Sigurnost informacijskih sustava zatvora u Gospiću

Matković, Krešimir

VELEUČILISTE „NIKOLA TESLA“ U GOSPIĆU

Krešimir Matković

SIGURNOST INFORMACIJSKIH SUSTAVA ZATVORA U GOSPIĆU
SAFETY OF INFORMATION SYSTEMS PRISON IN GOSPIĆ

Završni rad

Gospić, 2018.

VELEUČILISTE „NIKOLA TESLA“ U GOSPIĆU

Prometni odjel

Stručni studij cestovnog prometa

SIGURNOST INFORMACIJSKIH SUSTAVA ZATVORA U GOSPIĆU
SAFETY OF INFORMATION SYSTEMS PRISON IN GOSPIĆ

Završni rad

MENTOR

Mile Vičić, mag. oec.

predavač

STUDENT

Krešimir Matković

MBS: 2961000148/08

Gospić, svibanj 2018.

Veleučilište „Nikola Tesla“ u Gospiću

Prometni odjel

Gospić, 5.5. 2018.

ZADATAK

za završni rad

Pristupniku KREŠIMIR MATKOVIĆ JMBAG: 2961000148/08

Studentu stručnog studija CESTOVNOG PROMETA izdaje se tema završnog rada pod nazivom

SIGURNOST INFORMACIJSKIH SUSTAVA ZATVORA U GOSPIĆU

–

SAFETY OF INFORMATION SYSTEMS PRISON IN GOSPIĆ

–

Sadržaj zadatka :

1. Općenito o informacijskim sustavima
2. Sigurnost informacijskih sustava
3. Informacijski sustav u Zatvoru u Gospiću

Završni rad izraditi sukladno odredbama Pravilnika o završnom radu Veleučilišta „Nikola Tesla“ u Gospiću.

Mentor: MILE VIDIĆ zadano: 5.4.2018., _____

(ime i prezime) (nadnevak) (potpis)

Pročelnik odjela: Mladena Čuljat, pred. predati do: 5. lipnja 2018. _____

(ime i prezime) (nadnevak) (potpis)

Student: KREŠIMIR MATKOVIĆ primio zadatak: 5.4.2018., _____

(ime i prezime) (nadnevak) (potpis)

Dostavlja se:

- mentoru
- pristupniku

IZJAVA

Izjavljujem da sam završni rad pod naslovom **„Sigurnost informacijskih sustava Zatvora u Gospiću“** izradio samostalno pod nadzorom i uz stručnu pomoć mentora **Mile Vičića, mag. oec**.

Student:

Krešimir Matković

SAŽETAK

U modernom društvu svaka ljudska djelatnost zahtijeva pristup mnoštvu informacija koje su nužne za donošenje poslovnih odluka. Do tih informacija se dolazi prikupljanjem, obradom, distribucijom i pohranjivanje podataka, što je kontinuiran proces nužan u svim područjima ljudskog djelovanja. Pri tome je važno da informacije budu točne, pouzdane i pravovremene, te dostupne samo onim korisnicima kojima su namijenjene. Informacije u modernom društvu imaju određenu vrijednost, pa su često predmet napada mnogih kriminalnih skupina. Stoga je nužno osigurati što viši stupanj zaštite podataka, što se postiže kvalitetnom opremom i educiranim korisnicima. Briga za sigurnost podataka zadaća je svakog korisnika informacijskog sustava.

Ključne riječi: informacijski sustav, podatci, sigurnost, hardver, softver

SUMMARY

In modern society, every human activity requires access to a multitude of information that is necessary for making business decisions. This information comes from collecting, processing, distributing and storing data, which is a continuous process necessary in all areas of human activity. It is important for the information to be accurate, reliable and timely, and only accessible to those users who are intended to do so. The information in the modern society has a certain value and are often subject to the attack of many criminal groups. It is therefore necessary to ensure the highest level of data protection, which is achieved with quality equipment and educated users. The concern for data security is the task of each user of the information system.

Key words: information system, data, security, hardware, software

SADRŽAJ

1. UVOD

Svaka ljudska djelatnost u modernom društvu zahtijeva pristup mnoštvu informacija bez kojih bi bilo nemoguće donijeti bilo kakvu korisnu poslovnu odluku. Stoga informacije postaju sve važnija roba bez kojih je bilo kakvo poslovanje nezamislivo. Sustav koji objedinjuje prikupljanje podataka, njihovu pohranu, obradu i pristup željenim informacijama zove se informacijski sustav. Čine ga svi podatci, oprema, procedure i ljudi koji njima rukuju.

Zbog svog značaja i vrijednosti, informacijski sustavi su oduvijek bili i uvijek će niti izloženi raznim oblicima ugroze. Svaki informacijski sustav ima određene slabosti i nedostatke, a kako je i čovjek kao nesavršeno biće dio tog sustava, sama njegova nazočnost u sustavu čini ga ranjivim. Tehnološki razvoj u uporaba računalstva i računalnih mreža u pohrani i razmjeni podataka znatno je olakšala obradu i razmjenu informacija, ali je znatno i povećana mogućnost neovlaštenog pristupa, krađe ili izmjene tih podataka. U mnogim poduzećima veliki dio zaposlenika ima pristup određenom dijelu informacija, iako često nisu svjesni važnosti zaštite niti svih mogućnosti ugroze podataka, kao ni posljedica koje mogu nastati zbog ugroze informacijskog sustava.

Jedno od glavnih obilježja modernog društva je dinamičnost u mnogim segmentima ljudske djelatnosti. Dinamično poslovno okružje, stalne promjene na tržištima, tehnološki razvoj osobito u informatičkom sektoru te česte zakonodavne promjene zahtijevaju brze promjene i prilagodbe informacijskih sustava. Može se zaključiti da su i u informacijskom sustave nužne stalne promjene s ciljem podizanja kvalitete prikupljanja, obrade i distribucije podataka uz stalno podizanje razine njihove sigurnosti.

1.1. Predmet rada

Predmet ovog rada je informacijski sustav u Zatvoru u Gospiću. Zatvor kao specifična institucija u kojoj se nalaze specifične kategorije ljudi osobito je osjetljiv na ugrozu informacijskog sustava. Osim zatvorenika veliki sigurnosni rizik čine posjetitelji, te službeno osoblje koje ima pristup zatvorenicima, poput odvjetnika, medicinskog osoblja, vještaka i slično.

1.2. Cilj i svrha rada

Svrha ovog rada je uvid u sigurnost informacijskog sustava u zatvoru. Nijedan sustav nije savršen, a najčešći razlozi ugroze sustava su ljudski faktor i tehnička ograničenja. Ugroza informacijskog sustava može biti motivirana stjecanjem osobne koristi, a njen cilj može biti i nanošenje štete i otežavanje rada određenoj instituciji ili ustanovi. Glavna obilježja zatvorskog sustava u Hrvatskoj, pa tako i zatvora u Gospiću, jesu ograničenost smještajnih kapaciteta i nedostatak ljudstva. Ova dva čimbenika znatno utječu na sigurnost informacijskog sustava u zatvoru.

