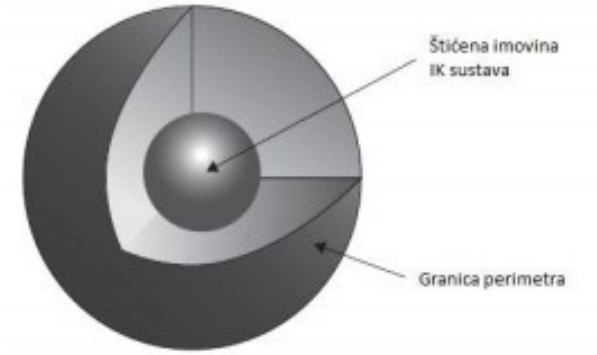
Iz slike 3 je vidljivo kako povećanje jednog elementa trijade ima negativan utjecaj na ostala dva elementa. Potrebno je postići ravnotežu prikazanih elemenata pa je sigurnosne kontrole kroz zaštitni model potrebno primjenjivati sukladno razini osjetljivosti štićenih podataka. Primjena neadekvatnih sigurnosnih kontrola unutar modela može se negativno odraziti na funkcionalnost i jednostavnost korištenja sustava [6].

2.2. Modeli sigurnosti i zaštite informacijsko komunikacijskog sustava

Velika većina korporativnih organizacija koristi sigurnosni model perimetra kako bi zaštitile svoje poslovno okruženje. Tipične obrane uključuju tehnologije poput vatrozida, sustava za otkrivanje upada (*Intrusion Detection System* - IDS), aplikacijskih *proxy* poslužitelja i virtualnih privatnih mrežnih (*Virtaul Private Network* - VPN) poslužitelja. Kada se pravilno konfigurira, obrana dopušta one aktivnosti koje su potrebne za obavljanje poslova. Koristeći model zaštite IK sustava, tehnologija perimetra sprječava, apsorbira ili otkriva napade, čime se smanjuje rizik za kritične IK sustave. IDS detektira napade i upozorava sigurnosno osoblje na vrijeme za provedbu analize i reakcija na napad prije nego što se ugrozi IK sustav. VPN rješenja mogu autentificirati i osigurati siguran kanal za legitimne korisnike. Opće prihvaćanje modela zaštite dogodilo se jer je daleko lakše (i naizgled manje skupo) osigurati jedan opseg nego osigurati veliku količinu aplikacija ili velik broj internih mreža. Postoje dva osnova pristupa odnosno modela koja se raspisuju u sljedećim potpoglavljima [7].

2.2.1. *Lollipop* model

Lollipop model je najčešće korišteni model zaštite IK sustava (Slika 4). Značajka modela je da okružuje objekte od važnosti izgradnjom virtualnog ili fizičkog zida odnosno perimetra za zaštitu IK sustava. Model se može usporediti sa primjerom kuće sa zidovima, vratima i prozorima koji štite imovinu koja se nalazi unutar perimetra zaštite.



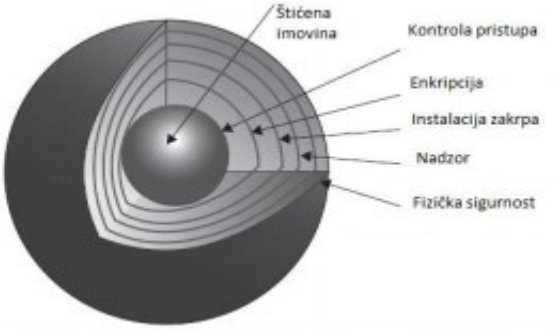
Slika 4. Lollipop model zaštite IK sustava.

Izvor: **[8]**

Potencijalni napadač je u mogućnosti iskoristiti i ugroziti perimetar mreže zbog njegovih nedostataka, posebice iz razloga što ovakav ne štiti u potpunosti IK sustava. Napadač može na mnogo načina iskoristiti mane ovakvog modela jer se IK sustav zaštićuje jednim osnovnim slojem, primjerice vatrozidom (*firewall*) koji samostalno nije u mogućnosti zaustaviti potencijalne, konkretne napade. Također vidljiva je velika prijetnja unutar modela, s obzirom da su svim zaposlenicima i članovima omogućeni pristupi, postoji velika opasnost od prijetnje unutar organizacije [8].Prema tome možemo zaključiti kako *Lollipop* nije dovoljno učinkovit model sigurnosti iako se u većini IK sustava primarno koristi.

2.2.2. Slojeviti model

Slojeviti model (također poznat kao *defense in depth*) je koncept zaštite IK sustava u kojemu se postavljaju višestruki slojevi sigurnosnih kontrola (obrana). Njegova je namjera osigurati zalihost u slučaju neuspjeha sigurnosne kontrole ili eksploatiranja ranjivosti koja može pokriti aspekte osoblja, proceduralne, tehničke i fizičke sigurnosti za trajanje životnog ciklusa sustava (Slika 5).



Slika 5. Slojeviti model zaštite IK sustava.

Izvor: **[8]**

Ovaj model pruža mehanizme zaštite imovine i nakon narušavanja sigurnosti perimetra. Nasljeđuje osobine *Lollipop* modela (zaštita perimetra), ali ih nadograđuje dodatnim mehanizmima zaštite implementiranih unutar perimetra. Zaštitna arhitektura sigurnosti otežava napadaču pristup imovini IK sustava jer mora zaobići ili narušiti sigurnost više mehanizama zaštite implementiranih u sustav. Obrana u dubini izvorno je vojna strategija koja nastoji odgoditi, a ne spriječiti napredak napadača.

Postavljanje zaštitnih mehanizama, procedura i politika ima za cilj povećati pouzdanost IK sustava, gdje višestruki slojevi obrane sprječavaju špijunažu i izravne napade na kritične sustave. Mjere „obrane u dubini“ ne bi trebale spriječiti sigurnosne prekršaje, već i povećati organizacijsko vrijeme za otkrivanje i reagiranje na napad te tako smanjiti i ublažiti posljedice kršenja [8].

2.3. Sredstva zaštite informacijsko – komunikacijskog sustava

Zaštita IK sustava svodi se na zaštitu od neovlaštenog pristupa sustavu, a time i na zaštitu od neovlaštenog pristupa podacima koji se unutar takvog sustava pohranjuju, obrađuju i prenose. Smanjenje vjerojatnosti da prijetnja utječe na rad IK sustava ili da se umanji nastala šteta kad prijetnja iskoristi ranjivost, uvode se sigurnosne kontrole. Postoji podjela na tri različite kontrole. Stoga pod pojmom logičkih kontrola podrazumijevaju se kontrole koje se implementiraju za IK sustav (npr. korisnička imena i zaporke, vatrozidi, enkripcija, logičke kontrole pristupa i sl.). Administrativne kontrole najčešće su različiti dokumenti (politike, pravilnici, procedure i sl.) na području IK sigurnosti koji definiraju pravila za korištenje IK

resursa. Fizičke kontrole su namijenjene fizičkoj zaštiti IK resursa (npr. Video nadzor, alarmni sustav, fizička kontrola pristupa i sl.) [6].

2.3.1. Logičke kontrole zaštite informacijsko – komunikacijskog sustava

Za adekvatnu sigurnost IK sustava podrazumijeva se zaštita perimetra, što predstavlja štićenu granicu lokalne računalne mreže koja sadrži jedan, sve ili kombinaciju mrežnih elementa koje je potrebno uzeti u obzir pri projektiranju sigurne IK-e infrastrukture.

2.3.1.1. Uporaba lozinki i log zapisi

Prilikom definiranja sigurnosnih mehanizama, njihovoj izgradnji i projektiranju potrebno je rukovoditi sa nekim osnovnim principima i operacijama koje su svojstvene za većinu sigurnosnih mehanizama što uključuje uporaba lozinki (npr. određivanje minimalne duljine lozinke, mogućnost posebnih znakova, itd.) [27]. Ponekad je potrebno provoditi promjene lozinki nakon određenog vremenskog razdoblja, isto tako unutar operacijskog sustava (*Operation system* – OS) potrebno je kontrolirati način da se ne dopušta promjena lozinke u već korištenu.

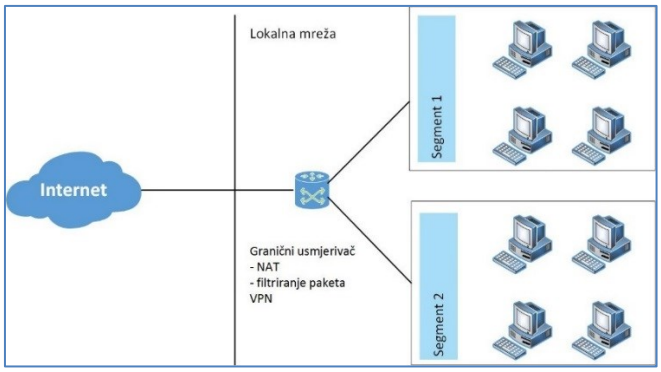
Log zapisi predstavljaju zapise događaja koji su se dogodili u organizaciji (npr. poslužiteljima, mrežnim uređajima, aplikacijama).

2.3.1.2. Uređaji za zaštitu informacijsko – komunikacijske mreže

Uređaji koji se koriste kao sredstva zaštite IK sustava u korporativnom okruženju se opisuju u nastavku.

Vatrozid označava mrežni uređaj, tj. mrežni čvor čija je funkcija zaštita IK sustava, te sadrži skup pravila koja definiraju koji mrežni paketi će se propustit, a koji odbiti. Osnovna funkcionalnost vatrozida je filtriranje mrežnih paketa na mrežnom i transportnom sloju OSI (*Open System Interconnection*) referentnog modela prema unaprijed definiranim pravilima. Fizički vatrozidi su pogodniji za rad u korporativnom okruženju, zbog ogromne količine mrežnog prometa, gdje se zahtjeva i visoka razina kvalitete usluge (*Quality of Service* - QoS) [7]. Vatrozidi se najčešće postavljaju na ulazno/izlaznim točkama lokalne mreže (zaštićene) prema javnoj mreži (nezaštićenoj), tj. između dvije mrežne zone različitog stupnja povjerljivosti. Primjena vatrozida smatra se još uvijek najefikasnijim načinom zaštite perimetra mreže. Kao opcija vatrozida često je korištena strategija pri zaštiti perimetra zvana demilitarizirana zona (DMZ). Web poslužitelju se pristupa putem Interneta, no moguće je pristupiti i putem lokalne računalne mreže [24].

Granični usmjerivač je (Slika 6) mrežni uređaj koji povezuje dvije ili više mreža, a uloga mu je usmjeravanje mrežnog prometa prema, iz ili unutar mreže. Često predstavlja prvu i posljednju crtu zaštite lokalne računalne mreže od zlonamjernih korisnika iako mu to nije primarna funkcija [7].



Slika 6. Usmjerivač na perimetru lokalne mreže.

Izvor: **[23]**

U posljednjih nekoliko godina praksa je objedinjavanje uređaja u jedno sigurnosno rješenje pod nazivom vatrozid sljedeće generacije (*Next Generation Firewall* - NGFW). Postoje razni uređaji koji su u mogućnosti pružiti veću razinu sigurnosti mreže, a to su: IPS, IDS, djelitelj opterećenja (*load balancer*), zatim vatrozidi koji imaju naprednije funkcije od onih u usmjerivaču, *proxy* vatrozidi, itd. Kvalitetna NGFW platforma nužno mora sadržavati karakteristike vatrozida prve generacije, a to uključuje klasifikaciju mrežnog prometa temeljenu na mrežnom i transportnom OSI sloju, NAT funkciju (*Network adress translation*), VPN. Uz to uključuje mogućnost klasifikacije prometa prema specifičnostima aplikacija, detaljni pristup zaštiti na aplikacijskoj i korisničkoj razini, integrirani IPS, visoku razinu dostupnosti i skalabilnosti što uključuje dijeljenje prometnog opterećenja i fizičku redundanciju [24].

Primarna funkcija sustav detekcije neovlaštenog upada (IDS) je analiza mrežnog prometa i identifikacija prijetnji detekcijom sumnjivih mrežnih paketa koji su karakteristični za raznovrsne metode napada. Uloga IDS-a osim identifikacije napada i sumnjivih aktivnosti, mogu se iskoristiti u identifikaciji slabosti i ranjivosti štićene mreže u svrhu poduzimanja potrebnih aktivnosti za njihovo uklanjanje. IDS u kombinaciji sa drugim elementima zaštite perimetra, može zaustaviti trenutno aktivne napade [24].

Sustavi zaštite od neovlaštenog upada (IPS) bazirani su na prethodno opisanim sustavima detekcije neovlaštenog upada. Postoji razlika između dva sustava koja je vidljiva u mogućnostima IPS-a, gdje IPS osim praćenja mrežnih paketa, poduzima aktivne radnje za sprječavanje napada. IPS propušta mrežni paket onda kada ne odgovara definiranim pravilima IPS-a koji su bazirani na već poznatim anomalijama mrežnih paketa. Možemo reći da IPS aktivno sudjeluje u zaštiti IK sustava [24].

2.3.1.3.Virtualne mreže

Bitan segment zaštite koje je potrebno izdvojiti predstavlja virtualna privatna mreža (VPN) koja je definirana kao kontrolirano komunikacijsko okruženje koje koristi javnu komunikacijsku infrastrukturu s ciljem povezivanja dviju ili više privatnih mreža. Također ona

predstavlja jeftiniju alternativu zakupljenim vodovima uz približnu razinu sigurnosti. Temeljni cilj VPN-a je osigurati komunikacijski kanal uz pomoć enkripcije podataka [24].

Često je potrebno segmentirati korisnike ili zaposlenike koji pripadaju istom sektoru te se iz tog razloga kreira virtualna lokalna računalna mreža (*Virtual Local Area Network* - VLAN). Uz pomoć VLAN-a moguće je grupirati korisnike ili zaposlenike bez obzira na njihovu lokaciju. Također uz pomoć VLAN-a moguće je lakše razmjenjivati povjerljive informacije.

2.3.1.4. Kontrola pristupa

Uz VPN definiraju se prava za kontrolu pristupa (*Access Control*) što ukazuje na dozvolu ili zabranu izvršavanja određenih operacija subjekta nad objektima IK sustava. Pod kontrolom pristupa obuhvaćaju se resursi IK sustava poput datoteka ili sklopovske opreme, korisnika, aplikacija ili procesa koji pokušava ostvariti pristup, te operacije/akcije koje se izvršavaju između korisnika i resursa IK sustava. Kao i prethodno definirano, kontrola pristupa se također temelji na aktivnostima: identifikaciji, autentifikaciji i autorizaciji [24].

2.3.2. Fizičke kontrole zaštite informacijsko - komunikacijskog sustava

Ovisno o vrsti resursa uz sigurnosne kontrole, gotovo uvijek je moguće, pa i potrebno primijeniti i fizičke mjere zaštite. Na taj način (IK) resursom se smatraju svi resursi nužni za rad IK sustava. U sljedećim naslovima opisati će se najčešće korištene fizičke mjere zaštite.

2.3.2.1. Građevine i prostorije za zaštitu informacijsko – komunikacijskog sustava

Počevši od prirodnih prijetnji i prijetnji iz okoliša, preko ljudskih prijetnji sve do društveno uzrokovanih prijetnji građevine i okoliš predstavljaju prvu razinu zaštite od svih vrsta prijetnji. Fizičke kontrole koje se uvode za zaštitu građevina i okoliša su ograde, video nadzor konstrukcija zgrade, zidovi i podovi, vrata, prozori, infrastrukturne instalacije te ostale kontrole (patrole, zaštitari i trenirani psi mogu imati visok efekt odvraćanja potencijalnih provalnika, vandala i drugih zlonamjernih pojedinaca i grupa). Prostorije je moguće zaštitit upotrebom identifikacijskih oznaka (magnetske ili pametne kartice i sl.), te korištenjem naprednijih, centraliziranih i IT upravljanih sustava [24].

2.3.2.2. Sustavi fizičke zaštite informacijsko – komunikacijskog sustava

Sustavi za detekciju neovlaštenih aktivnosti i uzbunjivanje/alarmni sustavi u velikoj mjeri služe za detekciju neovlaštenih aktivnosti, te otkrivanje pokušaja provale. Sustavi za detekciju su npr. elektromehanički sustavi, fotoelektrični sustavi, inteligentni sustavi za analizu slike i detekciju pokreta i ostali sustavi koji se temelje na detekciji akustičnih promjena, vibracija, magnetskog polja, itd. [24].

Za sigurnost IK infrastrukture potrebno je provesti ispravno kabliranje. Neispravno provedeni kablovi mogu uzrokovati probleme u radu, odnosno smanjenu propusnost komunikacijskog kanala ili njegov neispravan rad. Najčešće se koriste bakreni *ethernet* kablovi.

Sva komunikacijska infrastruktura koja nije smještena u sistemskoj sobi trebala bi biti smještena u posebne komunikacijske ormare i zaključana. Sustavi za zaštitu od požara predstavljaju sigurnosnu mjeru od važnosti koja se u raznim oblicima primjenjuje u gotovo svim organizacijama. Naravno da je danas većina organizacija ovisna o električnoj energiji i ona potpuno ovisi o IT sustavima i podršci koju one pružaju. Svaki prekid u napajanju el. energijom uzrokuje štete. Iz tog razloga potrebno je provesti ispravno kabliranje, koristiti uređaj kao neprekidni izvor napajanja (*Uninterruptable Power Supply* - UPS) – i generatore (koji se koriste u slučaju duljih nestanka struje) [7].

Računalna i mrežna - komunikacijska oprema predstavlja srce IK sustava te ju, bez obzira na vrstu organizacije, trebamo zaštititi. Sistemske sobe su posebne prostorije u kojima je smještena mrežna IK oprema. Ona podrazumijeva niz sigurnosnih kontrola, a osnovna funkcija sistemske sobe je osigurati adekvatnu razinu zaštite svim uređajima koji se u njoj nalaze [24].