1.3. Struktura rada

Rad se sastoji od četiri cjeline. U uvodnom dijelu su opisani cilj i svrha, te predmet rada. Drugi dio naziva „Općenito o informacijskim sustavima“ uvodi čitatelja u osnove informacijskih sustava, definira pojmove kao što su podatak, informacija, organizacija, sustav i slično, te opisuje zadaće i svojstva informacijskih sustava.

U trećem dijelu je opisan informacijski sustav Zatvora u Gospiću. To je složen sustav koji mora osigurati unos, obradu i prijenos podataka do svih korisnika, te je virtualnom privatnom mrežom povezan i s Ministarstvom pravosuđa.

Četvrti dio opisuje oblike ugroze informacijskih sustava, te mjere koje se poduzimaju s ciljem podizanja razine sigurnosti.

Zadnji dio je Zaključak u kojem je autor naveo spoznaje do kojih je došao tijekom izrade rada. Na kraju rada je popis literature, te popis slika.

2. OPĆENITO O INFORMACIJSKIM SUSTAVIMA

Ljudi, po prirodi društvena bića, tisućljećima žive u zajednicama s ciljem što jednostavnijeg postizanja željenih ciljeva na što jednostavniji način i uz što manje zalaganja. Iz navedenog se može zaključiti da organizacija predstavlja oblik udruživanja ljudi s ciljem ostvarivanja određenih zadaća, a čine je ljudi, rad, sredstva za rad i predmeti rada.[1] Ako je glavna misija organizacije određena poslovna djelatnost, takva organizacija se može nazvati poslovna organizacija.

Sustav je skup elemenata povezanih u neku cjelinu u kojoj su definirana obilježja tih elemenata i veze među njima.[2] On je dosta širok pojam i mogu ga činiti bilo koji elementi koji mogu tvoriti neku smislenu cjelinu. Primjeri sustava su Microsoft, Veleučilište „Nikola Tesla“ u Gospiću, GNK Dinamo, ali i puno manje cjeline poput živčanog sustava miša ili krvožilnog sustava ovce. Može se zaključiti da organizacija može sadržavati mnoštvo sustava (sustav proizvodnje, sustav prodaje, sustav prijevoza, sustav osiguranja,...), a istovremeno i sustav može biti sačinjen od mnoštva organizacija (sustavi kao što su NATO, Europska unija, Samsung, Katolička crkva, HP i drugi).

Jedna od važnih komponenti svake moderne poslovne organizacije je informacijski sustav. Za svaku modernu poslovnu organizaciju, neovisno o njenoj veličini i složenosti, nužno je učinkovito prikupljanje poslovnih informacija, njihova analiza i iznalaženje optimalnih rješenja za sve poslovne probleme. Informacijski sustav je skup svih povezanih dijelova nužnih za prikupljanje, obradu i prijenos informacija nužnih za poslovanje, planiranje i upravljanje poslovnom organizacijom.[3] Čine ga ljudi, komunikacijska oprema, cjelokupni softver i hardver, te informacije i procedure koje opisuju način upravljanja, odlučivanja i prijenosa informacija.

Projektiranje informacijskog sustava u pravilu je samo prva faza razvoja sustava. Tijekom praktične uporabe sustava neminovno dolazi do problema zbog opreme ili softvera, a troškovi održavanja i otklanjanja problema ponekad su veći od cijene samog sustava.

[1] Pavlić, Mile, Informacijski sustavi, Zagreb, Školska knjiga, 2011., str. 18.
[2] Ibid.
[3] Ibid., str. 14.

2.1. Elementi informacijskog sustava

Pred svaki informacijski sustav, neovisno o njegovoj veličini, postavljaju se najmanje dvije osnovne zadaće: prikupljanje i prijenos informacija nužnih za proces poslovanja i odlučivanja, te dokumentiranje poslovnog procesa. Prema složenosti može se podijeliti na jednostavne sustave koji su namijenjeni samo jednoj poslovnoj zadaći, najčešće uslužnoj (npr. knjigovodstveni servis), te na složene ili integralne sustave namijenjene za više korisničkih skupina i više raznovrsnih zadaća koje su međusobno povezane.

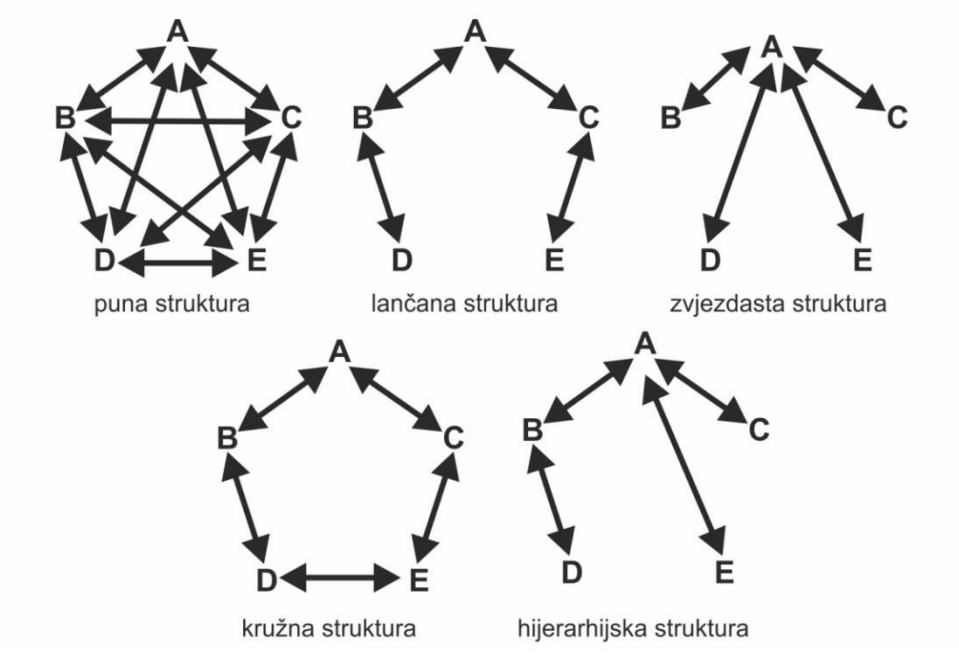
Bez obzira na složenost informacijskog sustava, on bi trebao sadržavati sljedeće cjeline:

- **hardware** čini sva informatička oprema poput računala i računalne periferije potrebne za unos i obradu podataka,
- **software** obuhvaća nematerijalnu komponentu sustava kao što su programi i metode za obradu i korištenje informacija i podataka,
- **netware** čini sva mrežna oprema nužna za komunikaciju s udaljenim računalima, a koja nije sastavni dio računala, poput mrežnih kablova, rutera, antena i druge mrežne opreme,
- **lifeware** čine zaposlenici čija je temeljna zadaća obrada i prijenos podataka, održavanje i unaprjeđenje sustava i
- **orgware** čine pravila i postupci koji sve elemente informacijskog sustava povezuju u jednu funkcionalnu cjelinu.[4]

Važan dio svakog informacijskog sustava je komunikacijska struktura. Ovisno o potrebama organizacije, ona se najčešće izvodi kao puna, zvjezdasta, lančana, hijerarhijska i kružna, a sheme povezivanja su prikazane na slici 1.