2.3.2.3. Metode zaštite fizičkih medija

Tijekom putovanja prijenosna računala se trebaju prenositi kao ručna prtljaga te je pogodno korištenje sigurnosnih brava ili lokota. Prijenosna računala se ne bi smjela nikada ostavljati u javnim prostorima bez nadzora. Postoje također i senzori za detekciju pokreta (oglašavanje glasnim alarmom) koja su danas već ugrađena u modernijim računalima ili ih je potrebno dodatno ugraditi. Bez obzira na fizičke mjere, prijenosna računala bi trebala biti zaštićena korištenjem neke od metoda enkripcije [24].

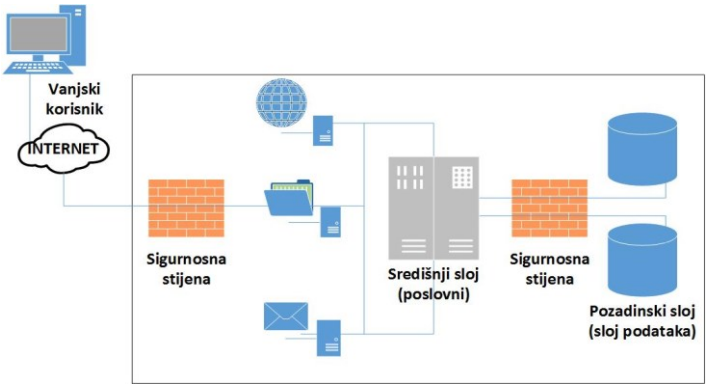
Papirnati i elektronički mediji također igraju bitnu ulogu u zaštita IK sustava (USB memorije/diskovi, optički CD/DVD mediji, magnetne trake itd.). Potrebno je osigurati korištenu razinu zaštite tijekom njihova životnog vijeka, pa tako i prilikom povlačenja iz upotrebe (sigurnog uništenja) s obzirom da se na takvim medijima pohranjuju ili prenose važne informacije od poslovnog značaja. Također postoje specijalizirani uređaji za demagnetizaciju/sigurno uništavanje [24].

3. Sigurnosna strategija unutar korporativnog okruženja

Promjenjive i nestabilne okolnosti unutar korporativnog okruženja stvaraju potrebu za formuliranjem i implementacijom kvalitetne strategije. Pod pojmom sigurnosna strategija podrazumijeva se uspostavljanje dugoročnih ciljeva, određivanje pristupa za njihovo ostvarivanje, te implementacija sigurnosnih rješenja, kontrola i vrednovanje ciljeva. Sigurnosna strategija u organizaciji kreira se istovremeno s korporativnom strategijom, i kad je ona definirana za jednu organizaciju ne može se primijeniti na neku drugu, jer različite organizacije imaju različite poslovne potrebe i ciljeve. Sigurnost zato predstavlja najvažniji dio sigurnosne strategije i kao takva mora biti u skladu s ciljevima organizacije i poslovnom strategijom. Stoga sigurnosna strategija unutar korporativnog okruženja predstavlja ključ poslovnog uspjeha. Zbog različitih potreba i ciljeva organizacije sigurnosna strategija unutar korporativnog okruženja može se definirati kroz arhitekturu sigurnosnog sustava, te kroz „uspostavu sustava za upravljanje informacijskom sigurnošću“ koji su detaljnije raspisani u nastavku.

Općenito se strategija sigurnosti IK sustava odnosi na sigurnost koji uključuje tehničku arhitekturu, mrežu, komunikacije i računala dok strategija sigurnosti korporativnog IK sustava podrazumijeva puno šire područje što uključuje izgradnju, implementaciju i korištenje IK sustava, što se automatski povezuje sa organizacijom tvrtke i poslovnim procesima, zakonima i cjelokupnim okruženjem [9]. Prema tome definirani su opći ciljevi strategije unutar korporativnog okruženja:

- Kvalitetni sustavni pristup usklađen sa zakonodavnim okvirom i međunarodnim obvezama te globalnim trendovima IK sigurnosti.
- Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti IK sustava.
- Uspostavljanje učinkovitijeg mehanizma pristupa, obrade i razmjene informacija/podataka potrebnim za osiguravanje više razine sigurnosti IK sustava.
- Jačanje svijesti o sigurnost i zaštiti IK sustava unutar korporativnog okruženja kroz edukaciju zaposlenika, te provedbu različitih aktivnosti usmjerenih osvješćivanju korporativnog okruženja kroz sigurnosne domene.
- Poticanje razvoja e-usluga kroz razvoj povjerenja korisnika u e-usluge definiranjem odgovarajućih minimalnih sigurnosnih zahtjeva.
- Poticanje istraživanja i razvoja u svrhu aktiviranja potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora.
- Sustavni pristup koji omogućava učinkovit prijenos znanja i koordiniranu razmjenu, ustupanje i pristup potrebnim podacima između različitih nacionalno nadležnih tijela, institucija i sektora društva, a s ciljem prepoznavanja i stvaranja sposobnosti za uspješno sudjelovanje u poslovnim aktivnostima u korporativnom okruženju.



Slika 7. Troslojna arhitektura IK sustava s pristupnim, središnjim i pozadinskim slojem.

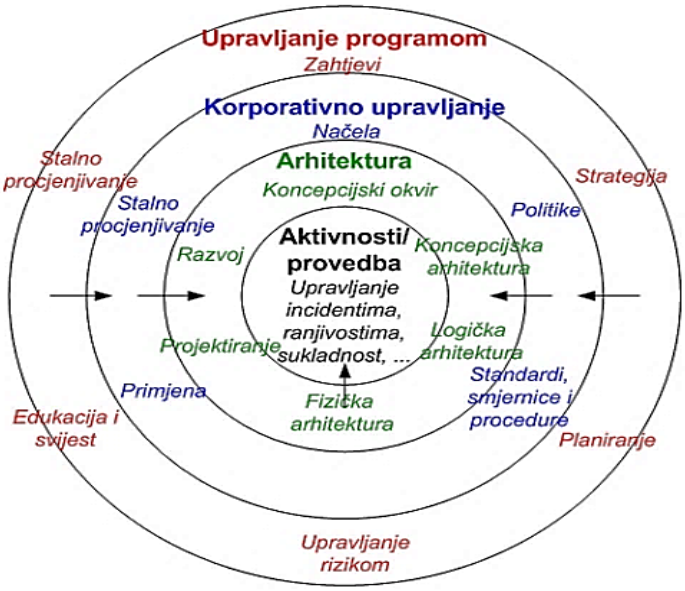
Izvor: **[7]**

Razmjenu informacija i podataka između dva ili više entiteta osiguravaju brojni sustavi komuniciranja. Iz tih razloga ovaj rad se ograničava na IK sustav u kojem se koristi suvremena IK tehnologija za obradu, prijenos i korištenje raspoloživih informacija za potrebe poslovnog odlučivanja i upravljanja sigurnosnom strategijom organizacije. Prema istraživanju [10], 51% hrvatskih korporacija ne razvija sustav IK sigurnosti. To objašnjava da dio profita treba investirati u sustave poslovne sigurnosti iz razloga što IK sigurnost slovi kao jedna od ključnih sigurnosnih potreba. Otvorenost prema mreži Interneta i kompleksnost IK sustava, tj. potreba za javnim IK uslugama, dovodi do primjene višeslojne arhitekture IK sustava (tipično dvoslojne i troslojne) (Slika 7).

3.1. Arhitektura sigurnosnog sustava na korporativnoj razini

Tokom vremena globalne ekonomije, stalne ekspanzije i promjene rizika kojom su konstantno izložene organizacije, uspostavljanjem suradnje među partnerima i *on - line* trgovine, sigurnost IK sustava predstavlja sve više poslovni problem za koji je potrebno omogućiti i unaprijediti poslovanje. Uloga sigurnosti IK sustava trenutno još nije dovoljno dobro definirana u mnogim organizacijama pogotovo iz razloga što mnoge organizacije vide IK sigurnost kao mjesto troška. Može se dokazati da organizacije koje konstantno ulažu, prate inovativna rješenja zaštite i ispravno upravljaju sigurnošću IK sustava ostvaruju kvalitetne, učinkovite i racionalne poslovne ciljeve. Prema sigurnosnoj arhitekturi uspostavlja se slojeviti pristup čime se bolje definira složenost sigurnosnog IK sustava. Primarna namjena uspostavljanja svake arhitekture sustava jest osigurati konzistentnost u dizajnu IK sustava.

Na slici 8 je prikazana veza između koncentričnih krugova koji predstavljaju segmente modela korporativne sigurnosne arhitekture razrađene u [12]. Kada bi se podnijeli novi zahtjevi kroz segment upravljanja programom, generirali bi se novi principi, upravljanje, politika i standardi, kao i primjena nove tehnološke arhitekture. Također se tokom procesa implementacije novih standarda i arhitekture (koja je usmjerena prema IK sustavu) uzrokuje stvaranje novih sigurnosnih procesa ili drugih sposobnosti.



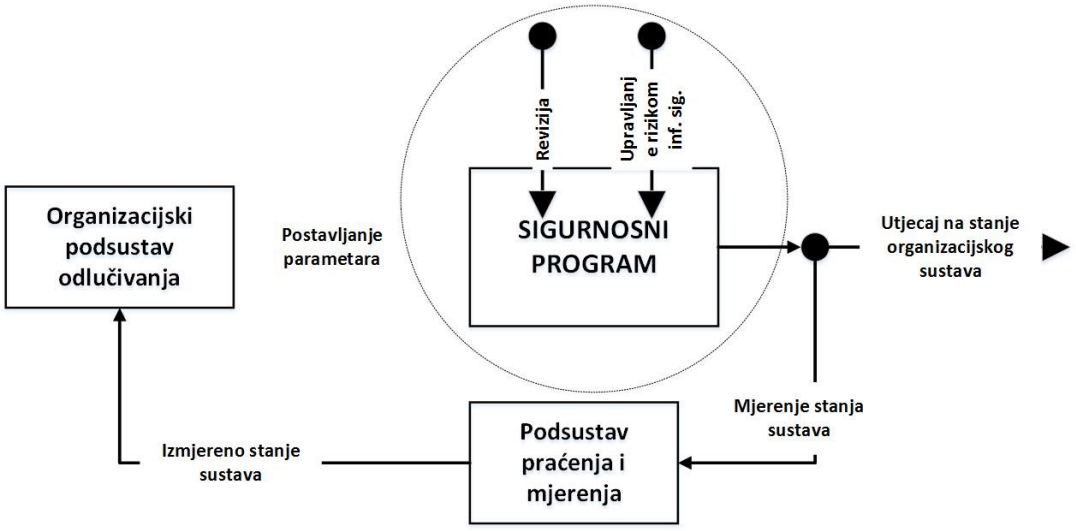
Slika 8. Model programa sigurnosti na korporativnoj razini.

Izvor: **[12]**

U nastavku se provode aktivnosti upravljanja incidentima i ranjivostima, te definira sukladnost sa elementima organizacijske arhitekture.

3.1.1. Korporativni model

Korporativni model prikazan slici 9 prikazuje skup odgovornosti koje provodi organizacijska uprava. Organizacijska uprava definira sigurnosni program na temelju kojeg želi kontrolirano upravljati rizicima i zaštiti organizacijsku imovinu. Također želi se pružiti podrška za realizaciju poslovnih ciljeva organizacije.



Slika 9. Model korporativnog upravljanja informacijskom sigurnošću.

Izvor: **[8]**

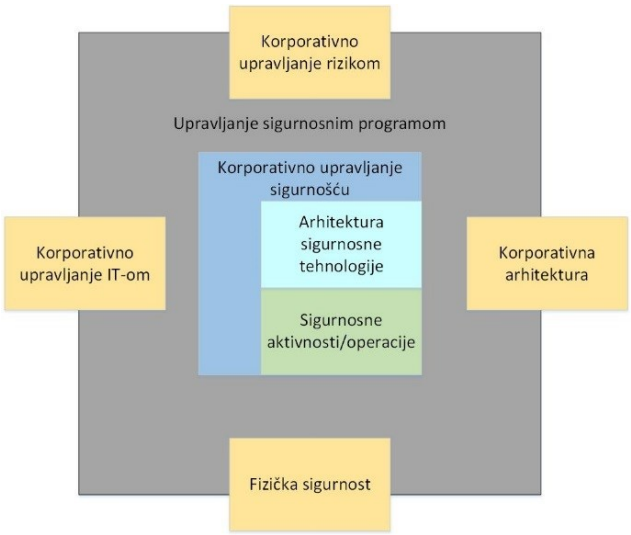
Unutar korporativnog modela provode se mjere za ublažavanje rizika i smanjenja utjecaja na kritične točke. Uz to provode se mjerenja stanja sustava, odnosno nadzor i izvještavanje o potencijalnim nedostacima i poteškoćama. Stoga model korporativnog

upravljanja usmjerava IK sigurnost uz primjenu pravila i procesa za kvalitetno provođenje sigurnosnih programa prema ciljevima organizacije.

3.1.2. Korporativno upravljanje sigurnošću

Zbog tržišne konkurencije, stalne potražnje, profitabilnosti i protoka novca, te zadovoljenje zakonskih okvira i osiguranje poslovnog ugleda, sigurnost IK sustava može biti od presudne važnosti. Korporativno upravljanje stoga predstavlja točno definirani skup odgovornosti i praksi koje provodi uprava organizacije s ciljem pružanja strateškog usmjeravanja poslovanja. Takvim pristupom se želi osigurati da ciljevi budu dostignuti, uz provjeru odgovarajuće upravljanih rizika i odgovornog korištenja korporacijskih resursa [11].

Na slici 10 prikazane su na vanjskom rubu četiri korporativne komponente s kojima sigurnosna arhitektura mora biti na određeni način usklađena: korporativno upravljanje rizikom, korporativno upravljanje IT-om (*Information Technology*), korporativna arhitektura i fizička sigurnost. Korporativno upravljanje na ovaj način usmjerava IK sigurnost, pri čemu mora biti implementirano sa strukturom, pravilima i procesima koji će odgovarajuće usmjeravati sigurnosni program prema ciljevima definiranim na poslovnoj razini. Ovaj koncept je usko povezan s regulativnim obvezama odgovornosti uprave, koje podrazumijevaju obvezu uprave organizacije da kontinuirano procjenjuju i analiziraju rizike s kojima se organizacija suočava. Sve navedeno se provodi u svrhu zaštite zaposlenika, partnera, kooperanata i klijenata organizacije, od potencijalnih gubitaka u poslovanju [11].

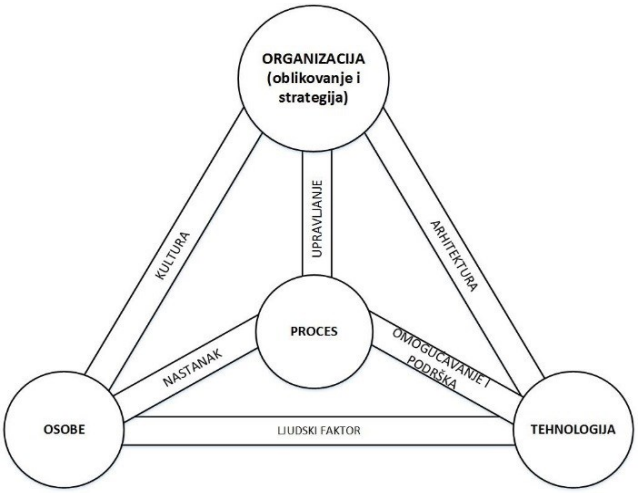


Slika 10. Komponente korporativne sigurnosne arhitekture.

Izvor: **[11]**

Struktura poslovnog modela (Slika 11) upravljanja IK sigurnošću uključuje dodatni element organizacije (oblikovanje i strategija), u odnosu na zastupljene elemente osoba, procesa i tehnologije. Pored toga, model uključuje i dinamičke međuodnose između ova četiri elementa [14]. Model se isključivo orijentira prema poslovnom rješenju upravljanja IK sigurnošću. Potpunost i dinamičnost modela dokazuje da IK sigurnost treba biti pro-aktivna i

predvidiva. Struktura poslovnog modela u osnovi predstavlja primjenu teorije sustava, odnosno sveobuhvatnog pristupa problematici IK sigurnosti na najvišoj organizacijskoj razini, da bi se upravljanje IK sigurnošću provodilo temeljem ulaznih veličina proizašlih iz poslovnih ciljeva. Navedeni model se sastoji od četiri glavna elementa koja su usko povezana sa šest dinamičkih poveznica (organizacijska kultura, nastajanje, arhitektura, omogućavanje i podrška, ljudski faktor, korporativno upravljanje).



Slika 11. Struktura poslovnog modela.

Izvor: **[14]**

Ovakav model ne zamjenjuje izvore najbolje prakse sigurnosnih programa, ali nudi pogled na aktivnosti programa IK sigurnosti u puno širem kontekstu. Model svojim pristupom omogućava integraciju različitih komponenata koje bi se inače tretirale nepovezano iako u suštini čine jedinstvenu organizacijsku cjelinu. Navedeni model se upotrebljava unutar zakonskih i regulatornih zahtjeva, za globalizaciju, rast i proširenje. Programi IK sigurnosti trebaju uzeti u obzir da su organizacija, njezino osoblje, procesi i tehnologija međusobno povezani i da međusobno djeluju [14]. Vođenje i upravljanje organizacijom, kultura, ljudski faktor i arhitektura podupiru ili otežavaju mogućnost organizacije da zaštiti svoje IK sustave i upravlja rizikom koji dovodi do sigurnosti IK sustava. Drugim riječima IK sustav djeluje unutar određenog poslovnog sustava, te mu na taj način omogućava da vrši komunikaciju unutar sebe i sa svojom okolinom. IK sustav preuzima informacije, obrađuje ih i prerađene prezentira poslovnom sustavu ili okolini. Dakle, IK sustav predstavlja podsustav poslovnog sustava.

3.2. Upravljanje sigurnošću informacijsko – komunikacijskog sustava

Svaka organizacija posjeduje sustav upravljanja poslovanjem, te obuhvaća sve politike koje se odnose na nadzor i upravljanje u svrhu postizanja ciljeva organizacije. Segment takvog sustava upravljanja koji se odnosi na IK sigurnost je sustav upravljanja informacijskom sigurnošću (*Information Security Management System* – ISMS). ISMS definira instrumente i metode koje je potrebno primijeniti za jasno upravljanje (planiranje, usvajanje, implementaciju, nadzor i unaprjeđenje) procesima i aktivnostima s ciljem postizanja željene

razine IK sigurnosti [15]. Proces upravljanja IK sigurnošću podrazumijeva trajno usavršavanje zakonskih pravila uzimajući u obzir sigurnosne politike, provedbene uredbe, pravilnike i smjernice, pa do detaljnih procedura postupanja pojedinih tijela državne uprave. Upravljanje IK sigurnošću stoga obuhvaća postupke kao što su identifikacija resursa, klasifikacija podataka, upravljanje rizikom, planiranje i implementacija mjera, postupci certifikacije osoblja i uređaja, postupci akreditacije sustava za rad, nadzor implementacije i učinkovitosti mjera i postupaka, praćenje IK sustava tijekom životnog ciklusa, sustavna edukacija i sl.

Dobro organiziran ISMS jedne organizacije ima preventivni utjecaj na ukupno stanje sigurnosti te čini temelj za razvoj suvremenog IK društva. Procesno rješenje za ISMS koje je korišteno u ISMS familiji normi, a koje je bazirano na principu upravljanja je općenito poznato kao (*Plan-Do-Check-Act* - PDCA) proces (*Deming-ov* ciklus) prikazan u tablici 1.

Tablica 1. Procesni pristup (PDCA).

Plan (uspostavljanje ISMS)	*Uspostavljanje* ISMS *politike, ciljeva, procesa i procedura važnih za upravljanje rizikom i povećanje IK sigurnosti kako bi dali rezultate u skladu s ukupnom politikom i ciljevima organizacije*
Do (implementacija i pokretanje ISMS)	*Implementiranje i pokretanje* ISMS *politike, kontrola i procedura*
Check (nadgledanje i kontrola ISMS)	*Procjena i gdje je primjenjivo, mjerenje performansi procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo te izvještavanje uprave o rezultatima.*
Act (održavanje i unapređivanje ISMS)	*Izvođenje korektivnih i preventivnih akcija zasnivanih na rezultatima* ISMS *procjene (audita) i procjene uprave ili ostalim bitnim informacijama, da bi se* ISMS *kontinuirano usavršavao*

Izvor: **[16]**

Prema [16], osnovni cilj ISMS-a je implementacija prikladnih metrika za eliminaciju ili smanjenje utjecaja, koje različite prijetnje i ranjivosti mogu imati na organizaciju. Pri tom ISMS omogućava implementaciju željenih kvalitativnih karakteristika usluga koje organizacija nudi (npr. dostupnost usluge, očuvanje povjerljivosti i integriteta podataka, itd.). Razlika korporativnog upravljanja IK sigurnošću u odnosu na ISMS je u tome da se sigurnost ovdje promatra integrirano u funkciji poslovnih ciljeva organizacije. Najočitija prednost ovakvog pristupa jest opravdanost sigurnosnih investicija, jer se ciljevi politike IK sigurnosti usmjeravaju prema ciljevima na poslovnoj razini.

4. Zakonska regulativa, politika i standardi informacijske sigurnosti

Zbog tržišne konkurencije, stalne potražnje, profitabilnosti i konstantnog protoka novca za zadovoljavanje zakonskih okvira i osiguranje poslovnog ugleda, sigurnost IK sustava može biti od presudne važnosti. Iz tog razloga u Europi je poduzeto nekoliko inicijativa za definiranje sigurnosnih standarda [17]:

- Godine 1990. (*Commercial Computer Security Center* – CCSC) je publicirao *Criteria for Security product Evaluation for Information Systems*, poznata kao *White Books.*
- Godine 1947. osnovana je Međunarodna organizacija za standardizaciju (*International Standards Organization* – ISO) čija je zadaća priprema, prihvaćanje i objavljivanje međunarodnih normi koje pomažu razvoju gospodarstva i uklanjanju prepreka međunarodnoj trgovini. Međunarodna organizacija za standardizaciju je distribuirana okolina gdje sigurnosni zahtjevi trebaju biti strogo definirani te je ona odgovorna za definiranje sigurnosnih standarda.
- Europska udruga proizvođača računala *(Euorpiean Computer Manufactures Association* - ECMA) je grupa od 50 europskih proizvođača koja je također uključena u definiranje sigurnosnih standarda od 1988 godine. Rad ECMA-e je prvenstveno orijentiran na definiranje mrežne sigurnosne politike za nadzor pristupa objektima (računala/aplikacije) različitih domena.

Druge inicijative uključuju grupu Europskih i Američkih (*United States of America* – USA) proizvođača u definiranju standarda za otvorene sustave koji su bazirani na sigurnosnim standardima. Američki nacionalni institut za norme (*American National Standards Institute* - ANSI) je odgovoran za odobrenje standarda, a *International federation for Information processing* (IFIP) okuplja multinacionalne profesionalne i tehničke organizacije koje rade u području IK sustava [19].

Sigurnosnu akreditaciju nacionalnih i međunarodnih IK sustava u RH provodi Zavod za sigurnost informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost koji će u sljedećem potpoglavlju biti detaljnije opisani. Uz zakonodavna tijela u nastavku su opisane i temeljne norme koje se koriste da bi se što kvalitetnije zaštitio IK sustav, te sigurnosna politika koja predstavlja primarni i početni okvir na temelju kojeg se dalje razvijaju sigurnosni i zaštitni mehanizmi IK sustava u poslovanju.

4.1. Zakonodavna tijela i radni okvir upravljanja sigurnošću informacijsko – komunikacijskog sustava

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo zaduženo za poslove tehničkog područja informacijske sigurnosti državnih tijela. Spomenuti poslovi obuhvaćaju standarde sigurnosti IK sustava, sigurnosne akreditacije IK sustava, upravljanje kripto-materijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na ugroze sigurnosti IK sustava. Osim navedenoga, ZSIS-ova zadaća je i reguliranje

standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima i njihovo trajno usklađivanje s međunarodnim standardima i preporukama te sudjelovanje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava. Kao tijelo za sigurnost akreditacije (*Security Accreditation Authority* - SAA) preuzima odgovornost za provedbu sigurnosne akreditacije IK sustava u kojima se koriste klasificirani podaci [3].

Ured Vijeća za nacionalnu sigurnost (UVNS) središnje je državno tijelo za IK sigurnost, koji koordinira, usklađuje i nadzire primjenu mjera i standarda IK sigurnosti u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti IK sustava i sigurnosti poslovne suradnje. UVNS ostvaruje i koordinira međunarodnu suradnju u području IK sigurnosti te odlukom Vlade u ime Republike Hrvatske zaključuje međunarodne sigurnosne ugovore za zaštitu klasificiranih podataka [3].

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) provodi postupak analize tržišta zbog procijene djelotvornosti tržišnog natjecanja, čiji je osnovni cilj utvrditi postoji li na tom tržištu operator ili više operatora koji imaju značajnu ili zajedničku značajnu tržišnu snagu na mjerodavnom tržištu. HAKOM je nadležan za praćenje i poticanje razvoja mreža sljedeće generacije (*Next Generation Networks* - NGN), pri čemu posebno vodi računa o otvorenosti, neutralnosti te pristupnim tehnologijama i uslugama. Radi postavljanja kvalitetnijih regulatornih okvira potrebnih za razvoj otvorenog pristupa, osobito se pazi da poslovni modeli budu prilagođeni vertikalnoj, slojevitoj arhitekturi radi minimiziranja potencijalnih diskriminacija u pružanju maloprodajnih usluga [18].

Agencija Europske unije za mrežnu i informacijsku sigurnost (*European Network and Information Security Agency* - Enisa), stručni je centar za IK sigurnost u Europi. ENISA pomaže EU-u i njezinim državama članicama da se bolje opreme i pripreme za sprečavanje, otkrivanje i odgovor na probleme IK sigurnosti. ENISA pruža praktične savjete i rješenja za javni i privatni sektor u državama članicama EU-a te za institucije EU-a. ENISA također objavljuje izvješća i studije o pitanjima IK sigurnosti. ENISA pomaže u sastavljanju nacrta politika i prava EU-a u području IK sigurnosti [19].

Radni okvir kontrolnih ciljeva informiranja i srodne tehnologije (*Control Objectives for Information and related Technology* - COBIT) opisuje način provedbe upravljanja IK tehnologijama. Poslovni procesi mnogih organizacija uvelike ovise o pouzdanoj i dobroj funkcionalnosti njihovih IK sustava. COBIT sadrži 5 područja, 37 ključna informacijska procesa, više od 300 detaljnih IK provjera, 18 aplikacijskih i 6 procesnih provjera i funkcionira prema unaprijed definiranim principima. COBIT *Framework 5* (radni okvir) omogućuje optimizaciju IK resursa kao što su programski paketi, informacije, infrastruktura i ljudski resursi. COBIT preporuča praksu koja je produkt rada stručnjaka i dobre prakse, primjenjive u bilo kojoj organizaciji. Radni okvir definira generički model IK procesa koji se mogu pojaviti u jednom IK sustavu. Na taj način pripisuje model rada IK sustava poslovnom i informacijskom menadžmentu. Za uspješno upravljanje njime, menadžment mora primijeniti potrebne

provjere koje su propisane za sve COBIT-om definirane IK procese. Budući da su ciljevi primjene nadzora unutar COBIT-a organizirani po IT procesima, tada okvir zapravo daje stvarnu vezu između primijenjenih provjera, procesa i upravljanja IK sustavima [20].

TM Forum je globalno trgovinsko udruženje koje pruža radne okvire, standarde, alate i praktične savjete koji pomažu organizacijama u smanjenju troškova i rizika poslovanja, povećavaju poslovnu agilnost te pospješuju rast poslovanja općenito. Objedinjuju više od 85000 stručnjaka i više od 900 članova organizacija s ciljem razmjene iskustava, kolaboracije i brzog rješavanja ključnih poslovnih izazova uključujući IT transformaciju, optimizaciju poslovnih procesa, analizu velikih količina podataka, upravljanje *cloud* okruženjem, upravljanje korisničkim iskustvom i IK sigurnošću. *TM Forum* je 2011. godine razvio i publicirao model upravljanja sigurnošću s ciljem upotpunjavanja skupa rješenja pod nazivom (*Frameworx)* zajednički okvir [21].

4.2. Sigurnosna politika

Sigurnosna politika dio je sustava upravljanja sigurnošću IK sustava. Svrha sigurnosne politike je da se definiraju neprihvatljivi i prihvatljiv načini ponašanja, tj. da se jasno raspoređuju odgovornosti i zadatci, te da se propišu sankcije u slučaju nepridržavanja. Sigurnosna politika može se definirati kroz dva primjera. Prvi primjer se odnosi na kopiranje već definirane sigurnosne politike, odnosno implementiranje jedne od normi. Ovakav primjer prikladan je za organizacije koje nemaju dostatna sredstva za detaljnu sigurnosnu politiku niti imaju potrebu za njom. Drugi primjer provođenja sigurnosne politike je detaljno proučavanje IK sustava, definiranje mogućih potencijalnih kritičnih točaka, te provedba analize kako će se ona zaštiti uz testiranje cjelokupne sigurnosti sustava. Sigurnosna politika definirana ovakvim oblikom pruža veću sigurnost, ali zbog toga ima i puno veću cijenu [9]. Sigurnosna politika unutar korporativnog okruženja prilagođava se potrebama, te nije jednaka za sve. Sigurnosnu politiku predstavlja službena izjava ili plan organizacije koji obuhvaća ciljeve, smjernice i prihvatljive postupke. Ona uključuje sljedeće zahtjeve [11]:

- potrebno je poštovati pravila definirana sigurnosnom politikom,
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija,
- usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike i
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima i smjernicama.

Zbog korisnika kojima je sigurnosna politika namijenjena i koji moraju s njom biti upoznati potrebno je definirati politiku tako da bude kratka i jasna, napisana na način da ju korisnici mogu razumjeti. Politiku napisanu opširno i stručnim jezikom običan korisnik ne razumije i površno ju ili nikako ne analizira, pa je stoga ne može niti primijeniti.

4.2.1. Organizacija sigurnosne politike

Organizacija IK sigurnosti predstavlja dio standarda koji je namijenjen primarno za osobe odgovorne za sigurnost i zaštitu IK sustava unutar korporativnog okruženja. Na temelju njihovih odluka, stavova, i koordinacije sigurnosti postižu se unaprjeđenja i umanjuju rizici prilikom procesa poslovanja. U sljedećim potpoglavljima detaljnije je opisana organizacija sigurnosne politike [27].

4.2.1.1. Zadaća voditelja sigurnosti

Unutar organizacije definiraju se zadaci voditelja sigurnosti (*Chief Security Officer* – CSO) koji aktivno provodi sigurnosnu politiku svojim čvrstim stavom u pogledu sigurnosti, pružajući potporu svim potrebnim zahtjevima za uspostavu sigurnosti te strogo kažnjavajući one koji je se ne pridržavaju. Uz to potrebno je formulirati i provjeravati sigurnosnu politiku, provjeravati efikasnost implementirane politike, te osigurati podršku za sigurnosne inicijative i resurse koje iziskuje IK sigurnost. Također rukovoditelj treba odrediti specifične uloge i odgovornost za IK sigurnost unutar organizacije, kao i osigurati implementaciju sigurnosnih kontrola u skladu s organizacijom i odrediti postoji li potreba za savjetodavnim stručnjakom IK sigurnosti [27].

4.2.1.2. Koordinacija informacijsko – komunikacijske sigurnosti

Unutar velikih organizacija poželjno je da se formira tim za koordinaciju, a oni predstavljaju sve relevantne dijelove organizacije. Takav tim dogovara specifične uloge i odgovornosti za IK sigurnost cijele organizacije, te dogovara metode i procese vezane za sigurnost (npr. za upravljanje rizikom, klasifikaciju informacija). Tim isto tako osigurava da je sigurnost dio procesa planiranja i razvoja, zatim procjenjuje valjanost sigurnosnih kontrola i koordinira uvođenje kontrola u novim IK sustavima i servisima. Važno je da tim promovira potporu IK sustava sigurnosti kroz cijelu organizaciju, te pregledava izvješća o sigurnosnim incidentima. Kvalitetan tim se sastoji od organizacijskih sigurnosnih stručnjaka koji definiraju uslugu informiranja i savjetovanja prema svim sigurnosnim aspektima, koristeći vlastita znanja i vanjske savjete. Kvaliteta procjene prijetnji i savjetovanja sigurnosnih stručnjaka o sigurnosnim kontrolama može odrediti učinkovitost zaštite i sigurnosti IK sustava [27].

U skladu sa sigurnosnom politikom nužna je i podjela odgovornosti. Skup odgovornosti koji utječe na zaštitu resursa i na izvršavanje sigurnosnih procesa trebaju biti jasno definirani i dokumentirani. Unutar sigurnosne politike se pružaju smjernice za dodjelu sigurnosnih uloga i odgovornosti u organizaciji. Također treba jasno definirati lokalnu odgovornost za pojedine dijelove IK sustava i fizičke imovine. Vlasnici IK imovine mogu prenositi svoje sigurnosne odgovornosti na pojedinačne članove i vlasnik ima konačnu odgovornost za sigurnost imovine [27].

4.2.2. Dokumenti i doprinos sigurnosne politike

Dokumenti sigurnosne politike trebaju biti odobreni od strane sigurnosnih stručnjaka, timova i odgovornih osoba koji su zaduženi za kvalitetnu provedbu sigurnosne politike. Dokument u konačnici treba biti objavljen i predan svim zaposlenicima i korisnicima kojima je namijenjen.

Stav organizacije se kroz postupak dokumentiranja i bilježenja svakog pristupa održava kroz ugovor o povjerenju za kojim organizacija ima potrebu zaštiti vrijednost koju posjeduje. Ugovori o povjerenju imaju svrhu da na temelju zakona, zaštite vrijednosti organizacije od kopiranja, uništavanja i svih ostalih neželjenih radnji od strane zaposlenika, partnera ili treće strane. Ugovor o povjerenju treba sadržavati očekivano trajanje ugovora, odgovornost i akcije nadležnih osoba, te postupke koji se provode prilikom raskida ugovora. Potrebno je točno definirati što treba zaštiti da bi se spriječilo ugrožavanje cjelokupnog korporativnog okruženja. Također ugovor o povjerenju treba sadržavati koja prava imaju ovlašteni partneri/korisnici pri uporabi informacija i koji se procesi koriste za obavještavanje neovlaštenog širenja informacija. Potrebno je uz to definirati i popis informacija koje moraju biti uništene, promijenjene ili vraćene pri prekidu ugovora, te akcije koje je potrebno poduzeti ukoliko dođe do nepoštivanja ugovora [27].