[4] Šimović, Vladimir, Uvod u informacijske sustave, Zagreb, Golden marketing – Školska knjiga, 2010., str. 16.-17.

Slika 1: Sheme komunikacijskih struktura



Izvor: Šimović, Vladimir, Uvod u informacijske sustave, Zagreb, Golden marketing – Školska knjiga, 2010., str. 18.

2.2. Podatci, informacije i znanje

Osnovni element svakog informacijskog sustava su podatci. Oni se često poistovjećuju s informacijama, premda često podatak i informacija nemaju isto značenje. U stvarnom svijetu često mnoštvo podataka tvore jednu informaciju. Tako su npr. veljača 2018., Gospić, Veleučilište „Nikola Tesla“ i Krešimir Matković podatci koji nemaju točno određeno značenja, dok spoznaja da student Krešimir Matković na Veleučilištu „Nikola Tesla“ u Gospiću tijekom veljače 2018. godine piše završni rad predstavlja jednu cjelovitu informaciju sačinjenu od navedenih podataka.

Podatak je vrijednost neke veličine koja se može sastojati od jednog ili više znakova, a koja je nositelj informacija. On je najčešće prikazan u sljedećim formama: alfanumerički (slova i brojevi), grafički (slika, crtež), zvukovni (zvuk, glas), filmski (kontinuiran slijed slika i zvukova).[5]

Za informacija se može reći da je ona protumačeni podatak ili skupina podataka koja korisniku pruža određenu spoznaju, ovisno o kontekstu i njegovim spoznajnim sposobnostima.[6] Ono što je za određenu osobu informacija, za drugu može biti samo

[5] Pavlić, Mile, op. cit., str. 22.
[6] Ibid.

podatak, što ovisi isključivo o njegovoj percepciji. Ako neka osoba pročita tekst na stranom jeziku i ne razumije njegovo značenje, tad se radi samo o podatcima. Isto tako, ako netko ne zna vrijednost ledišta i vrelišta Kelvinove temperaturne ljestvice, tad mu podatak da je danas temperatura 270 kelvina ne predstavlja informaciju jer ga neznanje sprječava u točnoj percepciji tog podatka i to za njega predstavlja samo podatak. Iz navedenog se može zaključiti da je vrijednost neke informacije ovisna o percepciji samog korisnika. Svaki šifrirani ili na bilo koji drugi način nerazuman podatak predstavlja samo podatak i ne može postati informacija sve do trenutka njegovog dešifriranja.

Svaka informacija ima određenu vrijednost, ovisno o njenim značajkama. Neke značajke informacija su: točnost, pouzdanost, pravodobnost, sigurnost, potpunost, jednostavnost, relevantnost, dostupnost i druge. Svaka od navedenih značajki utječe na vrijednost informacije. Nepouzdana i netočna informacija mogu korisniku nanijeti veću štetu nego korist, a nepravovremena informacija bez obzira na pouzdanost zna često biti beskorisna. Isto tako, ako je korisnik uz pouzdanu i točnu informaciju zasut mnoštvom nebitnih informacija, to može znatno otežati donošenje ispravne odluke, te željenu informaciju učiniti puno manje vrijednom.

Mnoštvo informacija koje su razumljive čovjeku i koje su korisne za svako ljudsko djelovanje čine znanje. Ono nastaje u ljudskom mozgu i pohranjeno je u neuralnoj mreži koju čine povezani neuroni.[7] Ljudska djelatnost čiji je glavni cilj stjecanje znanja naziva se znanost. Znanje se pohranjuje i na mnoge druge medije kao što su knjige, filmovi, softver, audio zapisi, razni analogni i digitalni zapisi itd. Ono se sastoji od činjenica, ideja, uvjerenja, spoznaja, iskustava, predviđanja, očekivanja i mnogih drugih elemenata ljudskog intelekta.

U ekonomskom smislu, ugradnjom znanja u proizvode ostvaruje se određena dodana vrijednost, čime se može znatno povećati vrijednost proizvoda. Znanje može znatno povećati funkcionalnost i mogućnosti bilo kojeg proizvoda, a utjecaj znanja na povećanje dodane vrijednosti možda je najlakše vidjeti na informacijsko-telekomunikacijskim uređajima poput mobilnih telefona ili računala.

[7] Pavlić, Mile, op. cit., str. 25.

2.3. Zadaće informacijskog sustava

Od svakog informacijskog sustava se očekuje ispunjenje temeljnih zadaća, a one su:

- prikupljanje i upisivanje podataka,
- obrada podataka,
- prijenos potrebnih informacija krajnjim korisnicima,
- pohrana i arhiviranje podataka.

Današnja tehnološka rješenja omogućuju postizanje visokog stupnja sigurnosti i zaštite podataka uporabom računala i mrežne infrastrukture. Pohrana podataka je puno jeftinija i brža, puno lakše je pronaći željene informacije iz arhiviranih podataka, a mnoge radnje je moguće u velikoj mjeri automatizirati i na taj način svesti troškove informacijskog sustava na najmanju moguću mjeru. Kod klasičnog arhiviranja uobičajeni troškovi su sljedeći:

- troškovi opreme čine 5% ukupnih troškova,
- troškovi za potrošni materijal su 5% ukupnih troškova,
- troškovi prostora iznose oko 20% ukupnih troškova,
- troškovi rada su oko 70% ukupnih troškova.[8]

Kako troškovi rada i prostora kod klasičnog arhiviranja iznose oko 90% ukupnih troškova, zadnjih desetljeća se podatci uglavnom arhiviraju u digitalnom obliku uporabom softverskih rješenja koja obuhvaćaju obradu, prijenos i arhiviranje podataka na diskove ili optičke medije. Ovakva rješenja se obično nazivaju *Document Management Imaging Processing* (DMIP) i u pravilu omogućuju visok stupanj automatizacije obrade i arhiviranja podataka. Time se troškovi arhiviranja višestruko smanjuju, omogućuje se znatno brži pristup željenim informacijama, a sigurnost podataka je znatno viša. Naime, puno je lakše fizički osigurati od neovlaštenog pristupa jedan ili nekoliko tvrdih diskova nego nekoliko polica registratora s tiskanim podatcima.

U informacijskom sustavu čovjek je često najslabija karika, bilo zbog svojih intelektualnih ograničenja, subjektivnog pristupa informacijama, utjecaja okoline ili bilo kojeg drugog čimbenika. Što viši stupanj automatizacije obično znači i viši stupanj sigurnosti i pouzdanosti, te smanjuje mogućnost pogreške koju čovjek može učiniti zbog umora, nemara i slično.

[8] Šimović, Vladimir, op. cit., str. 25

2.4. Oslonjivost informacijskog sustava

Iz godine u godinu sve je viši stupanj ovisnosti korisnika o informacijskim sustavima. Često sami korisnici nisu ni svjesni koliko su ovisni o tim sustavima, a njihov značaj se osjeti tek kad dođe do kvara ili bilo kakvog drugog zatajenja. To se osobito odnosi na veće ustanove, premda i svaki pojedinac osjeti ovisnost o tehnologiji u slučaju gubitka mobilnog telefona, kvara računala ili bilo kojeg oblika gubitka podataka pohranjenih na elektroničkom uređaju.