Temelj za implementaciju IK sigurnosti unutar organizacije se predstavlja kroz sigurnosnu politiku. Značaj sigurnosne politike u većini organizacija potpuno je zanemarena. Implementiranje tehničkih sigurnosnih rješenja, uz pravodobnu procjenu rizika ili mogućnost postojanja strukturiranog dokumenata sigurnosne politike uz procedure i preporuke za provedbu implementacije bez kvalitetnog strateškog planiranja i identifikacije resursa su pogreške koje se vrlo često pojavljuju. S obzirom da se konstantno uvode novi elementi i povlače stari, te se IK i druga imovina koju koristi organizacija tokom vremena izmjenjuje i prilagođava uporabi, podrazumijeva se da se pritom kontinuirano mijenja i dokument sigurnosne politike [2].

4.3. Sigurnosni standardi

Nakon uspostavljanja sigurnosne politike potrebno je odabrati standard prema kojem će se sigurnosna politika uspostaviti. Kako bi se organizacijama javnog i privatnog poslovnog sektora pomoglo pri uvođenju sustava IK sigurnosti u svrhu prevencije od zlouporabe, gubitka ili oštećenja podataka i informacija, u Velikoj Britaniji razvijena je norma BS 7799 pod nazivom *Industry Code of Practice* (Industrijski kodeks prakse). Iz norme BS 7799 proizašle su ISO/IEC 17799, odnosno ISO/IEC 27002 te ISO/IEC 27001 kao međunarodne norme [17].

Poslovanje u skladu s normom (standardom) omogućava sigurno i kvalitetno upravljanje IK sigurnošću sustava i stvara povjerenje u poslovanju s međunarodnim organizacijama. Razvijene norme ISO 27001 i 27002 iz normi BS 7799-2 i BS 7799-1. prihvaćene su i kao hrvatske norme od strane Hrvatskog zavoda za norme. ISMS familija normi su definirane prema sljedećem [17]:

- ISO/IEC 27000: 2009, sustavi upravljanja IK sigurnošću,
- ISO/IEC 27001: 2005, sustavi upravljanja IK sigurnošću – zahtjevi,
- ISO/IEC 27002: 2005, kodeks prakse upravljanja IK sigurnošću,
- ISO/IEC 27003, smjernice za implementaciju sustava upravljanja IK sigurnošću,
- ISO/IEC 27004, upravljanje IK sigurnošću – mjerenje,
- ISO/IEC 27005: 2008, upravljanje rizikom IK sigurnosti,
- ISO/IEC 27006: 2007, zahtjevi za tijela koja pružaju reviziju i certifikaciju ISMS-a,
- ISO/IEC 27007, smjernice za reviziju sustava upravljanja IK sigurnošću i
- ISO/IEC 27011, smjernice za upravljanje IK sigurnošću telekomunikacija.

Tablica 2. Opis ISO normi

ISO/IEC 17799	ISO/IEC 17799 je norma formulirana na mnogim postavkama BS 7799 norme koja od 1995., kada je donesena, predstavlja najraširenij pokušaj uvođenja međunarodno priznatih normi na području upravljanja IK sigurnošću. ISO/IEC ističe da je 17799 prvenstveno namijenjena širenju svjesnosti o potrebi organizacije sustava zaštite informacija kroz opis najboljih već primijenjenih metoda i principa za uspostavu i održavanje takvih poslovnih IK sustava. ISO 17799:2005 norma razlikuje provjeru sigurnosne politike, ljudskih resursa, komunikacija i operativnog sustava, nabavu, organizaciju i održavanje IK sustava, odgovor na incidente te općenito pridržavanje uobičajenih poslovnih običaja. Najveći dio dokumenta odnosi se na provjeru sustava komunikacija i ostalih IK tehnologija koje se koriste u poslovnim procesima.
ISO/IEC 27001	ISO 27001 je međunarodna norma objavljena od strane Međunarodne organizacije za standardizaciju (ISO) i opisuje kako upravljati IK sigurnošću u organizacijama. ISO 27001 može biti implementiran u bilo kojoj organizaciji, neovisno o njenoj veličini ili namjeni. Razvijena je od strane stručnjaka iz područja IK sigurnosti i propisuje metodologiju za primjenu upravljanja IK sigurnošću u organizaciji. Također, omogućava organizacijama dobivanje certifikata, što znači da neovisno certifikacijsko tijelo daje potvrdu da je organizacija implementirala IK sigurnost sukladno ISO 2700135. Norma ISO 27001 sastoji se od 11 područja, 39 kontrolnih ciljeva i ukupno 133 kontrole koje koriste kao pomoć prilikom identifikacije, upravljanja i smanjenja niza prijetnji kojima je IK sustav izložen. Također, osigurava se usklađenost s važećom zakonskom regulativom, aktivnostima unutar organizacije kao i pouzdanost sustava u slučaju nesreće, ali i edukacija zaposlenika. Norma ISO 27001 pomaže u zaštiti tajnosti informacija na način da ih drži dostupnima samo ovlaštenim osobama. Norma također čuva integritet, točnost i cjelovitost informacije te dostupnost ovlaštenim subjektima informacije i mogućnost korištenja istih.
ISO/IEC 27002	ISO/IEC 27002 je „pomoćna“ norma koja detaljnije opisuje na koji način provesti mjere zaštite definirane normom ISO/IEC 27001. ISO/IEC 27002 uspostavlja smjernice i opće principe inicijacije, implementacije, održavanja i unaprjeđenja upravljanja informacijskom sigurnošću unutar organizacije. Kontrole navedene normom obuhvaćaju specifične zahtjeve identificirane posredstvom procjene rizika. Norma pruža smjernice i prilikom razvoja standarda organizacijske sigurnosti te učinkovite prakse upravljanja sigurnošću, kao i pomoć u izgradnji povjerenja za unutar organizacijske aktivnosti. Trenutna inačica norme sadrži 114 kontrola naspram 133 sadržanih unutar inačice norme iz 2005. godine.

Izvor: **[17], [22].**

Opći koncept regulativnog okvira IK sigurnosti temelji se na kombinaciji zakonodavnih propisa, međunarodnih i nacionalnih normi te unutarnjih standarda svake pojedine organizacije (državnog tijela ili pravne osobe – tvrtke). U tablici 2 su detaljnije opisane norme ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 27002 koje predstavljaju temelj izgradnje kvalitetne sigurnosti i zaštite IK sustava. Ukratko je opisan značaj ISO dokumenta, tj. što predstavlja ili bi trebao predstavljati organizaciji unutar korporativnog okruženja i na koji način djeluje standard. ISO norme su zapravo temeljni zahtjevi koje organizacija mora ispuniti da bi mogla obavljati svoju djelatnost u skladu sa relevantnim propisima i zahtjevima korisnika/partnera. One su primjenjive na sve vrste organizacija i ukoliko su kvalitetno provedene pridonose sigurnosti i zaštiti IK sustava unutar korporativnog okruženja.

5. Primjer sigurnosti i zaštite informacijsko – komunikacijskog sustava u korporativnom okruženju

Sigurnost IK sustava predstavlja važnu ulogu za uspješno poslovanje organizacije. S obzirom na to, u ovom poglavlju predstavljena je stvarna organizacija na čijem primjeru će se utvrditi kako provođenje sigurnosti i zaštite IK sustava izgleda u praksi. Zbog sigurnosnih razloga i politike organizacije, njezino ime u daljnjem će se tekstu koristiti u obliku tvrtka – X (realni poslovni subjekt).

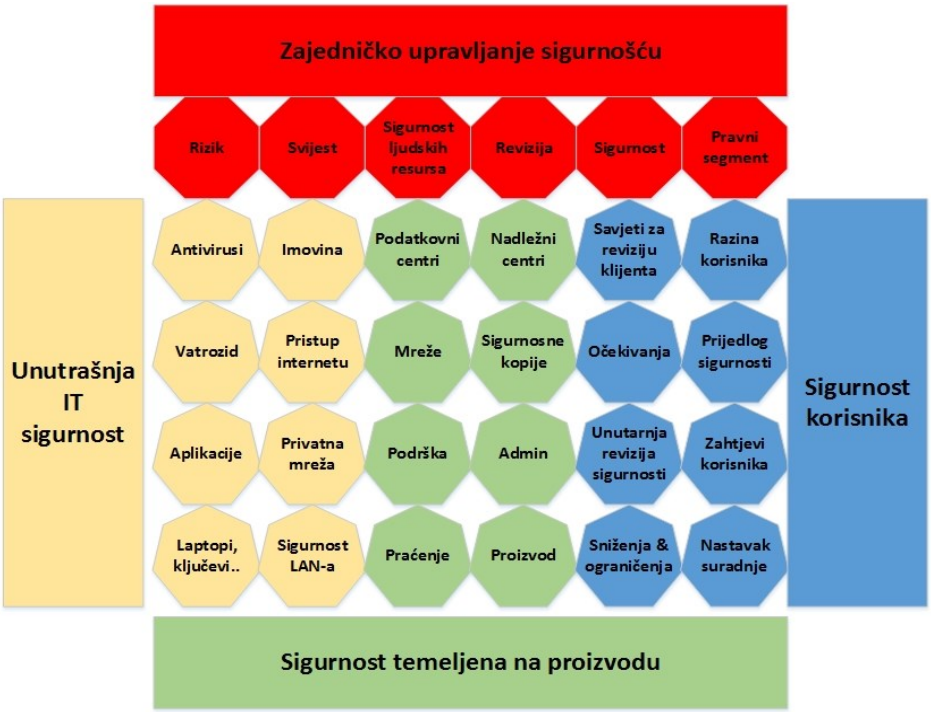
Tvrtka – X je dio grupacije koja je globalni lider na području digitalne transformacije s oko 100.000 zaposlenih u 72 zemlje svijeta. U Hrvatskoj s više od 100 zaposlenika djeluje na područjima *Big Data, Cybersecurity, High Performance Computing* i *Digital Workplace*, te isporučuje *Cloud usluge*, *Infrastructure & Data Management*, *Business & Platform rješenja*. Korištenjem najmodernijih tehnologija, digitalnom stručnošću i industrijskim znanjem tvrtka - X podržava digitalnu transformaciju korisnika na različitim tržišnim područjima: obrana, financijske usluge, zdravstvo, proizvodni sektor, mediji i komunalne usluge, javni sektor, trgovina, telekomunikacije i promet.

Tvrtka – X blisko surađuje sa organizacijama u softverskim aplikacijama, infrastrukturi i savjetovanju za upotpunjavanje cjelokupnog portfolia u savjetovanju, rješenjima i uslugama.

5.1. Model sigurnosti informacijsko – komunikacijskog sustava

Prema slici 12 prikazan je sigurnosni model realnog poslovnog subjekta tvrtke - X. Sigurnosni model se dijeli na četiri cjeline koje su međusobno usko povezane, kroz koje organizacija djeluje unutar svog korporativnog okruženja. Na temelju zajedničkog upravljanja sigurnošću određuju se globalna pravila koja su donesena od strane sigurnosnih službenika. Kroz segment zajedničkog upravljanja sigurnošću djeluje se na procese procjene rizika, svjesnosti i sigurnosti osoblja, reviziju te zakonsko upravljanje dijelovima organizacije.

Unutrašnja IT sigurnost djeluje u skladu s politikom organizacije te pruža redovito izvješćivanje s obzirom da surađuje i sa drugim elementima organizacije. Sigurnost proizvoda i usluga se pruža u svakoj servisnoj liniji, te se uz to dijeli infrastruktura i usluga sa ostalim elementima organizacije. Stvara se sigurnosna strategija za svaku uslugu ili proizvod. Sigurnost temeljena na korisnicima definirana je prema ugovoru sa korisnicima koja se povezuje sa proizvodom ili uslugom. Unutar tog segmenta se ponajviše djeluje na specifične potrebe korisnika, zahtjeve i nastavak suradnje.



Slika 12. Sigurnosni model tvrtke - X.

Izvor: **[28]**

Podjela je definirana kako bi se pružilo lakše poslovanje kroz segmente korporativnog okruženja. Tvrtka – X ima izgrađenu viziju sigurnosti i omogućava komunikaciju prema svim organizacijskim entitetima i klijentima. Temelj unutar tvrtke - X je osigurati pouzdanu i konsolidiranu viziju o organizacijskom sigurnosnom okruženju i redovito ga kontrolirati od strane tima za upravljanje.

Tablica 3. Sigurnosno osoblje i infrastruktura.

Sigurnosno osoblje	Infrastruktura	
12 svjetskih glavnih sigurnosnih voditelja sigurnosti IK sustava.	3 sigurnosna centra za zaštitu.	32 podatkovnih centra.
10 glavnih sigurnosnih referenta podijeljeni prema regijama.	1 globalni protuvirusni centar.	+ 1 glavno centralno upravljano računalo.
200 sigurnosnih stručnjaka.	Specifična zaštitna rješenja.	+ 4,700 vatrozida.
600 sigurnosnih konzultanata/stručnjaka.	1.100 IT poslužitelja.	+ 100.000 virtualnih poslužitelja.
1 Voditelj sigurnosti IK sustava 11 IT sigurnosnih referenta.	70.000 radnih stanica.	70.000 fizičkih poslužitelja.
1.100 IT poslužitelja.	75 aplikacija.	+ 80.000 TB mrežne pohrane.

Izvor: **[28]**

Na temelju opremljenosti sigurnosnog sustava (Tablica 3) provode se sigurnosni prioriteti za obavještavanje i upravljanje poslovanjem. Na taj način se definira čvrsta linija koja usklađuje ciljeve sigurnosnih propusta sa sigurnosnim prioritetima. Uz to tvrtka – X neprekidno

unaprjeđuje sigurnosne postavke, te usklađuje pravovremenu reakciju i obavještavanje o sigurnosnim incidentima. Također se optimizira organizacija sigurnosti, i na taj način izgrađuje sigurnosna svijest u cijelom korporativnom okruženju što pridonosi poboljšanju sigurnosnih ponuda.

Tablica 4. Uloga organizacijskih jedinica unutar IK sigurnosnog modela.

Izvršni odbor sigurnosti (*Executive Committee* – Excom) / (*Senior Executive Vice President* -SEVP)	• *Izvršni odbor sigurnosti - Definira viziju i misiju o sigurnosti IK sustava.* • *Dodjeljuje izvršne odgovornosti za sigurnost IK sustava.* • *Prati postignuća sigurnosnih inicijativa.* • *Prilagođava sigurnosnu strategiju u IK sustav.* • *Obavlja sigurnosne procjene i upravlja ranjivostima IK sustava.*
Sigurnosna grupa	• *Upravlja strategijom, smjerom i izvedbom IK sigurnosti imovine.* • *Preuzima odgovornost za upravljanje programom.* • *Definira i upravlja mjerama, izvještavanjem i globalnim ISMS-om.* • *Upravlja ukupnim sigurnosnim rizikom tvrtke.* • *Definira i provodi politike, standarde, procedure i kontrole.*
Jezgreni dio upravljanja sigurnošću IK sustava	• *Upravlja strategijom sigurnosti, definira i implementira sigurnosne politike za svoje poslovanje na globalnoj razini.* • *Osigurava osnovne sigurnosne usluge svojim klijentima. Implementira sigurnosne usluge i upravlja katalogom usluga.* • *Upravlja i nadzire IK sustava proizvodnje (ISO27001 ili PCI DSS)* • *Obavještavanje o sigurnosnim rizicima, sigurnosnim incidentima.*
Sigurnosni portfolio	• *Razvija portfelj sigurnosnih mjera i dizajnira sigurnosna rješenja.* • *Osigurava usluge sigurnosnog konzultiranja za partnere.* • *Održava znanja i poglede na sigurnost IK sustava.* • *Osigurava sigurnosni uvid, napredne sigurnosne usluge i rješenja za unutarnju sigurnost organizacije.*

Izvor: **[28]**

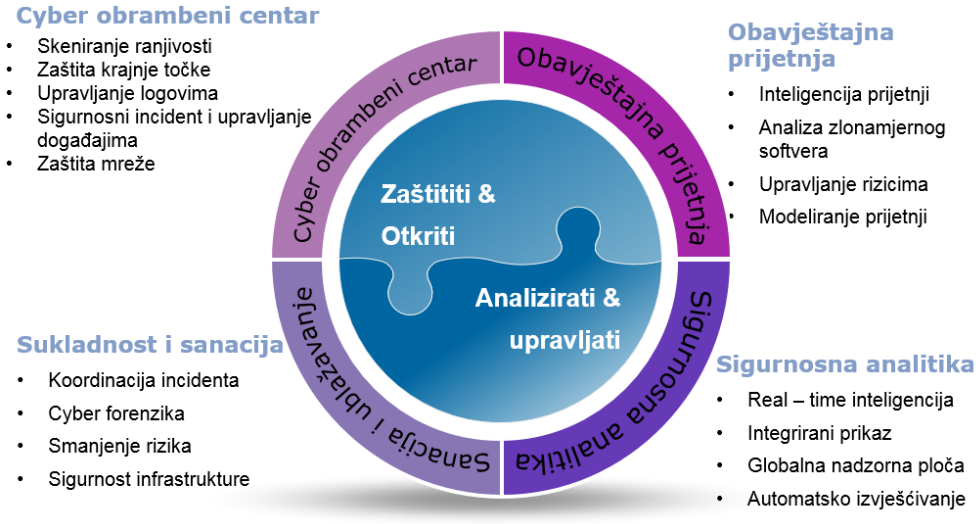
Svaki entitet uključen u sigurnosnu organizaciju definiran je sa unaprijed jasnim pravilom, bez naknadne promjene te u svrhu očuvanja suvereniteta IK sustava. Prema tablici 4 definirane su uloge organizacijskih jedinica koje djeluju unutar sigurnosnog modela IK sustava. Organizacijske jedinice strukturirane su prema zadaćama i procesima koje obavljaju. Također viša uloga donosi veću odgovornost i definira važnije odluke koje se unutar organizacije provode nakon raznih testiranja, praćenja i nadzora.