Oslonjivost informacijskog sustava sastoji se od sljedećih obilježja:

- **dostupnost** (*engl. availability*) je raspoloživost informacijskog sustava za korištenje u bilo kojem trenutku,
- **pouzdanost** (*engl. reliability*) podrazumijeva kontinuiranu dostupnost usluge informacijskog sustava bilo kada,
- **sigurnost** (*engl. safety*) - predstavlja izostanak bilo kakvih poteškoća ili zatajenja informacijskog sustava,
- **povjerljivost** (*engl. confidentiality*) - podrazumijeva izostanak neautoriziranogpristupa podatcima u informacijskom sustavu,
- **cjelovitost** (*engl. integrity*) - podrazumijeva izostanakneispravnih podataka koji narušavaju integritet informacijskog sustava,
- **lakoća održavanja** (*engl. maintainability*) - podrazumijeva jednostavnost održavanjai ispravki pogrešaka informacijskog sustava.[9]

Najčešći uzrok zatajenja informacijskog sustava je kvar, pa metode smanjenja mogućnosti pojave kvara predstavljaju i podizanje razine oslonjivosti sustava. Metode smanjenja mogućnosti pojave kvara: prevencija kvara, smanjena osjetljivost na kvar, predviđanje nastanka kvara i mogućnost uklanjanje kvara.[10]

Prevencija pojave kvara postiže se izborom više kvalitete softvera i hardvera. Redovito ažuriranje, modularnost i druge mjere mogu znatno smanjiti mogućnost nastanka kvara, dok hardverska prevencija podrazumijeva odabir kvalitetnog hardvera, rukovanje sukladno uputama, redovito održavanje hardvera i slične preventivne mjere. Maliciozni kvarovi preveniraju se vatrozidom, kvalitetnom antivirusnom zaštitom i sličnim mjerama.

[9] Jakupović, Alen, Utjecaj oslonjivosti informacijskog sustava na poslovne organizacije, Zbornik Veleučilišta u Rijeci, 1(1), 165-178. 2013., Dostupno na https://hrcak.srce.hr/103341 (14.1.2018.), str. 167.

[10] Ibid, str. 169.

2.5. Poslovne funkcije i funkcije informacijskih sustava

Svaka ustanova, organizacija ili poduzeće imaju svoje poslovne funkcije koje objedinjene čine cjelokupnu djelatnost te ustanove. Najjednostavnije ih je objasniti na primjeru bilo koje poslovne organizacije čija je osnovna djelatnost proizvodnja određenih proizvoda. Kako je u središtu svake poslovne djelatnosti kupac, sam proizvodni proces čini tek jednu od poslovnih funkcija. Proizvodnja sama po sebi i nema smisla ukoliko taj proizvod ne može naći put do kupca ili ako ne postoji potražnja za njim.

Osnovne funkcije poslovne organizacije su sljedeće:

- planiranje,
- proizvodnja,
- kontrola proizvodnje,
- marketing,
- komercijala,
- financije,
- računovodstvo,
- upravljanje (engl. management),
- personalni poslovi i drugo.[11]

Iz navedenog se može zaključiti da je svaka poslovna djelatnost kompleksan skup međusobno ovisnih poslovnih funkcija čija je zadaća proizvodnja određenih proizvoda ili usluga, njihova prodaja i u konačnici ostvarivanje određene zarade. Problemi u bilo kojoj poslovnoj funkciji odražava se na ostvarivanje ukupnog proizvodnog procesa. Ukoliko u proizvodnom procesu nedostaje sirovina, zaposlenika ili financija, teško da će proizvodni proces biti uspješan. Isto tako, nedostatak planiranja ili marketinga teško mogu bilo kakvu poslovnu djelatnost održati uspješnom na duže staze. Moderno društvo zahtijeva interakciju poslovnih sustava s tržištem, osluškivanje potreba tržišta i prilagodbu proizvodnog procesa potrebama i zahtjevima krajnjih korisnika – kupaca.

Kao što svaki poslovni proces ima svoje funkcije, tako i svaki informacijski sustav ima svoje specifične funkcije koje omogućuju uspješno funkcioniranje sustava. One su nužne za funkcioniranje svakog sustava, bez obzira na njegovu veličinu i kompleksnost.

[11] Pavlić, Mile, op. cit., str. 25., str. 31.

Glavne funkcije informacijskog sustava su:

- **prikupljanje i unos podataka u bazu**, što se može provoditi ručno (ručnim upisivanjem, skeniranje i slično), pomoću softvera (pretraživanje interneta, automatsko snimanje i slično) ili na druge načine;
- **obrada podataka**, može se provoditi ručno ili automatski, pomoću softvera, što obuhvata pristup podatcima u bazi podataka, računanje, sortiranje, analiziranje i sve druge operacije koje mogu kao rezultat dati nove podatke koji su korisni za planiranje i upravljanje;
- **prikaz i distribucija podataka** podrazumijeva prezentiranje podataka dobivenih obradom, te njihova distribucija krajnjim korisnicima;
- **arhiviranje i čuvanje podataka** podrazumijeva njihovo spremanje s ciljem da im se po potrebi može naknadno bilo kada pristupiti.

U novije vrijeme se funkcije informacijskih sustava u pravilu izvode u digitalnom obliku, premda se sve funkcije mogu izvoditi i u tiskanoj formi. Digitalna forma omogućava jeftiniju i bržu obradu i arhiviranje podataka, te puno brži i jednostavniji naknadni pristup arhiviranim podatcima.

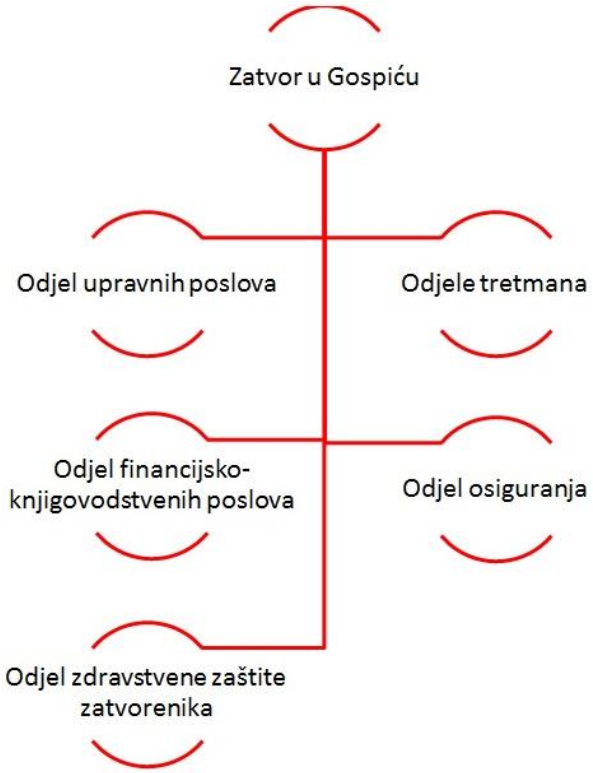
3. INFORMACIJSKI SUSTAV U ZATVORU

Zatvor u Gospiću je specifična ustanova koja je znatno zatvorenija za javnost od mnogih drugih ustanova, a koja zbog mnogih potreba mora komunicirati s drugim sličnim ustanovama, Ministarstvom pravosuđa, te lokalnim poduzećima. Prema ograničenju slobode kretanja osoba lišenih slobode ovaj zatvor je zatvorenog tipa, ali u svom sastavu uz zatvoreni ima i poluotvoreni i otvoreni odjel. Zatvor svoju djelatnost obavlja na tri lokacije:

- Ulici Senjskih žrtava 15,
- Nikole Šubića Zrinskog bb i
- Ljubovo bb

Voditelj Zatvora u Gospiću je upravitelj, a ustroj je prikazan na sljedećoj slici.