5.2. Model upravljanja infrastrukturom

Tvrtka - X kroz model upravljanja infrastrukturom (Slika 13) definira obrambeni centar unutar kojeg se skeniraju ranjivosti krajnjih točaka IK sustava. Obrambeni centar upravlja log zapisima, sigurnosnim incidentima i događajima za zaštitu mreže tvrtke - X. Unutar modela

upravljanja definirana su dva temeljna zahtjeva, zaštita IK sustava uz otkrivanje sigurnosnih propusta, te analiza rizika i upravljanje sigurnosnim incidentima. Navedeni zahtjevi dijele se na šire procese unutar aktivnosti obavještavanja, sigurnosnu analitiku i sanaciju IK sustava.

Obavještajne aktivnosti sadrže procese upravljanja rizicima i prijetnjama, te se oni koriste da se na vrijeme upozori na moguće propuste . Nakon uočavanja, praćenja i analize provodi se sigurnosna analitika u stvarnom vremenu kroz integrirani prikaz i detaljno automatsko izvještavanje unutar organizacijskog okruženja. Nakon definiranih prethodnih aktivnosti i procesa korištenih za zaštitu IK sustava provodi se proces koordinacije incidenta i sanacije problema. Također pružaju se novije nadogradnje i zakrpe za poboljšanje sigurnosti infrastrukture i smanjenje rizika koji može ugroziti IK sustav i sigurno poslovanje.



Slika 13. Model upravljanja infrastrukturom sa aspekta sigurnosti IK sustava.

Izvor: **[28]**

Kroz model upravljanja infrastrukturom tvrtka - X pomaže organizacijama unutar korporativnog okruženja da prepoznaju i otklone nedostatke, osiguravaju svoje okruženje i opseg, te kontinuirano prate i zaštićuju poslovanje. Tvrtka - X provodi mehanizme zaštite za svu imovinu organizacije i partnera (osobe, informacije, uključujući osobne podatke, web stranice, materijale, intelektualno vlasništvo) u skladu sa zakonima, ugovorima, propisima i organizacijskom sigurnosnom politikom. Također implementirala je sustav upravljanja sigurnošću temeljen na ISO standardima (tj. ISO27001).

Za kvalitetno provođenje sigurnosti svi menadžeri su izravno odgovorni za primjenu organizacijskih sigurnosnih politika i standarda unutar njihovih poslovnih područja. Isto tako sigurnosno osoblje ima odgovornost pridržavati se sigurnosnih politika [28].

5.3. Sredstva zaštite informacijsko – komunikacijskog sustava

Na temelju analize provedenih sigurnosnih mjera i politike tvrtke - X definirani su osnovni koraci koji se provode za zaštitu od unutarnjih prijetnji, grešaka, *hacktivista, cyber* prijetnji, ucjena i ostalih prijetnji koje mogu ugroziti IK sustav. Tvrtka - X koristi sredstva zaštite

IK sustava prema definiranim sigurnosnim standardima opisanim u prethodnim poglavljima. Prvi korak u zaštiti IK sustava je proces provođenja autentifikacije za svakog zaposlenika. Autentifikacijom se dokazuje identitet i omogućava pristup resursima IK sustava. Ukoliko dođe do prijetnji, pokušava se otkriti ranjivost kroz proces skeniranja ranjivosti na organizacijskoj infrastrukturi. Skeniranjem se definiraju ranjive točke u sustava koje se otklanjaju nadogradnjom i održavanjem uz pomoć ISMS-a.

Tvrtka - X isporučuje i upravlja fizičkim i logičkim sigurnosnim sustavom pametnih kartica. Time se omogućuje povezivanje fizičke sigurnosti (poslovnih prostora organizacije) sa sigurnim pristupom IK sustava. Drugim riječima to predstavlja proces provjere autentičnosti kroz organizacijske PKI kartice (*Public key infrastructure*).

5.3.1. Integrirana sredstva zaštite informacijsko – komunikacijskog sustava

Upravljanje sigurnosnim informacijama i događajima (*Security Information and Event Management* - SIEM) predstavljaju rješenja koja postaju glavni dio sigurnosne infrastrukture svake organizacije. SIEM tehnološki projekti su tipično orijentirani na nekoliko većih slučajeva korištenja: izvještavanje o regulatornoj sukladnosti (npr. *Payment Card Industry Data Security Standard* - PCI DSS), upravljanje prijetnjama, odgovaranje na incidente i forenziku. Unaprjeđenje izvještavanja o regulatornoj suglasnosti i identificiranje sigurnosnih incidenata glavni su razlozi postavljanja ovog rješenja. SIEM predstavlja integrirano sigurnosno rješenje sa sljedećim zadaćama [28]:

- sakupljanje i arhiviranje podataka IK sustava (sistemski zapisi, *logovi, eventi*),
- obrada i korelacija podataka,
- automatizirane akcije kako ih definiraju sigurnosna pravila i procedure,
- forenzička analiza i
- izvještavanje.

Navedena rješenja podržavaju dugotrajno spremanje sistemskih zapisa i izvještavanje nad prikupljenim podacima, te se jednostavno integriraju s postojećim mrežnim, sigurnosnim i infrastrukturnim aplikacijama i uređajima. SIEM rješenja nadziru događaje unutar aplikacije ili na transakcijskim logovima a sve to u svrhu otkrivanja mogućih događaja koje mogu biti indikator neovlaštenog korištenja sustava. Kritični događaji mogu biti neprimijećeni s obzirom da nema načina da se vidi uzročno-posljedična povezanost važnih događaja ili postoji mogućnost da nema prikladnog procesa nadgledanja sustava. Stoga SIEM rješenje može imati važnu ulogu u detekciji prijetnji, pravovremenoj reakciji, te detaljnoj analizi prilikom zaštite IK sustava.

Praćenje promjena unutar mreže tvrtke – X i njenog okruženja izuzetno je važno za provedbu sigurnosne politike i održavanje prihvatljive razine IK sigurnosti. Jedini efikasan način kontrole promjena nad ključnim podacima i sustavima jest implementacija sustava za osiguranje integriteta podataka, koji će u realnom vremenu pratiti promjene na podacima i sustavima i uspoređivati ih sa zadanim vrijednostima. Takav način kontrole donosi *Tripwire*

Enterprise koji omogućuje detektiranje neovlaštenih promjena sistemskih i drugih datoteka, automatsku usporedbu trenutnog stanja sustava sa zahtjevima sigurnosnih IT standarda (poput PCI DSS standarda), kao i automatski popravak sustava koji nisu sukladni sigurnosnim zahtjevima IK standarda.

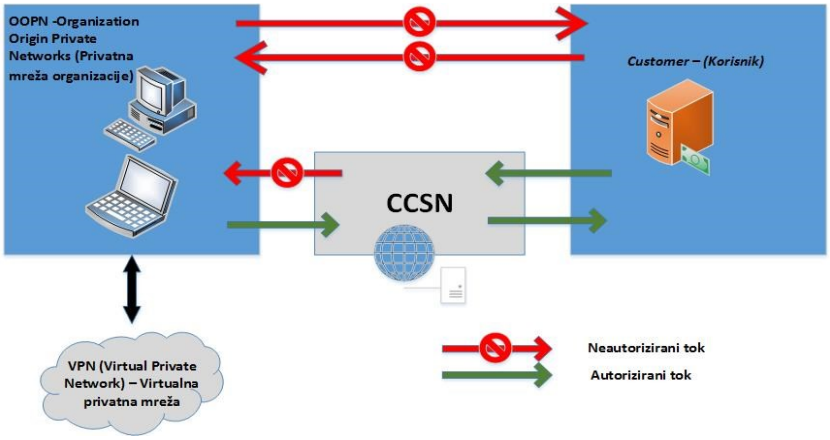
Prethodno spomenuti PCI DSS standard vrlo je važan čimbenik u svakodnevnom poslovanju pružatelju usluga kartičnog plaćanja. S obzirom da pružatelji takvih usluga obrađuju velike količine podataka svojih klijenata, njihova zaštita i tajnost iznimno su bitni. *Tripwire Enterprise* između navedenih nudi i sljedeće funkcionalnosti [28]:

- usklađivanje sa regulatornim zahtjevima (npr. PCI DSS),
- praćenje promjena nad važnim datotekama,
- integracija sa SIEM rješenjima,
- automatsku ocjenu stanja sigurnosti infrastrukture,
- izvještaji za različite profile korisnika i
- mogućnost automatskog povratka sustava.

5.3.2. Pristup mreži organizacije

Pristup mreži partnera, odnosno drugim organizacijama, vrši se putem mreže za korisničku službu u zemlji (*Country Customer Service Networks* - CCSN) na *Shared Services* (Zajednička usluga*)* mreži unutar tvrtke - X. Da bi se pristupilo infrastrukturi partnera ili druge organizacije, zaposlenik tvrtke - X trebao bi imati [28:]:

- organizacijsko računalo,
- valjani osobni korisnički račun u organizacijskom okruženju,
- važeći pristup na organizacijski CCSN i
- važeći račun na infrastrukturi partnera ili druge organizacije.



Slika 14. Generalna sigurnosna pravila pristupa IK sustavu.

Izvor: **[28]**

Na taj način se koriste resursi platforme partnera ili druge organizacije, kojem se pristupa na siguran način kroz VPN tvrtke - X (Slika 14). Ova vrsta veze putem organizacijskog CSSN-a omogućuje razvrstavanje protokola, zabranjujući izravni pristup između tvrtke - X i

mreže partnera. CSSN možemo poistovjetiti kao neku vrstu DMZ-a posvećen sigurnosti IK sustava.

5.4. Primjer normativnog okvira tvrtke – X

Tvrtka – X obavezala se poštivati zakonske, regulatorne i ugovorne zahtjeve vezane za sigurnost IK sustava unutar korporativnog okruženja. Struktura dokumenta usklađena je s najboljim praksama sigurnosti IK sustava kako je opisano u ISO/IEC 27002 sigurnosnom standardu. Za certifikacijsku listu ISO 27001:2005 tvrtka – X trenutno raspolaže certifikatima u više od 10 zemalja, što daje veliki značaj poslovnom uspjehu.

Tablica 5. Opis certifikata koje posjeduje tvrtka - X.

Certifikati/potvrde	Kratki opis (opseg, institut standarda)
ISO 9001:2008	*Certifikat ISO 9001: 2008 za IT usluge i poslovni proces outsourcinga širom svijeta.*
ISO/IEC 20000-1 : 2005	*Organizacije je Implementirala i održava sustav upravljanja IK uslugama.*
ISO/IEC 27001 : 2005	*Organizacije implementirala i održava sustav upravljanja IK sigurnošću.*
ISO 14001	*Posjeduje certifikat ISO 14001 u cijeloj tvrtki. Stvorila je globalni tim koji je odgovoran za izvještavanje organizacijskih postignuća a danas ih koriste sve najbolje korporacijske organizacije.*
SMM (ITIL) Model upravljanja uslugama	*Upotrebljavaju se specifične metodologije, vještine i tehnike kao što je Service Management Model (SMM) koji je 100% ITIL kompatibilan. SMM je u potpunosti usklađen s međunarodnim standardima kvalitete ISO 9001, ISO 27001, ISO 20000 i IT-CF 4.0.*
Prince2	*Opremanje programskih i projektnih menadžera za uspjeh. Usvajanjem PRINCE2 kao preferirane metodologije upravljanja projektima.*
SAS70/SOX Tip 1 & 2	*Razvojni projekti provode se prema „Prince2“, što je standardna metoda za upravljanje projektima i programima. „Prince2“ također osigurava odgovarajuće uključivanje svih dionika, potrebnih za pružanje na vrijeme isporuke. Svi voditelji projekata su certificirani za „Prince2“.*
CMMI & IT Service CMM Level 3	*Implementirala je kontrolni okvir za sastavljanje SAS70 revizorskih izjava za ispunjavanje propisa propisanih u (Sarbanes-Oxley -* SOX*) Zakonu iz 2002. godine, za vlastitu organizaciju kao i za podršku svojim klijentima. Revizorski standard SAS70 koristi revizore usluga za procjenu internih kontrola uslužne organizacije. Konačna verzija izjave o reviziji SAS70 podnosi se klijentima ako se ugovorom dogovore, čime korisnici mogu procijeniti valjanost organizacijske interne kontrole.*
CMMI Level 5 Model zrelosti integriranih procesa	*Ima vrlo aktivan program za certificiranje svog poslovanja na razini 3 (Capabilities Maturity Model Integration- CMMI). CMMI model predstavlja sustavan i iscrpan opis zrelosti programskih procesa, te je kao takav od neprocjenjive vrijednosti i pomoći za sve organizacije koje su dostigle razinu svijesti da trebaju unaprijediti svoje odnosno svoj proces razvoja i održavanja programskih aplikacija.*

Izvor: **[28]**

Organizacija ISMS-a ima certifikat ISO/IEC 27001: 2005 o opsegu *outsourcing* IT usluga i poslovnih procesa diljem svijeta od strane certifikacijske tvrtke (*Data Quality Services* – DQS) koju je akreditirala organizacija DakkS (*Certificate #302147* ISMS). Organizacija posjeduje ISO 27001 normu koja pokriva mnoge sigurnosne teme, uključujući fizičku i okolišnu IK sigurnost.

U tablici 5 detaljnije su opisani certifikati i potvrde koje Tvrtka – X posjeduje odnosno zadovoljava.

IT metodologija procjene rizika usklađena je s ciklusom „Planiraj-Uradi-Provjeri-Djeluj“ (*Plan-Do-Check-Act* - PDCA*)* prema ISO/IEC 27005: 2008 standardu. Prema ugovoru sa partnerom, tim IK sigurnosti odgovoran je za godišnju procjenu rizika i ocjenu rizika te izvještavanje. Glavni poslovi vezani uz procjenu rizika su:

- identifikacija rizika,
- analiza i evaluacija rizika,
- rizik oporavka i
- prijedlog sigurnosnih mjera.

Tvrtka - X posjeduje formalnu IK sigurnosnu politiku koja se temelji na zahtjevima BS7799/ISO17799. Ova su pravila obvezna i primjenjuju se u čitavoj tvrtki – X. Ciljevi se ispunjavaju kroz skup kontrola, koji uključuju politike, prakse, procedure i organizacijske strukture unutar tvrtke - X. Te kontrole čine dio sigurnosne politike i organizacijskog sustava upravljanja kvalitetom ISO9001. Fizičke sigurnosne procedure su u skladu s BS7799/ISO17799 sigurnosnim certifikacijskim zahtjevima i uz organizacijsku sigurnosnu politiku tvrtke – X koja se bolje opisuje u nastavku.

5.5. Primjer korporativne sigurnosne politike tvrtke - X

Sigurnosna politika unutar organizacije usmjerena je na rješavanje pitanja povjerljivosti, integriteta i dostupnosti. Predstavlja hijerarhijski strukturirani dokument koji se sastoji od više međusobno povezanih elemenata. Osnovni elementi dokumenta sigurnosne politike su sljedeći:

- politike,
- standardi,
- preporuke i
- procedure.

Sljedeća područja djelovanja unutar tvrtke - X navode sveobuhvatne ciljeve IK sigurnosti koje su raspisane prema domenama unutar organizacijske strukture. Poslovna politika odražava predanost tvrtke – X da se bavi zahtjevima IK sigurnosti za sve glavne domene prema standardu ISO27001: 2013 [28]:

- organizacija IK sigurnosti,
- sigurnost ljudskih resursa,
- upravljanje imovinom,
- kontrola pristupa,
- kriptografija,
- fizička i okolišna,
- sigurnost rada,

- sigurnost komunikacije,
- stjecanje, razvoj i održavanje sustava,
- upravljanje odnosima s dobavljačima,
- upravljanje incidentima u IK sigurnosti i
- usklađenost.

Ova područja djelovanja se smatraju referentnim za sve odluke vezane uz sigurnost IK sustava unutar organizacijske strukture tvrtke – X.

5.5.1.Organizacija informacijsko - komunikacijske sigurnosti

Organizacija IK sigurnost definirana je u trenutnoj verziji dokumenta ISMS za opseg uloga i odgovornosti, koja je usklađena s organizacijskom globalnom sigurnošću tvrtke - X. Svi mobilni računalni uređaji dodijeljeni tvrtki ili zaposlenicima koji ih koriste zajedno s bilo kojim računalom, podacima ili mrežnim uređajem moraju slijediti organizacijske politike za sigurnu upotrebu [28]. To uključuje bilo koji hardver kao što su osobni digitalni asistenti (*Personal digital assistant* - PDA), *tablet* računala i srodni ovlašteni/licencirani softver koji bi se mogao koristiti za pristup korporativnim resursima. Zaposlenici koji zahtijevaju pristup mreži tvrtke - X moraju dobiti odgovarajuće odobrenje od strane odgovarajućih voditelja odjela, pružajući odgovarajuće poslovno opravdanje. Voditelj odjela pritom mora potvrditi zahtjev. Tim unutar međunarodne tvrtke – X za tehničku podršku (*International Technical Support Organization* – ITSO) mora dodatno pregledati i odobriti/odbiti zahtjev kako je definirano u pravilima korištenja uređaja.

Svi ovlašteni zaposlenici i agencije ili osobe s podugovorom mogu koristiti isključivo opremu tvrtke - X kod kuće uz svoje osobne računalne resurse, kao što je kućni širokopojasni pojas za povezivanje s umreženim uslugama tvrtke - X. Ovlaštenim korisnicima mora se osigurati daljinska povezanost preko sloja sigurnosnog povezivanja (*Secure Sockets Layer* – SSL) koja je definirana kao metoda kriptiranja web prometa. SSL sprječava osobama kojima to nije namijenjeno pristup do web paketa. Korisnik ne smije kopirati nikakve podatke iz sustava dodijeljenog organizaciji na osobni uređaj. U slučaju kršenja sigurnosti koje korisnik provodi tijekom rada na daljinu, kao dio procesa istrage incidenta, korisnički sustav će biti odgovoran za reviziju/forenzičku provjeru i disciplinske mjere pokrenute protiv korisnika [28].