Slika 2: Ustroj Zatvora u Gospiću



Izvor: https://pravosudje.gov.hr/zatvorski-sustav/tijela-zatvorskog-sustava/zatvori/zatvor-u-gospicu/o-zatvoru-7529/7529 (21.2.2018.)

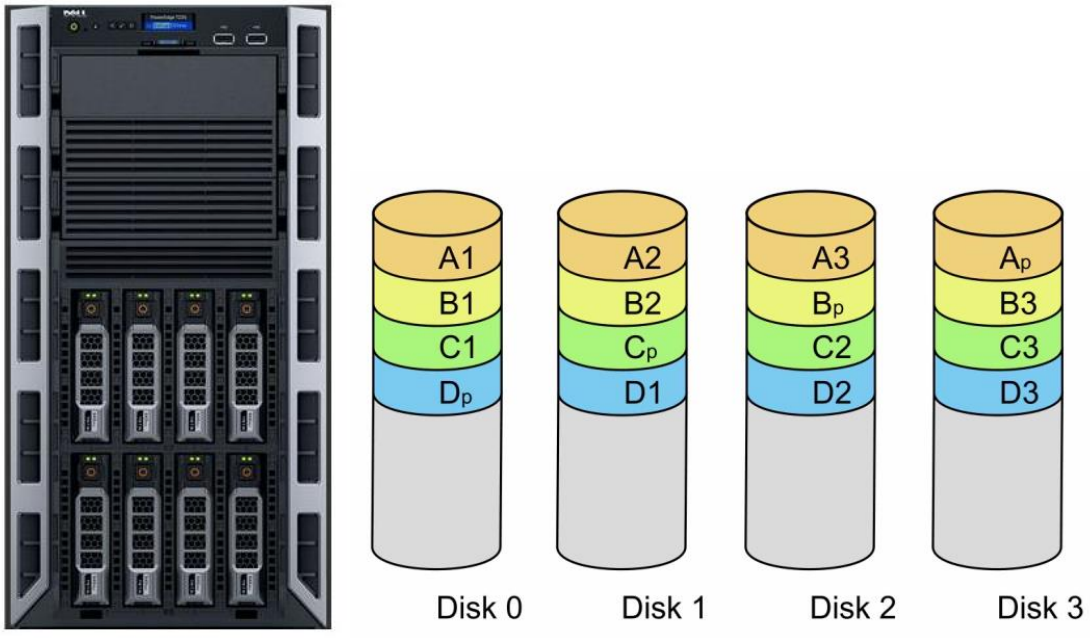
3.1. Lokalna računalna mreža u Zatvoru u Gospiću

Sva računala u Zatvoru su međusobno umrežena u lokalnu mrežu, te pomoću mrežnog preklopnika (*engl. switch*) spojena na poslužitelj DELL T330. Operacijski sustav na poslužitelju je Windows Server 2012 R2 Standard. Na poslužitelju su kreirani korisnički računi, te je svakom korisniku dodijeljena zasebna mapa za pohranu podataka. Veza između računala i prespojnika je žičana (UTP kabel) a bežično povezivanje je onemogućeno, kako bi se smanjila mogućnost neovlaštenog pristupa mreži. Mreža je opremljena i vatrozidom koji sprječava neovlašteni pristup podacima korisnicima izvan Zatvora.

Specifikacije poslužitelja su sljedeće:

- procesor je Intel Xeon E3-1220v6 – 4jezgre, 3 GHz s 8 MB L3 Cache memorije
- matična ploča je Intelova, Chipset Intel C236 s 8GB RAM-a DDR4 radnog takta 2400 MHz, proširivo do 64 GB
- za pohranu podataka namijenjena su 4 SATA diska, svaki po 1TB i 7200 o/min, spojeni u polje RAID 5, 6Gb/s 3.5in Hot-plug
- računalo posjeduje optički pogon DVD±RW, te 2 mrežne kartice 10/100/1000 MB/s

Slika 3: Poslužitelj i diskovi u polju RAID 5



Izvor: https://dellservervr.dell.com/poweredge-t330/

Na lokalnoj mreži (*engl. Local Area Network - LAN*) Zatvora u Gospiću je velika pozornost posvećena sigurnosti pohranjenih podataka. Svi korisnici moraju svoje dokumente pohranjivati na diskovima na poslužitelju. Za pohranu je poslužitelj opremljen s 4 SATA diska veličine 3,5 inča i kapaciteta po 1 TB svaki disk, a spojeni su u RAID 5 polje. Diskovi podržavaju tzv. *Hot-plug* izmjenu, tj. zamjenu diska bez isključivanja računala. Poslužitelj se nikad ne gasi, a opremljen je i uređajem za neprekidno napajanje (UPS) koji se aktivira kao izvor energije u slučaju nestanka električne energije. U takvim slučajevima Zatvor koristi dizelski agregat kao pomoćni izvor, a do uključivanja agregata poslužitelj radi na bateriju iz UPS-a.

RAID 5 polje diskova osigurava integritet podataka i u slučaju kvara nekog od diskova. Na tri diska se zapisuju podatci, dok se na četvrtom uvijek nalazi kopija podataka koji su zapisani na preostala 3 diska. Pri tome se teži da zauzeće svakog diska bude ujednačeno, kao što je prikazano na slici 3. U slučaju kvara na bilo kojem disku, nakon njegove zamjene rekonstruiraju se podatci na pokvarenom disku na temelju zapisa na tri preostala ispravna diska. Ovakav način zapisivanja umanjuje performanse kod zapisivanja, ali zato znatno povećava sigurnost spremljenih podataka.

Dodatno osiguranje integriteta podataka postiže se redovitim arhiviranje koje svakog petka od 13 sati provodi mrežni administrator. Podatci se spremaju na vanjski disk koji se nakon završetka tjednog arhiviranja posprema u kasu u uredu upravitelja Zatvora u Gospiću. Kasa je uvijek zaključana i onemogućen je bilo kakav neovlašten pristup tim podatcima.