5.5.2. Sigurnost ljudskih resursa

Kretanje zaposlenika unutar prostora tvrtke – X omogućeno je pristupnim PKI karticama na temelju individualne autorizacije pristupa za pojedina područja, odnosno urede [28]. Sigurnosno osoblje ima pravo provjeriti kartice kada se to smatra potrebnim. Za postizanje što bolje kvalitete rada i sigurnost poslovanja, svi zaposlenici dužni su proći obaveznu obuku o IK sigurnosti te potpisati dokument o povjerljivosti podataka. No osim zaposlenika, potpisivanju dokumenta moraju pristupiti i svi vanjski suradnici te klijenti.

5.5.3. Postupci kontrole pristupa

Informacije su klasificirane na temelju svoje osjetljivosti i važnosti za poslovanje. Klasifikacija je na: tajno, povjerljivo, unutarnja uporaba i javna uporaba. [28]. Vlasnici informacija moraju se pridržavati odgovarajućih pravila o očuvanju povjerljivosti, cjelovitosti i dostupnosti informacija. Korisnici ne smiju otkrivati, u potpunosti ili djelomično, bilo kakve podatke koji su klasificirani kao sadržaj visoke osjetljivosti. Isto se primjenjuje i na poslovne osjetljive podatke čak i ako se informacije ne klasificiraju (npr. narudžbe proizvoda, cijene, popis klijenata). Korisnici moraju voditi brigu o pristupu i korištenju informacija prema klasifikaciji. Dužni su obavijestiti vlasnika podataka o bilo kakvim ranjivosti ili sigurnosnim povredama koje se odnose na korištenje ili pristup klasificiranim podacima.

Svaki korisnik, odnosno zaposlenik ima pravo na jedinstveni korisnički ID i lozinku. On postaje njihov apsolutni vlasnik i sukladno tome odgovoran je za sve aktivnosti koje obavlja putem računa. Za pristupanje sa zajedničkim ID-em i/ili lozinkom, svaki korisnik je osobno odgovoran za čuvanje pristupnih podataka. Lozinke za takve pristupe usklađene su sa smjernicama navedenim u organizacijskim uputama tvrtke – X. One se tretiraju kao osjetljive i povjerljive informacije. [28].

Pristup e-mailu tvrtke - X dostupan je svim zaposlenicima unutar korporativnog okruženja. Usluge e-pošte ne smiju se koristiti za razmjenu zakonski zabranjenih materijala i drugih neovlaštenih materijala. Sva razmjene pošte unutar tvrtke - X podržava mehanizam provjere autentičnosti putem aktivnog direktorija.

Svi internetski pregledi su kontrolirani i svaki pokušaj zaobilaženja tih kontrola će se smatrati kršenjem pravila. Svi korisnici Interneta trebaju koristiti računalne resurse i Internet na profesionalan, zakonit i etičan način. Pristup internetskim stranicama i protokolima je praćen i kontroliran da bi se smanjili rizici za poslovanje. Uspostava izravne veze između IK sustava i vanjskih organizacija putem Interneta ili druge javne mreže koristi snažnu autentifikaciju i šifriranje prometa ovisno o klasifikaciji podataka.

5.5.4. Kriptografija i zaštita fizičkog pristupa

Tvrtka - X koristi *BitLocker* šifriranje diska na svim organizacijskim prijenosnim računalima unutar tvrtke koji predstavlja jednostavno i iznimno sigurno rješenje za enkripciju podataka na cjelokupnom logičkom ili fizičkom disku. Uz to koristi se i identifikacija PKI kartice koju moraju aktivirati/posjedovati svi zaposlenici tvrtke - X . Potrebno je slijediti organizacijske smjernice za korištenje PKI-a navedene unutar sigurnosne politike tvrtke - X [28].

Fizičke lokacije su razdvojene na temelju kritičnosti i korištenja. Mjere kontrole fizičkog pristupa osigurane su na svim mjestima za ovlašteni pristup prostoru. Mjere sigurnosti koriste se za smanjenje rizika od požara i dima, poplave, potresa, prekida napajanja, problema s vlagom, munja, tehničkih kvarova, sabotaže i krađe. Sve dijeljene periferijske opreme (kao što su pisači, skeneri, faksovi, fotokopirni uređaji itd.) koji pohranjuju, proizvode i/ili prenose

povjerljive ili osjetljive podatke su zaštićeni od nehotičnog ili neovlaštenog pristupa. Umreženi pisač i skener su dostupni na svakoj lokaciji za opću upotrebu [28].

5.5.5. Odgovornost zaposlenika

Razina pristupa poslužiteljima temelji se na poslovnoj potrebi i ulozi. Svi pristupni zahtjevi i dodjela su praćeni od strane *helpdesk*-a nakon odgovarajućih odobrenja prema definiranom ISMS procesu.

Svakom zaposleniku se osigurava radna stanica (laptop, stolno računalo, itd.) za koju je i on osobno odgovoran. Radna stanica je povezana s mrežom za poslovne funkcije da bi se spriječila mogućnost krađe podataka. Sve radne stanice su zaštićene od operativnih OS ranjivosti i prijetnji, uključujući viruse, crve, trojance, *rootkitove, spyware, malwares, adware* i sl. Svi zaposlenici s administratorskim pravima prema IK sustava moraju osigurati da se izvršavaju ovlašteni poslovni aktivi. Zahtjev za administratorski pristup na sustavima koji su povezani s domenom tvrtke - X mora odobriti voditelj odjela unutar kojeg se korisnika nalazi i to za određeno razdoblje na temelju poslovnih opravdanja.

5.5.6. Sigurnost komunikacija

Mreža se redovito skenira za ranjivosti prema rasporedu globalne ranjivosti i skeniranje se prati mjesečno putem alata organizacijskog *Compliance Engine-a*. Sanacija ranjivosti obavlja se prema definiranom organizacijskom procesu upravljanja ranjivosti. Mrežom se upravlja u kontroliranom okruženju i odvojeno od vanjske mreže. Ona je logički odvojena na temelju njene uporabe. Organizacijsko unutarnje okruženje nema nikakvu vanjsku mrežu/mrežni priključak, osim ako postoji poslovno opravdanje i eksplicitno je odobreno od strane vrha menadžmenta. Bežični LAN (*Local area network*) pristup (unutarnji) ograničen je na korisnike ovlaštenih laptopa. Vanjski Wi-Fi pristup se osigurava na temelju poslovnih potreba i odobrenja od voditelja tima/odjela. Odgovarajuća razina sigurnosti osigurana je na bežičnim mrežama instaliranim u uređajima prema ISMS procesu. Zabranjena je veza s neovlaštenom/otvorenom pristupnom točkom (*Access Point* – AP). Niti jedan neovlašteni uređaj (npr. *Smartphone/i-Pad/tablet/phablets*) ne smije biti povezan s organizacijskim unutarnjim Wi-Fi mrežama unutar tvrtke - X. Bežična pristupna točka za unutarnju mrežu je zaštićena prema standardu (*Wi-Fi Protected Access* - WPA2/WPA*)* provjere autentičnosti. Za vanjsku/gostujuću mrežu bežični AP treba biti zaštićen prema standardu WEP autentifikacije. Podatkovna kartica koja je dodijeljena tvrtki ovlaštena je za korištenje zaposlenika u sklopu tvrtke - X za osiguranje kontinuiteta poslovanja [28].

Svi korisnici tvrtke - X dužni su pažljivo razmjenjivati informacije, bilo interno unutar tvrtke ili vanjskim stranama, kako bi zaštitili poslovni interes kako je definirano politikom tvrtke. Korisnici su dužni strogo slijediti sve standarde i smjernice navedene u organizacijskoj politici unutar tvrtke - X i postupcima prema razmjeni informacija. Razmjena podataka se provodi u poslovne svrhe, tj. informacije neće biti otkrivene resursima koji ne trebaju informacije ili nemaju dozvolu za pristup informacijama. Razmjena informacija s dobavljačima

slijedi formalnu proceduru sporazuma koja obvezuje sve strane na zaštitu povjerljivosti, integriteta i dostupnosti informacija. Informacije se moraju razmjenjivati s dobavljačima u onoj mjeri dopuštenoj u ugovorima kako ih definira organizacijska politika tvrtke - X.

5.5.7. Razvoj, testiranje i korištenje aplikacija

Razvoj aplikacija, testiranje i proizvodna okruženja trebaju biti odvojeni. Pristup svim aplikacijama je kontroliran na temelju poslovne potrebe i uloge. Pristup je osiguran pravilnom autorizacijom i provjerom autentičnosti. Aplikacija je kontrolirana validacijom ulaznih podataka, internih procesa i izlaznih podataka [28]. Aplikacije razvijene unutar tvrtke - X i aplikacije za klijente moraju slijediti sigurnosne zahtjeve klijenta i sigurne standarde kodiranja kako je definirano organizacijskom politikom tvrtke - X. Aplikacije prije korištenja i upotrebe moraju biti podvrgnute sigurnosnim ispitivanjima i odobrenju.

5.5.8. Upravljanje odnosima s dobavljačima

Ugovor za isporuku proizvoda ili usluga mora sadržavati ugovori o tajnosti podataka (*National Distribution Authority* - NDA) gdje se korisnik/partner obavezuje na povjerljivost informacija stečenih prije, za vrijeme i nakon korištenja proizvoda/usluge [28]. To će također odrediti odgovarajuće odgovornosti ugovornih strana u slučaju bilo kakvih kvarova ili kršenja sigurnosti IK sustava u korporativnom okruženju. Tamo gdje usluge uključuju upotrebu računalne tehnologije, dobavljač mora nadoknaditi štetu (uključujući zahtjeve za gubitkom poslovanja) koji proizlaze iz računalnog napada na bilo koju organizaciju koja potječe od bilo kojeg od svojih vlastitih poslužitelja Ili komunikacijsku opremu koja se nalazi u prostorijama. Ugovor o pružanju proizvoda ili usluga mora odrediti intelektualno vlasništvo i dodjelu autorskih prava nad svim informacijama i/ili drugim proizvodima nastalim tijekom trajanja ugovora, uključujući i zaštitu bilo kakvog zajedničkog rada. Dobavljač mora vratiti sve vlasničke podatke nakon prestanka ili poništenja usluge. Također mora osigurati da svi vlasnički podaci budu sigurno očišćeni od medija koji nisu vlasništvo tvrtke – X. Uključujući, ali ne ograničavajući se na, fiksne diskove, prijenosne diskove, kasete, CD-ROM-ove i CD-ove s mogućnošću ponovnog pisanja CD-a. Performanse dobavljača prate se i pregledavaju temeljem ugovora između partnera i tvrtke - X. Ponovni odabir usluge ili promjena dobavljača temelji se na izvješću koje se povremenom vrši (najmanje jednom godišnje).

6. Preporuke i metode zaštite informacijsko – komunikacijskog sustava

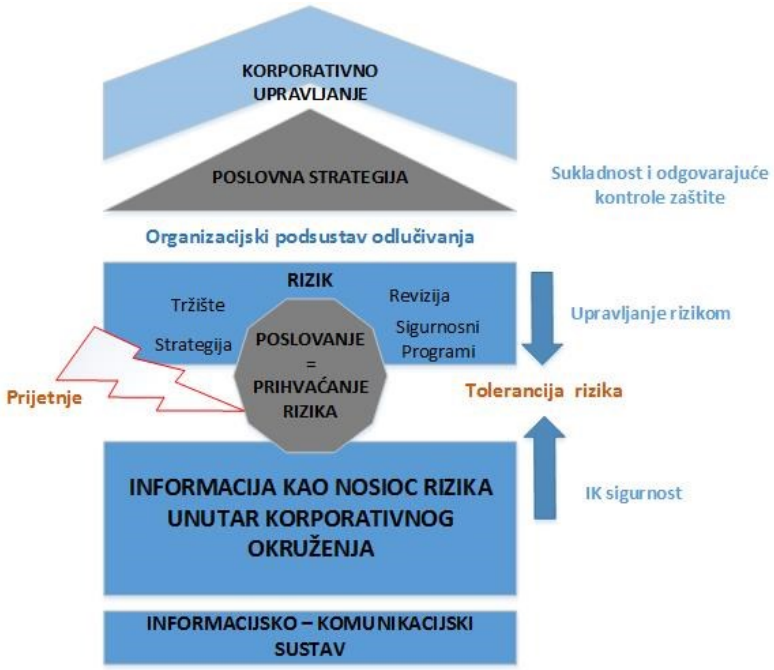
Sigurnost unutar korporativnog okruženja ima važnu ulogu u ostvarivanju poslovnih ciljeva. Na temelju toga potrebno je ustrojiti korporativnu sigurnost na organizacijske jedinice s jasnim odgovornostima i ovlastima za ispunjavanje poslovnih obaveza, što je slučaj u većim korporativnim okruženjima. Kod organizacija s manjim brojem zaposlenika dovoljno je postaviti sigurnosni odbor ili imenovati voditelja odjela sigurnosti koji će izravno odgovarati vrhovnom odboru sigurnosti. S obzirom da se svako korporativno okruženje u svojem poslovanju susreće s nekom vrstom informacija, odnosno podataka, nužno je da osobe zadužene za primjenu sigurnosti raspolažu znanjima i pravima u svezi sa zaštitom podataka (korisnika/partnera i organizacije). Da bi se izgradnja IK sustava sigurnosti mogla provesti, potrebna je potpuna suglasnost uprave organizacije.

Kako primjena suvremenih metoda zaštite izgleda u realnom poslovanju, detaljnije je opisano u poglavljima koja slijede.

6.1 Model korporativnog upravljanja sigurnošću informacijsko – komunikacijskog sustava

Kao i mnoga druga tehnološka dostignuća, model sigurnosti IK sustava ima svoje prednosti i nedostatke. Na slici 15 prikazan je model korporativnog upravljanja sigurnošću IK sustava koji predstavlja skup odgovornosti koje organizacija provodi. Svaka organizacija na temelju svog područja djelovanja strukturira svoj sigurnosni model koji čini razliku između velikih i malih organizacija. Obim posla te broj zaposlenika u velikim organizacijama uvjetuju bolju sigurnosnu zaštitu, te veća ulaganja, dok manje organizacije na temelju manjeg broja aktivnosti i procesa mogu sustavno lakše pratiti i implementirati nove zakrpe. Ulaganje u sigurnost IK sustava mnoge organizacije zanemaruju, što kasnije uzrokuje velike štete i gubitke u poslovanju. Osim toga, cjelokupno korporativno okruženje može biti ugroženo i zbog propusta od strane partnera. Uspješne organizacije pak, vrlo sustavno i predano pristupaju problemu sigurnosti i zaštite IK sustava, te mu posvećuju odgovarajuću pažnju, vrijeme i resurse.

Osim nedostatka ulaganja u sigurnost IK sustava, problem također predstavlja kada organizacije previše vremena i financijskih sredstava troše na zaštitne mehanizme koji im možda nisu niti potrebni. Potrebno je provoditi one sigurnosne mjere i kontrole zaštite koje štite poslovanje organizacije i njeno okruženje. Iz tog razloga je potrebno postaviti adekvatne stručnjake i voditelje sigurnosti i zaštite, te provoditi stalne edukacije zaposlenika, kontrolirati poslovanje na temelju vlastitih interesa, te postepeno uvoditi promjene prema novijim tehnološkim dostignućima.



Slika 15. Model korporativnog upravljanja informacijsko - komunikacijskom sigurnošću.

Izvor: **[8]**

Unatoč brojnim izvorima i definicijama sigurnosti IK sustava, može se reći da niti jedan IK sustav nije u potpunosti siguran i zaštićen od raznih napada i prijetnji. Sa tim saznanjem, svaki sustav moguće je opisati terminom „sigurnosno - ranjiv sustav“ koji je potrebno svakodnevno nadgledati i održavati ispravnim i funkcionalnim.

6.2. Normativni okvir sigurnosti u korporativnom okruženju

Razlozi prepoznavanja potrebe za certificiranjem IK sustava i poslovanja organizacije različiti su. Ovise o okruženju u kojem organizacija posluje, ali prije svega o stavu vrhovnog odbora za provedbu sigurnosti i zaštite IK sustava unutar korporativnog okruženja. Prilikom definiranja normativnog okvira koji se temelji na odgovornom poslovanju, ključni čimbenik koji treba uzeti u obzir je da svaka organizacija teži ostvarenju profita.

Uspješna primjena IK sigurnosti zahtijeva sustavno upravljanje u skladu s odgovarajućim standardima i normama. Standard čini politiku učinkovitom, a ona uključuje tehničke opise za određene korištene komponente i procese unutar organizacije. Smjernice imaju značenje jer predstavljaju preporuke i upute stručnjaka koje se temelje na već provedenim analizama. One nisu obavezne, no služe kao pomoć pri uspostavi kvalitetnog programa sigurnosne politike unutar korporativnog okruženja.

Prilikom oblikovanja sigurnosti IK sustava prvi je korak uspostavljanje sigurnosne politike. Zatim slijedi odabir standarda prema kojoj sigurnosna politika odgovara, a na kraju se provode smjernice koje će omogućiti učinkovitost cjelokupne provedbe kvalitetne sigurnosne politike. Vodeća međunarodna norma za upravljanje informacijskom sigurnošću je norma ISO/IEC 27001:2005. Prihvaćena je 2006. godine kao hrvatska norma, koja definira zahtjeve za uspostavu, održavanje i kontinuirano poboljšavanje sustava upravljanja informacijskom

sigurnošću. Certifikatom ISO 27001 se potvrđuje da je informacijska sigurnost u organizaciji provedena na najbolji mogući način. Certifikati i zakoni pomažu organizacijama u izgradnji povjerenja u njihov proizvod ili uslugu, jer on predstavlja nezavisan i rigorozan standard koji ocjenjuje kvalitetu poslovanja organizacije.

Re-certifikacije se u prosjeku vrši svake dvije godine, da bi organizacije bile kontrolirane u skladu sa najnovijim rješenjima i pravilima. Time se organizacije potencijalno nameću kao glavni konkurent na tržištu. To ujedno predstavlja korist organizacijama za dugoročno usklađivanje ciljeva i stvaranja vrijednosti, koje uključuje sigurnost i zaštitu IK sustava unutar korporativnog okruženja.

Dobivanje certifikata ne predstavlja krajnji cilj kvalitetne zaštite. Ono predstavlja dobro polazište za izgradnju i uređenje IK sustava u korporativnom okruženju koji će biti u stanju generirati pozitivne efekte i pokazati svoje prednosti, ublažiti ili eliminirati nedostatke.

6.3. Prednosti i nedostaci informacijsko – komunikacijskih sustava malih korporativnih okruženja

Potencijalne prijetnje i nedostaci su prisutni u svim sustavima. Izvori prijetnji mogu biti razni: pogreške ili kvarovi na resursima, napadi (izvana i iznutra), havarije (požari, elementarne nepogode itd.), ljudske pogreške i drugi.

Istraživanja provedena na institutu za kontinuitet poslovanja (*Bussines Continuity Institute* - BCI) pokazala su da će u prosjeku 20% svih organizacija iskusiti neki oblik neplaniranog događaja barem jednom u svakih pet godina. Gotovo 10% neplaniranih događaja predstavlja opasnost, ali upravo one imaju potencijal oštetiti najveće vrijednosti kompanije, njezino ime i reputaciju. Popravak poslužitelja nije dovoljan za nastavak poslovanja ako zaposlenici nemaju gdje obavljati svoj posao. Dugotrajniji gubitak struje, nedostupnost telefonske i/ili Internet veze, krađe i slični incidenti nisu više problem isključivo IT odjela nego cijele organizacije.

6.3.1. Prednosti zaštite informacijsko – komunikacijskih sustava malih korporativnih okruženja

Male korporacije odlikuje fleksibilnost zbog njihove veličine što im omogućuje vrlo elastičnu ponudu i brzu prilagodbu za zaštitu IK sustava. Također pokazuju veću spremnost da staru tehnologiju zamjene novom, te tu zamjenu brže obavljaju. Osim toga one brže primjenjuju nova znanja i poslovne modele za zaštitu i osiguranje poslovanja. Na taj način ekonomska samostalnost i spremnost na podnošenje rizika u poslovanju potiče da se male korporacije povezuju i umrežavaju radi ostvarivanja uspješnijeg zajedničkog poslovanja, ali i lakšeg podnošenja rizika. Iz navedenih razloga može se zaključiti da male korporacije imaju bolju tržišnu prilagodljivost jer se zbog svoje veličine mogu brzo prilagoditi tržišnim promjenama i novonastalim prilikama te napadima, te bez većih promjena svoju djelatnost orijentirati zahtjevima korisnika.

6.3.2. Nedostatci zaštite informacijsko – komunikacijskih sustava malih korporativnih okruženja

Sa druge strane nedostatak malih korporacija je što nisu uvijek u stanju angažirati vrsne stručnjake, tj. većinu posla pokušavaju realizirati sami. U tom slučaju postoji mogućnost ugrožavanja manjih organizacija zbog nedostatka iskustva i educiranost o zaštiti IK sustava. Podložnija su financijskoj slabošću zbog svojih ograničenih financijskih mogućnosti. Ti parametri ukazuju da male korporacije nisu u mogućnosti ulagati u sigurnost i zaštitu IK sustava u istoj mjeri kao i velike korporacije. Najočitiji nedostatci malih korporativnih okruženja nisu samo troškovi implementacije sigurnosnih rješenja.

Prvenstveno iz razloga obima posla i poslovanja sa partnerima, male korporacije nisu u mogućnosti pratiti isti ritam, jer velike korporacije svojom strukturom i modelom imaju mogućnost proširenja i individualnosti. Velike korporacije na svakoj razini poslovanja imaju definirani sigurnosni pristup i mjere kojima mogu otkriti potencijalne ranjivosti i moguće posljedice. One ulažu puno više u sigurnost IK sustava zbog velike mogućnosti ugrožavanja poslovanja, infrastrukture, imidža korporacije, te korisnika u konačnici što im daje lošu poziciju na tržištu.

Sigurnost IK sustava je jednako važna i malim i velikim korporativnim organizacijama. No izbor kontrola ovisi o organizaciji i njenoj djelatnosti na tržištu. Efikasno upravljanje incidentom može imati pozitivno djelovanje na tržišnu vrijednost korporacije i odnos uključenih partnera. U slučaju sigurnosnog incidenta, korporacija može biti cjenjenija u odnosu na svoje rivale po pitanju načina na koji rješavaju incidente i nude sigurnost svojim partnerima i korisnicima.

Kada se govori o napadima na male korporacije, istraživanje koje je provela sigurnosna tvrtka Symantec prikazuje da je 2012. godine porastao broj napada za čak 300 % u odnosu na 2011. A to je doba kada je počeo istinski procvat modernih načina poslovanja. Napadi na mala korporativna okruženja bilježe rast od 26% i 30%, prema *Internet Security Threat* izvješću (travanj 2015). Problematičan detalj je svakako to da 60 % svih ciljanih napada ide na mala korporativna okruženja.

Organizacije bi trebale nadograđivati i ažurirati novije verzije sustava kako ne bi propustile nove mogućnosti. Jedno rješenje koje će zaštiti IK sustav predstavlja malo ograničenje prema zlonamjernim korisnicima, stoga je potrebno ulagati u nova rješenja, biti inovativan i otvoren prema novim rješenjima.

Još uvijek pojedine organizacije posjeduju ograničene mjere zaštite, ne ulažu u svoje resurse, te se izlažu rizicima zlonamjernih prijetnji. Tim postupcima, ugrožavaju organizacijsko okruženje, tržišni utjecaj, poslovanje i ono najbitnije imovinu organizacije i zaposlenika. Iz svega prethodno navedenog vidi se da je proces sigurnosnog upravljanja i zaštite IK sustavima prilično složen proces koji zahtjeva mnogo znanja. Najsigurniji način je odabir adekvatnih osoba, educiranih stručnjaka koji se profesionalno bave navedenim područjem.

6.3.3. Razlozi ulaganja u sigurnost i zaštitu informacijsko – komunikacijskog sustava unutar korporativnog okruženja

Istraživanjem dostupnih internetskih [15] i knjižničnih izvora [29] te iskustvom velikih korporativnih okruženja u vezi s unapređenjem sigurnosti IK sustava utvrđeno je da se za procjenu rizika sigurnosti IK sustava koriste raznovrsni pristupi, metode, tehnike i alati. Na temelju analize rizika provodi se postupak kojemu je cilj uočiti ranjivosti sustava, ustanoviti moguće prijetnje, te na konkretan način kvantificirati moguće posljedice, kako bi se odabrao najefikasniji način zaštite, odnosno procijenila opravdanost uvođenja dodatnih mjera zaštite.

Prema „*Gartner* i *Standish Group*" istraživanju prosječan financijski gubitak uslijed prekida odvijanja poslovnih procesa IK sustava unutar jednog sata iznosio je [30]:

- investicijsko posredništvo 6,5 milijuna USD,
- kartično poslovanje (autorizacija kreditnih kartica) oko 2,6 milijuna USD,
- logistika i paketna distribucija oko 150.000 USD,
- rezervacijski sustavi za zrakoplove oko 90.000 USD i
- *fortune* 500 lista (lista Američkih organizacija) - prosječan gubitak je oko 96.000 USD po minuti.

Dakle, iz navedenog istraživanja vidljivo da organizacije čiji procesi ovise o IK sustavima imaju velike financijske gubitke ukoliko dođe do prekida njihovih izvođenja. Dostupnost IK sustava je bitna ne samo jer su veliki financijski gubitci u slučaju nedostupnosti sustava, već uz pomoć njih organizacije ostaju u utrci s konkurencijom.

Organizacija provodi mjere za osiguranje željene razine funkcionalnosti sustava te integriteta podataka. U nastavku su nabrojani razlozi ulaganja u sigurnost IK sustava u korporativnom okruženju:

- Minimalno ometanje redovnog rada korporativnog okruženja na temelju brze implementacije sigurnosnih rješenja i zaštite IK sustav (programi + edukacija zaposlenika).
- U kratkom vremenskom periodu provode se određeni noviteti i poboljšanja u sustavu, kako bi se u pratio tehnološki napredak te bilo u toku sa najnovijim ugrozama. Na temelju toga organizacije mogu osigurati bolji povrat investicije što rezultira poboljšanjem poslovnih procesa.
- Pokazuje se mogućnost integracije procesa i podataka.
- Podaci vezani za organizaciju, partnera ili kupca bivaju sigurniji, te se omogućava cjelokupnom korporativnom okruženju sigurno poslovanje.
- Uz konkurentu prednost osigurava se i povjerenje partnera.
- Pružaju se mnoga rješenja kroz modularnost i prilagodljivost promjenama u poslovnim procesima i organizacijskim strukturama.
- Skalabilnost i strukturiranost IK sustava pruža mogućnost rasta poslovnog uspjeha.

- Učinkovitost zaštite i funkcionalnost rješenja su ovisni parametri o broju korisnika, informacija ili podataka i količine poslovnih procesa i uspjeha.
- Na kraju cjelokupnog procesa sigurnost omogućava zaštitu podataka od neželjenih i neovlaštenih intervencija koja spada među najvažnije zahtjeve korporativnog IK sustava.
- Kvalitetan program, odnosno uređaj/aplikacija ili softver predstavlja sloj zaštite i korištenjem takvog oblika ili modela zaštite, te pravilnim očuvanjem organizacija postiže prednost pred konkurencijom, veći profit i poslovni uspjeh.
- Mogućnost zaštite IK sustava putem *outsourcinga* organizacije kojoj je primarna zadaća sigurnost i zaštita IK sustava, kako bi se organizacija mogla usredotočiti na svoju glavnu aktivnost/uslugu i razvoj novih poslovnih procesa.

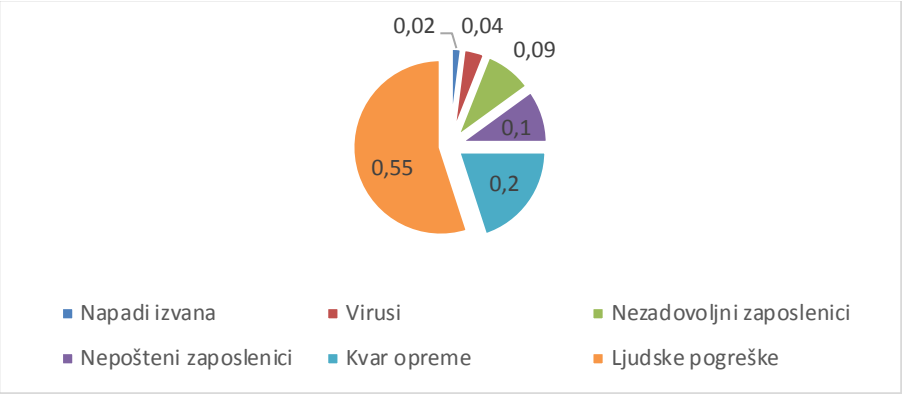
6.4. Smjernice i preporuke sredstava zaštite informacijsko – komunikacijskog sustava

Korporativno okruženje prema današnjim uvjetima poslovanja intenzivno komunicira s unutrašnjim i vanjskim subjektima. No pristup na tržištu povlači za sobom i izlaganje pred različitim prijetnjama ne isključivo na IK sustav, nego i na čitavo poslovanje organizacije. Posve razumno je da IK sigurnosni stručnjaci moraju znati predvidjeti potencijalne prijetnje i rizike tokom različitih procesa poslovanja. Oni također analiziraju i provode odgovarajuće mjere. Uz to stručnjaci imaju mogućnost korištenja različitih programa, komponenata, uređaja i aplikacija koje se danas nude za olakšavanje postupka kvalitetne obrane IK sustava. Budući da su poslovne informacije od neprocjenjive važnosti, korporativni IK sustav zauzima važnu ulogu u evidentiranju, pohranjivanju i izvješćivanju o poslovnim događajima nastalima u korporativnom okruženju.

Istraživanje prema [11] potvrđuje da približno 40% napada dolazi izvana (putem Interneta), a oko 60% napada dolazi unutar organizacije. Statistički podaci koji su prikazani na grafu 1 pokazuju da najvećim postotkom probleme sigurnosti unutar korporativnog okruženja uzrokuju ljudske greške. Takve posljedice se najčešće događaju zbog nedovoljne pažnje i educiranosti zaposlenika. Educiranjem zaposlenika vjerojatnost njihove pogreške se smanjuje te se pritom povećava sigurnost i integritet IK sustava. Pridržavanjem propisanih pravila organizacije pokušava se suzbiti zlouporaba sustava sa aspekta zaposlenika, te se uz to uvode kontrole pristupa i definiraju sankcije za one koji ih se ne pridržavaju.

Prema rezultatima iz grafa 1 vidljivo je da je za sigurnost poslovnih procesa potrebna itekako visoka razina kontrole i zaštite IK sustava. No kako bi se osigurala učinkovitost suradnje i poslovanja unutar korporativnog okruženja, nužno je koristiti određena sredstva za zaštitu IK sustava, koja su definirana u prethodnim poglavljima. Korporativno okruženje sve više shvaća važnost zaštite IK sustava, što zahtjeva veću edukaciju zaposlenika. Kroz provedbu edukacije zaposlenika i poticanjem za bolji poslovni uspjeh daje se značaj za smanjenje sigurnosnih

napada. Bez kvalitetnog plana i programa sigurnosti IK sustava nije moguće u cijelosti zaštiti sustav, korisnika niti dobrobit korporativnog poslovanja unutar okruženja.



Graf 1. Problemi sigurnosti u korporativnom okruženju.

Izvor: **[11]**

Stoga postoji niz sredstva zaštite kojima je moguće ostvariti kvalitetnu sigurnost IK sustava, a u nastavku su spomenuta najčešća sredstva koje organizacije koriste.

Zaštitno sredstvo najčešće korišteno predstavlja vatrozid koji je opisan u poglavlju dva. Izvor [31] navodi kako je *Sidewinder* od strane *Secure Computing-a* jedan od najsigurnijih dostupnih vatrozida i do sada nikada nije bio u potpunosti hakiran. Vatrozid se sastoji od pet elemenata: vatrozid, antivirusni/antispam program, virtualna privatna mreža i sustav za detekciju/prevenciju. Uz vatrozid korisno sredstvo zaštite predstavlja IPS koji je razvijeniji u odnosu na vatrozid jer automatski sprema sumnjive pakete u posebnu mapu.

UTM (*Unified Threat Management*) je najnoviji trend kojim se nastoji spriječiti prijetnja sustavu. Pruža različite mogućnosti kao antivirus, VPN, usluga vatrozida, antispam, kao i prevenciju upada. Najveće prednosti su jednostavnost rada i konfiguracija. S obzirom na to da se njegove sigurnosne značajke mogu brzo ažurirati, prijetnje se relativno rano otkriju.

Uz uređaje za zaštitu IK sustava koriste se i logičke kontrole zaštite kao autentifikacijski sustav koji mora biti sposoban prepoznati koji korisnik ili zaposlenik pristupa mreži organizacije. U korporativnom okruženju fizički dokaz više ne može predstavljati dokaz identiteta, stoga se korisniku ili zaposleniku dodjeljuje ID (kartica ili slična metoda autentifikacije) putem koje korisnik ili zaposlenik ostavljaju zapis u sustavu. Na temelju registracije u sustavu korisniku ili zaposleniku je dozvoljen pristup, te je uz to moguće uočiti potencijalne sumnjive radnje zlonamjernog korisnika ili zaposlenika. Kako bi se povećala učinkovitost sigurnosnog sustava, potrebno je provesti mnogo jači oblik autorizacije. Kao najjače sredstvo autentifikacije izvor [31] navodi kombinaciju hardverskog uređaja (*token*, pametne kartice, biometrijski uređaji) i nečega što korisnik zna da bi mogao izvršiti prijavu u sustav.

6.5. Prioritet kvalitetne sigurnosne politike

Zlonamjerni napad predstavlja svaki stvarni ili potencijalno štetni događaj odnosno ugrozu koja negativno utječe na sigurnost IK sustava, stoga su u daljnjem tekstu definirane preporuke za kvalitetnu implementaciju sigurnosne politike unutar IK sustava. U suštini, napadi imaju za posljedicu gubitak povjerljivosti, cjelovitosti ili raspoloživosti podatka. Iz tog razloga potrebno je održavati kontakte s organizacijama koje se bave sigurnošću, zakonodavnim i koordinativnim tijelima, pružateljima IK usluga te razmotriti mogućnost članstva u sigurnosnim grupama i forumima. Razmjena informacija treba biti ograničena radi osiguranja povjerljivih korporativnih podataka i informacija.

6.5.1. Postupci provedbe sigurnosne politike

Sigurnosna politika opisana u prethodnim poglavljima pokazuje da je lako formalno propisati postupke sigurnosne politike IK sustava, no dosta je teže, a i zahtjevnije inzistirati na njenoj sustavnoj provedbi. Iz primjera je vidljivo da, osim postojanja formalne sigurnosne politike, ipak više pozornosti treba posvetiti njezinoj provedbi u svakodnevnom poslovanju kako bi se IK resursi poslovanja štitili ili koristili na učinkovit način.