3.2. Vatrozid

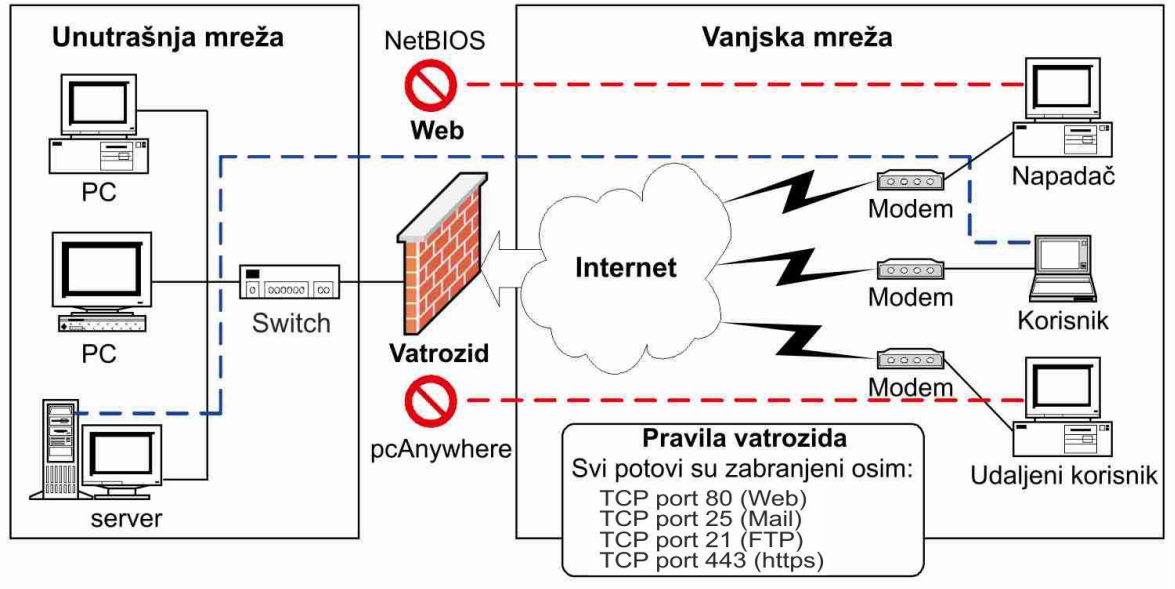
Za svakodnevno poslovanje Zatvora u Gospiću nužna je komunikacija sa preostala dva odjela, kao i sa Ministarstvom pravosuđa. Za tu komunikaciju nužna je uporaba javne mreže (interneta), što predstavlja određeni sigurnosni izazov. Sigurnost prometa podataka izvan ustanove ostvaruje se uporabom virtualne privatne mreže, uz pomoć vatrozida. Vatrozid je uređaj pomoću kojeg se štiti privatna mreža od korisnika na javnoj mreži. Glavna mu je zadaća omogućivanje sigurnog pristupa iz privatne na javnu mrežu. Vatrozid koji se koristi u Zatvoru Gospić je proizvod tvrtke Sonic Wall, model TZ 600. U njemu je integrirano više razina zaštite od neovlaštenog pristupa (zatvaranje portova, skrivanje IP adresa klijenata u LAN-u), što će biti objašnjeno u nastavku.

Slika 4: Vatrozid LAN-a Zatvora u Gospiću

Izvor: https://www.sonicwall.com/en-us/products/firewalls

Kod uobičajenog pristupa računala javnoj mreži na računalu je omogućeno mnoštvo ulazno-izlaznih priključaka (*engl. portova*) koji nisu nužni za normalan rad na računalu. Uporabom vatrozida, kao što je prikazano na slici 4, blokiraju se svi portovi koji nisu nužni za obavljanje poslovnih aktivnosti, čime se znatno smanjuje mogućnost neovlaštenog upada u lokalno računalo. Ostaju otvoreni samo oni portovi nužni za komunikaciju, kao što su port 80 za pristup webu, port 25 za slanje i primanje e-maila, port 443 preko kojeg se odvija https promet, te port 21 za razmjenu datoteka (*engl. File Transfer Protocol – FTP*).

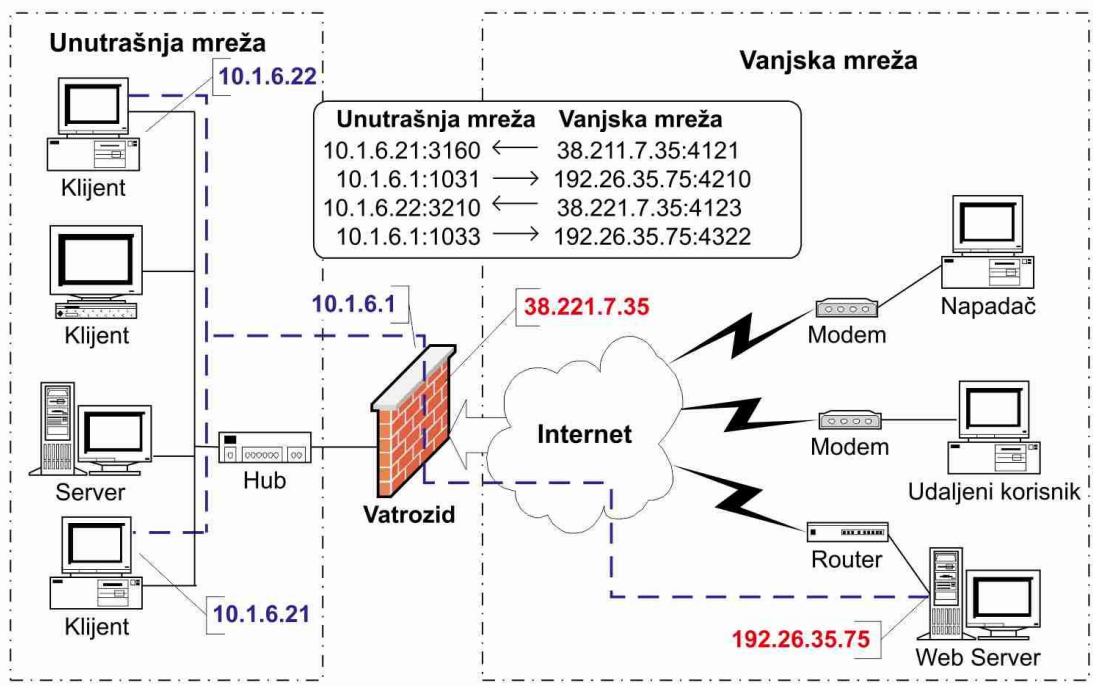
Slika 5: Shema lokalne mreže i popis otvorenih portova



Izvor: 8. Sviličić, Boris, Kraš, Antun, Zaštita privatnosti računalnog sustava, Pomorstvo, 19(1), 275-284. 2005., dostupno na https://hrcak.srce.hr/3962 (10.2.2018.), str. 277.

Osim zatvaranja nepotrebnih portova, vatrozid skriva IP adrese lokalnih računala, čime onemogućava neovlašteni pristup tim računalima. Potencijalnim napadačima se prikazuje neispravna IP adresa, te se njihovi napadi usmjeravaju na nepostojeće adrese, kao što je prikazano na slici 6.

Slika 6: Uporaba vatrozida za skrivanje IP adresa

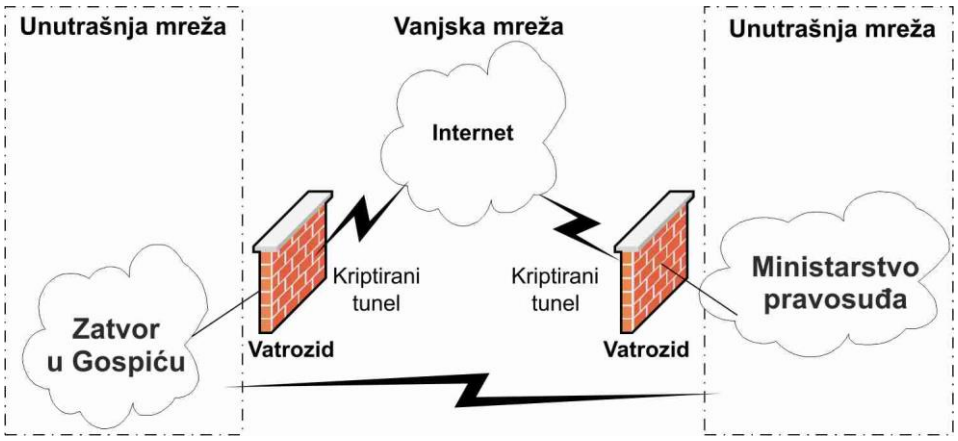


Izvor: 8. Sviličić, Boris, Kraš, Antun, Zaštita privatnosti računalnog sustava, Pomorstvo, 19(1), 275-284. 2005., dostupno na https://hrcak.srce.hr/3962 (10.2.2018.) str. 279.

Za povezivanje lokalnih mreža na velikim udaljenostima koristi se virtualna privatna mreža, koja koristi javnu infrastrukturu ali je po prirodi privatna. Ovakve mreže zovu se virtualne privatne mreže (VPN).

Kod virtualnih privatnih mreža svaka ima svoj vatrozid koji onemogućava pristup korisnicima izvan te lokalne mreže, te je „kriptiranim tunelom“ povezan s drugom lokalnom mrežom, kao što je prikazano na slici 7.

Slika 7: Uporaba vatrozida za kreiranje VPN



Izvor: Sviličić, B., Kraš, A. (2005). *Zaštita privatnosti računalnog sustava,* str. 282.

Iz navedenog mogu se identificirati osnovne funkcije koje vatrozid ispunjava. Glavne funkcije vatrozida sadržane su u četiri osnovne metode djelovanja:

- paketno filtriranje, kojim se odbacuju neželjeni mrežni paketi na temelju izvorišne
- adrese računala, odredišne adrese primatelja ili na temelju vrste podataka koji putuju mrežom,
- prikrivanje mrežnih adresa s ciljem zaštite tajnosti mrežne konfiguracije,
- posredovanje pri ostvarivanju veze između klijenata i poslužitelja s ciljem skrivanja identiteta korisnika privatne mreže,
- stvaranje virtualne privatne mreže implementacijom kriptografske zaštite podataka radi sigurnog korištenja javne mreže.[12] (Sviličić, Kraš, 2005: 276)

3.3. Prijenos podataka putem računalne mreže

Za prijenos podataka putem računalne mreže nužna je određena mrežna infrastruktura, te korištenje određenih protokola, tj. pravila koja osiguravaju da određeni podatci stignu na željeno odredište bez ugroze. Za prijenos unutar lokalne mreže koristi se tzv. OSI referentni model, a za prijenos na Internetu TCP/IP model.

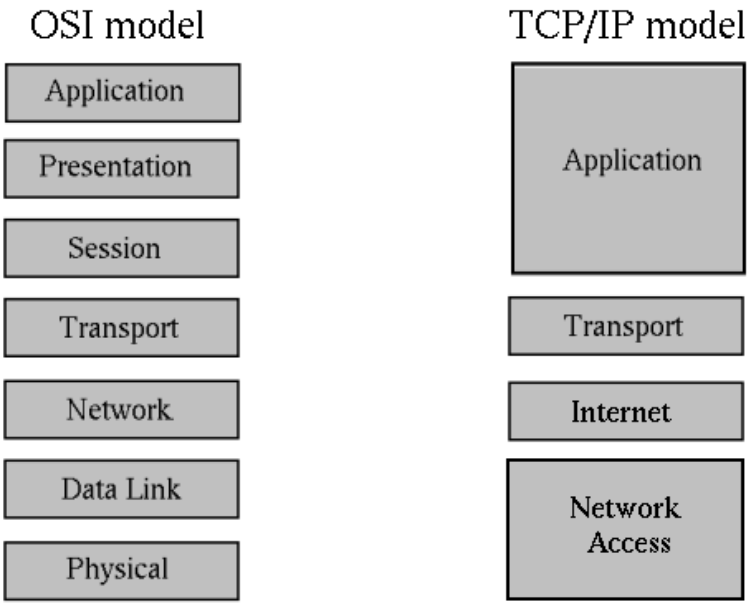
[12] Sviličić, Boris, Kraš, Antun, Zaštita privatnosti računalnog sustava, Pomorstvo, 19(1), 275-284. 2005., Dostupno na https://hrcak.srce.hr/3962 (10.2.2018.), str. 276.

OSI referentni model (*engl. Open Systems Interconnection Basic Reference Model*) zasnovan je na slojevima od kojih svaki sloj ima točno određenu funkciju. Slojevi ovog modela su:[13]

- Application (aplikacijski sloj),
- Presentation (prezentacijski sloj),
- Session (sloj sesija),
- Transport (transportni sloj),
- Network (mrežni sloj),
- Data Link
- Physical layer (fizički sloj).

TCP/IP je sličan OSI modelu, ali ima samo 4 sloja: Application, Transport, Internet i Network Access. Na sljedećoj slici je prikazana usporedba OSI i TCP/IP modela.

Slika 8: OSI i TCP/IP model prijenosa podataka



Izvor: CARNet, Računalne mreže – OSI referentni model, dostupno na https://sysportal.carnet.hr/node/352, (12.3.2018.)

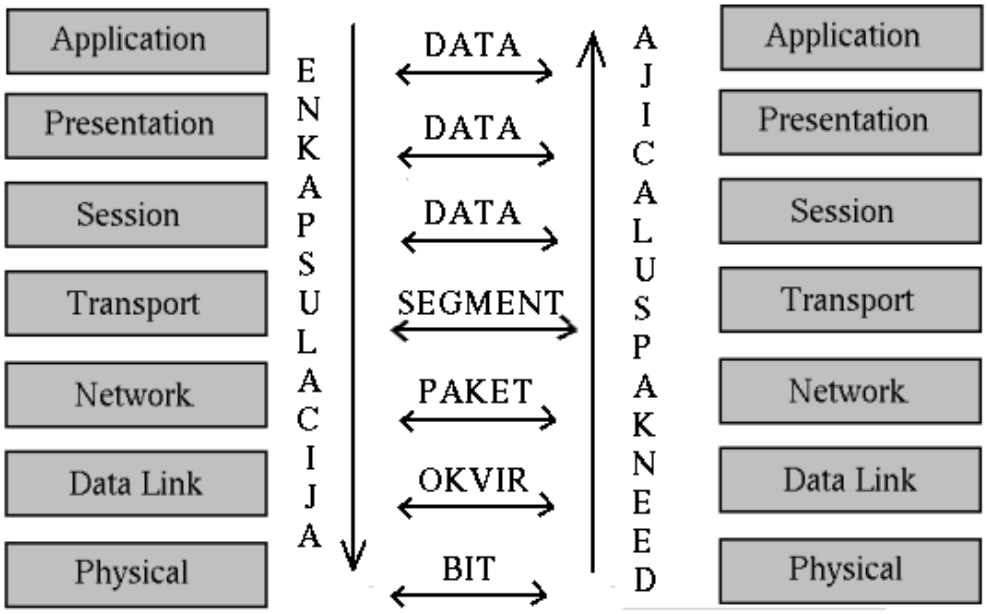
Prijenos podataka se odvija razbijanjem datoteka na pakete kojima se dodaje zaglavlje s adresama pošiljatelja i primatelja, te se kodirani šalju s polazišta na odredište. Cijeli postupak se zove enkapsulacija.