Vrlo često povećanje razine sigurnosti može rezultirati negativnim utjecajem na funkcionalnosti i jednostavnost obavljanja zadataka. Valja izdvojiti da kvalitetna identifikacija IK resursa te procjena rizika predstavlja važan element u procesu implementacije sigurnosne politike jer se tako mogu izdvojiti elementi IK sustava prema njegovoj vrijednosti za organizaciju. Korporativno upravljanje sigurnošću IK sustava zato predstavlja zahtjevan i odgovoran zadatak kojem se pristupa detaljno i analitički.

Prije implementacije sigurnosne politike potrebno je provesti identifikaciju rizika, odrediti veličinu rizika i potencijalnih nedostataka za pružanje određenih prava pristupa drugim organizacijama/partnerima. Prilikom identifikacije rizika potrebno je definirati kojim organizacijskim procesima i podacima treće strane pristupaju i na koji način im se omogućava pristup (fizički, logički pristup ili pristup mreži organizacije). Nužno je odrediti vrijednost i osjetljivost podataka kojima će pristupiti treća strana, te implementirati sigurnosne kontrole za zaštitu vrijednosti i sadržaja IK sustava za koje treća strana nema pristupa. Također je potrebno definirati razinu prava pristupanja, te koji korisnici imaju prava. Kako bi se povećala sigurnost potrebno je odrediti način identifikacije i postupak autorizacije nad korisnicima.

6.5.2. Dokumenti sigurnosne politike

Kroz dokumente i ugovore se potiče pridržavanje sigurnosnih postupaka i mjera za sve strane koje sudjeluju u procesu poslovanja. Nakon implementacije i provjere svih sigurnosnih kontrola i točaka pruža se pravo pristupa trećoj strani prema unaprijed dogovorenim pravilima ugovora. Unutar ugovora je potrebno definirati uvjete kako ne bi došlo do nesporazuma između organizacije i partnera/treće strane, te je nužno provesti i uključiti sigurnosnu politiku. Formalni ugovor se sastoji i referencira na sva pravila i zahtjeve sigurnosti, što osigurava usklađenost sa politikom sigurnosti organizacije i trenutnim standardima. Procedure koje

uključuju zaštitu imovine (izgubljena, izmijenjena), posebne kontrole sigurnosti povrata (*backup*), trajno uništavanja podataka na kraju ugovorenog odnosa (ili za točno određeno vrijeme), te integritet i dostupnost također trebaju biti unutar formalnog ugovora.

Formalni ugovor je potrebno sastaviti da bi i ovlaštene osobe provodile održavanje, praćenje korisničkih aktivnosti, nadzor sigurnosnih kontrola i ugovorene odgovornosti (npr. odgovornost prilikom instalacije i održavanja softvera/hardvera). Također je potrebno sastaviti detaljni opis servisa koju su dostupni, kroz razinu usluge i odgovarajuće obveze koji trebaju biti u skladu sa pravnim zahtjevima. Da bi poslovanje bilo na prihvatljivoj razini potrebno je provesti zaštitu zajedničkog poslovanja, sporazume o kontroli pristupa (dopuštene metode pristupa, te kontrolu i korištenje jedinstvenih identifikatora i proces autorizacije za dodjelu prava pristupa). Za jasno definiranje strukture potrebno je provesti jasne izvještaje i način izvještavanja unutar kojeg se provodi proces upravljanja promjenama, edukacija korisnika i timova o metodama, procedurama i sigurnosnim aspektima zaštite.

6.5.3. Proces odgovornosti kroz sigurnosnu politiku

Sigurnosna politika organizacije unaprijed definira pravila koje je neophodno koristiti pri sklapanju ugovora sa novim zaposlenikom, odnosno korisnikom. Ugovor se sastoji od brojnih podataka što čine pojašnjenja i stav kako bi novi zaposlenik, organizacija ili treća strana, prije dobivanja prava pristupa organizaciji, morali potpisati ugovor o povjerenju prema zakonskim pravima i odgovornostima svakog zaposlenika, korisnika ili partnera, te o akcijama koje je nužno provesti ukoliko dođe do nepridržavanja definiranih pravila prema sigurnosnoj politici. Jasno moraju biti propisani procesi i odgovornosti prilikom prekida radnog odnosa, raskida ugovorne obveze, promjene radnog mjesta i slično. Na temelju toga zaposlenik, partner ili treća strana moraju vratiti u posjed organizaciji, sve materijalne vrijednosti koje su dobili na korištenje tijekom radnog odnosa, osim ako je ugovorom drugačije dogovoreno. Slijedom toga nakon raskida ugovora oduzimaju im se sva prava pristupa imovini i drugim osjetljivim vrijednostima organizacije.

6.5.4. Primjena i aktivnosti sigurnosne politike

Sigurnosna politika organizacije prilagođava se potrebama, te ona nije jednaka za sva okruženja. Sigurnosnu politiku predstavlja službena izjava ili definirani plan organizacije koji obuhvaća smjernice i prihvatljive postupke. Sigurnosna politika treba sadržavati sljedeće bitne aktivnosti:

- poštivanje pravila definirana sigurnosnom politikom organizacije,
- nepoštivanjem pravila provode se kazne i sankcije odgovornih osoba,
- kvalitetna provedba sigurnosne politike pruža bolje rezultate i
- sigurnosnu politiku je potrebno implementirati prema definiranim standardima i smjernicama.

Sigurnosna politika se primjenjuje unutar korporativnog okruženja da se u prvom redu osigura fizička i osobna sigurnost. Također sigurnosnom politikom se utvrđuje kontrola

pristupa, usklađenost sa zakonskim propisima, te obuhvaćaju područja razvoja i održavanja IK sustava. Ona se uz to primjenjuje za kvalitetno upravljanje operacijama i komunikacijama, te za planiranje kontinuiranosti poslovnih procesa da bi se smanjili povremeni prekidi rada sustava.

Osiguranje IK sustava nije moguće isključivo upotrebom sredstava zaštite, te se iz tog razloga uvode dodatne mjere, među kojima je i definiranje sigurnosne politike. Za zaštitu vrijednosti IK sustava koje uključuju podatke, opremu i programsku podršku, određuju se prihvatljivi i neprihvatljivi načini ponašanja, što predstavlja ujedno i primarnu ulogu sigurnosne politike.

7. Zaključak

U ovom diplomskom radu provedena je analiza sigurnosti i zaštite IK sustava u korporativnom okruženju. IK sigurnost predstavlja sve složeniji segment IK tehnologije, ponajviše iz razloga implementacije IT tehnologije na svim funkcionalnim razinama unutar korporativnog okruženja. S obzirom na promjenjive i nestabilne okolnosti današnjice potrebno je kontinuirano provoditi proces kontrole, zaštite i sigurnosti u poslovanju.

Analiza sigurnosnog modela organizacije prikazuje konkretan način postavljanja kvalitetne strukture za zaštitu IK sustava. Nove mjere, pravila, standardi i propisi koji se svakodnevno razvijaju i nude na tržištu zahtijevaju pravilan pristup za unaprjeđenje dijelova IK sustava. Njima se provodi konstantan nadzor koji pruža sigurno poslovanje u korporativnom okruženju. No kod svega navedenog postoje potencijalne ugroze koje se mogu pojaviti na komunikacijskoj razini i prouzročiti izravne ili neizravne financijske gubitke. Iz tog razloga potrebno je, osim kvalitetnog IT osoblja u sustavu, podizati svijest krajnjih korisnika kako bi se pozitivno utjecalo na stupanj sigurnosti IK sustava.

Arhitekturom organizacije pojašnjeni su načini komunikacije i provedbe kvalitetnog programa suradnje koji je nužan za osiguranje organizacija, te da bi imale nesmetan rad i kvalitetnu provedbu poslovnih projekata. Konkretnim potezima i shvaćanjem problema ugrožavanja IK sustava povećat će se stupanj spremnosti za nadolazeće tehnološke napretke, smanjiti mogućnost nastajanja štete i vjerojatno razotkriti više prijetnji. Tehnološkim napretkom razvijeni su brojni alati i metode koji omogućuju postavljanje mjernih točaka unutar IK sustava za analizu prometa i uočavanju nedostataka.

Analizom organizacijskog modela i načina zaštite IK sustava iz navedenog primjera prikazano je kako organizacija konstantno unaprjeđuje i prati sredstva i metode zaštite. Uz to uspješno provodi poslovanje kroz certifikate koje posjeduje i koji se na godišnjoj razini potvrđuju. Na temelju toga moguće je donositi određene zaključke kako organizacija pokazuje sposobnost zaštite IK sustava u najvećoj mogućoj mjeri prateći sigurnosne standarde, mjere i načine zaštite.

Za planiranje kvalitetne sigurnosti IK sustava daje se prednost individualnim rješenjima, jer se iz tog pristupa otežava iskorištavanje i zlonamjerne radnje od strane neovlaštenih korisnika. Uz to sigurnost IK sustava vrlo je kompleksna i široka tema u kojoj je jasna činjenica da bez kvalitetnog programa sigurnosti sustav nije moguće u cijelosti zaštiti. Kvaliteta plana i programa sigurnosti IK sustava omogućuje uspostavu sigurnosnog segmenta na svim dijelovima sustava, sa bilo kojeg aspekta, pa prema tome program za dostizanje učinkovite zaštite IK sustava se predstavlja kroz definiranje sigurnosne politike unutar organizacije.

LITERATURA

[1] Dragičević, D.: Kompjutorski kriminalitet i informacijski sustavi, Zagreb, Informer, 1999.

[2] URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-05-265.pdf (pristupljeno: svibanj 2017.)

[3] Zakon o informacijskoj sigurnosti: Članak 7. Mjere informacijske sigurnosti propisat će se uredbom koju donosi Vlada Republike Hrvatske, a standardi za provedbu mjera propisat će se pravilnicima koje donose čelnici središnjih državnih tijela za informacijsku sigurnost, Narodne Novine, 79/07, Zagreb, 2007. (pristupljeno: lipanj 2017.)

[4] Krutz, R., L.; Vines, D., V.; The CISSP Prep Guide - Mastering the Ten Domains of Computer Security, Toronto: John Wiley & Sons, Inc., 2001.

[5] Grbavac V.&J.: Komunikacijski sustavi, DOIK, Zagreb, 2008.

[6] Bača, M.: Uvod u računalnu sigurnost, Narodne Novine d.d., Zagreb, svibanj 2004.

[7] Harris, S., CISSP, All-in-One, 3rd Ed. McGraw-Hill/Osborne, 2005.

[8] Autorizirani nastavni materijali kolegija Sigurnost i zaštita informacijsko komunikacijskog sustava URL: http://e-student.fpz.hr/Predmeti/S/Sigurnost_i_zastita_informacijsko_komunikacijskog_sustava/Materijali/SZIKS_-_P01-P02-S01-P03-P4-P5-S02-P06-P07-S03-P08-P9-S04.pdf (pristupljeno: svibanj 2017.)

[9] Charles P. Pfleger, "Security in Computing", Prentice Hall PTR, 1997.

[10] URL: http://novilist.hr/Vijesti/Gospodarstvo/Alen-Ostojic-Bez-cyber-zastite-tvrtka-pada-u-nekoliko-minuta (pristupljeno: svibanj 2017.)

[11] Network Applications Consortium (NAC), Enterprise Security Architecture, a Framework and Template for Policy Driven Security, 2004.

[12] Sherwood, J., Clark, A., Lynas, D., Enterprise Security Architecture, CMP Books, 2005.

[13] Hadjina, N.: Zaštita i sigurnost informacijskih sustava (nastavni materijali sa zbirkom zadataka), Fakultet elektrotehnike i računalstva Zagreb, Zagreb,2009.

[14] Srića, V.: Informatički inženjering i menadžment, Društvo za razvoj informacijske pismenosti, Zagreb, 1990.

[15] Puthuseer, Vinod Kumar: ISMS Implementation Guide,

URL: http://www.infosecwriters.com/Papers/VKumar_ISMS.pdf (pristupljeno: lipanj 2017.)

[16] Peltier, T.R., Information Security Risk Analysis, 2nd Ed, Auerbach Publications, 2005.

URL: http://www.nojutso.com/downloads/diplomado/ISRA%20Peltier.pdf (pristupljeno: lipanj 2017.)

[17] National Institute of Standards and Technology, Managing Risk from Information Systems, An Organizational Perspective, NIST SP 800-39 (2nd Public Draft), April 2008.

[18] URL: https://www.hakom.hr/UserDocsImages/2014/izvjesca_i_planovi/Godisnji%20program%20rada%20HAKOM-a%20za%202015.pdf (pristupljeno: svibanj 2017.)

[19] URL: https://www.enisa.europa.eu/topics (pristupljeno: svibanj 2017.)

[20] URL: http://www.cis.hr/dokumenti/cobitframework-5.html (pristupljeno: svibanj 2017.)

[21] URL: https://www.tmforum.org/about-tm-forum/ (pristupljeno: svibanj 2017.)

[22] The International Organization for Standardization – ISO.

Dostupno na: http://www.iso.org/iso/home/name_and_logo.htm (pristupljeno: srpanj 2017.)

[23] Cvitić, I.: Diplomski rad: Projektiranje sigurne infrastrukture informacijsko komunikacijskog sustava Fakulteta prometnih znanosti, Fakultet prometnih znanosti, Zagreb, 2013.

[24] Vacca, J.A.: Network and system security, Elsevier, USA, 2010.

[25] Bidgoli, H.: Handbook of Information Security, Wiley, 2006.

[26] URL: https://sysportal.carnet.hr/system/files/sigurnosna_politika_ustanove.pdf (pristupljeno: srpanj 2017.)

[27] URL: http://sigurnost.zemris.fer.hr/ISMS/2008_kovacevic/primjerSP_2.html (pristupljeno: lipanj 2017.)

[28] Interni dokumenti realnog poslovnog subjekta, Zagreb, 2013. – 2017.

[29] Antoliš,K. i dr.:Sigurnost informacijskih sustava, Algebra d.o.o., Zagreb, 2010.

[30] Spremić, M.: Primjena IT u financijskom izvještavanju: Računovodstveni informacijski sustavi, Ekonomski fakultet Zagreb, Zagreb, 2008.

[31] Vacca, J. R.: Network and System Security; Oxford; Elsevier Inc.; 2010.

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

AKRONIMI

BS	(engl. British Standard) – Britanski standard
CCSC	(engl. Commercial Computer Security Center) – Centar za komercijalnu sigurnost računala
CCSN	(engl. Country Customer Service Networks) - Mreže za korisničku službu unutar pojedine zemlje
CERT	(engl. Computer Emergency Response Team) - Tim za hitne računalne intervencije
COBIT	(engl. Control Objectives for Information related Technology) - Ciljevi kontrole za IK i povezane tehnologije
CSO	(engl. Chief Security Officer) – Voditelj sigurnosti
DSA	Sigurnost poslovne suradnje
ECMA	(engl. Euorpiean Computer Manufactures Association) – Europska udruga proizvođača računala
ENISA	(engl. European Network and Information Security Agency) – Europska agencija za mrežnu i informacijsku sigurnost
EU	(engl. European Union) - Europske unija
HAKOM	Hrvatska regulatorna agencija za mrežne djelatnosti
IDS	(engl. Intrusion Detection System) - Sustav detekcije neovlaštenog upada
IEC	(engl. International Electrotechnical Commission) - Internacionalna komisija za elektrotehniku
IK	(engl. information and communication) - Informacije i komunikacije
IPS	(engl. Intrusion Prevention System) - Sustav zaštite od neovlaštenog upada
ISMS	(engl. Information security management system) – Sustav upravljana informacijskom sigurnošću
ISO	(engl. International Organization for standardization) – Internacionalna organizacija za standardizaciju
IT	(engl. Information Technology) – Informacijske tehnologije
ITSO	(engl. International Technical Support Organization) - Međunarodna organizacija za tehničku podršku
NAT	(engl. Network address translation) – Prevođenje mrežne adrese

NATO	(engl. North Atlantic Treaty Organisation) – Sjeverno - atlantski vojni savez
NDA	(engl. National Distribution Authority) - Ugovori o tajnosti podataka
NGFW	(engl. Next Generation Firewall) – Vatrozid sljedeće generacije
NSA	(engl. National Security Authority) - Ured Vijeća za nacionalnu sigurnost
OS	(engl. Operation system) – Operacijski sustav
OSI	(engl. Open System Interconnection) - Međusobno povezivanje otvorenih sustava
QoS	(engl. Quality of Service) – Kvaliteta usluge
SAA	(engl. Security Accreditation Authority) - Tijelo za sigurnosne akreditacije
SLA	(engl. Service-level agreement) - Ugovor o razini usluge
SSL	(engl. Secure Socket Layer) - Sigurnosni protokol komunikacije
UPS	(engl. Uninterruptable Power Supply) – Neprekidan izvor napajanja
USB	(engl. Universal serial bus) - Univerzalna serijska sabirnica
UTM	(engl. Unified Threat Management) – jedinstveno upravljanje prijetnjama
UVNS	Ured Vijeća za nacionalnu sigurnost
VLAN	(engl. Virtual Local Area Network - VLAN) - Virtualna lokalna mreža
VPN	(engl. Virtual Private Network) – Virtualna privatna mreža
ZSIS	Zavod za sigurnost informacijskih sustava

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem da je _____DIPLOMSKI RAD_____

(*vrsta rada*)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom ANALIZA SIGURNOSTI I ZAŠTITE INFORMACIJSKO - KOMUNIKACIJSKOG SUSTAVA U KORPORATIVNOM OKRUŽENJU, na mrežnim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, _____ _____