[13] Pralas, Toni, Računalne mreže – OSI referentni model, dostupno na https://sysportal.carnet.hr/node/352, (12.3.2018.)

Zadaće pojedinih slove u OSI modelu su:[14]

- Aplikacijski sloj je zadužen za pružanje mrežne usluge programima, te upućuje zahtjev prezentacijskom sloju.
- Prezentacijski sloj osigurava da su podaci čitljivi na odredištu, brine se o formatu i strukturi podataka.
- Sesijski sloj je zadužen za uspostavljanje, upravljanje i prekid veze između aplikacija.
- Transportni sloj osigurava pouzdan prijenos podataka između uređaja, te otkriva i ispravlja greške u prijenosu (traži ponovno slanje u slučaju pogrešaka).
- Mrežni sloj osigurava povezanost i bira najbolje putanje za paket podataka. Podaci do odredišta mogu putovati različitim putanjama.
- Data Link sloj omogućuje pouzdan prijenos podataka preko medija, brine se o pristupu mediju i bira putanje između uređaja.
- Fizički sloj vodi računa o fizičkim komponentama mreže: medijima za prijenos, konektorima, razinama napona i signala, brzinama prijenosa podataka, itd.

Slika 9: Enkapsulacija u OSI referentnom modelu prijenosa podataka



Izvor: Pralas, Toni, Računalne mreže – OSI referentni model, dostupno na https://sysportal.carnet.hr/node/352, (12.3.2018.)

[14] Pralas, Toni, op. cit.

3.4. Adresiranje u računalnoj mreži

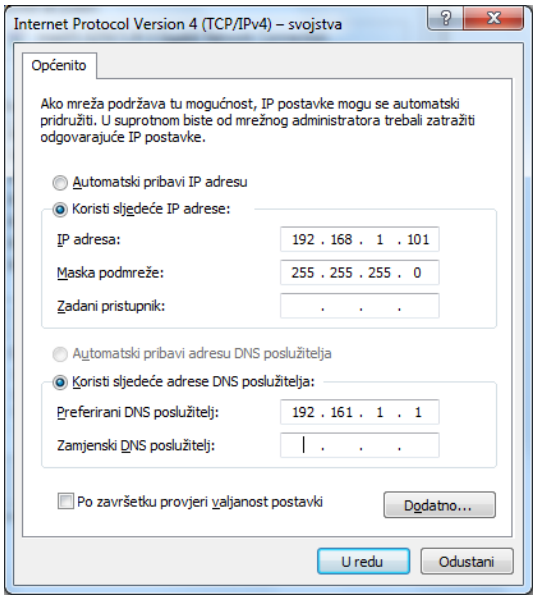
Kako bi se osigurala sigurna komunikacija računala s drugim računalima na Internetu, koriste se tehnologije mrežnog prevođenja adresa (*NAT – Network Address Translation*). Vatrozid ili preklopnik na kojemu je podešen NAT mijenja privatnu adresu sa svojom javnom koja se usmjerava Internetom. Po dobivanju odgovora od udaljenog računala ponavlja postupak, ovaj put mijenjajući javnu adresu sa odgovarajućom privatnom adresom računala koje je uputilo zahtjev.

Za fizičko adresiranje zadužen je drugi sloj OSI referentnog modela (Data Link) u kojem se poruci dodaje MAC adresa (*engl. Media Acess Control*) Svaki mrežni uređaj u sebi sadrži jedinstvenu MAC adresu koja je zapisana unutar hardware-a mrežnih kartica. Sastoji se od 48 bitova koji su u ROM-u (*engl. Read Only Memory*) u obliku 12 heksadecimalnih znamenki na sljedeći način:

- 6 parova znamenki odvojenih crticom (01-23-45-67-89-ab)
- 6 parova znamenki odvojenih dvotočkom (01:23:45:67:89:ab)
- 3 skupine po 4 znamenke odvojene sa točkom (0123.4567.89ab)

Svako računalo na mreži mora imati adresu, kako bi moglo komunicirati s drugim računalima, a ta adresa se zove IP adresa. Ona može biti ručno postavljena ili automatski dodijeljena. Na slici je prikazan način postavljanja IPv4 adrese.

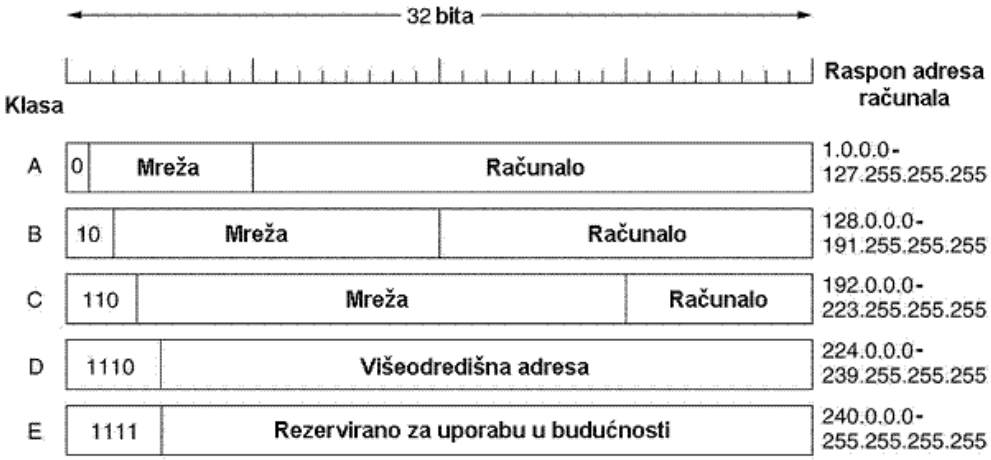
Slika 10: Postavljanje fiksne IP adrese



Izvor: Autor rada

Godinama se koristi protokol za adresiranje IPv4, a zadnjih godina je zbog nedostatka adresa sve češće u uporabi IPv6. IPv4 adresa je logički podijeljena u dva dijela: dio koji je namijenjen adresiranju mreže u kojoj se uređaj nalazi i dio koji označava sam uređaj. Adrese su podijeljene po klasama, a najčešće se koriste sljedeće klase adresa: A, B i C, a puno rjeđe D i E. Klasi A IPv4 adresa pripadaju sve adrese kojima prvi oktet počinje sa brojem između 1 i 126 (npr., 15.8.3.240, 111.16.12.9, itd).

Slika 11: Klase IPv4 adresa



Izvor: IP adresa, dostupno na http://mreze.layer-x.com/s030101-0.html, (20.3.2018.)

Većina adresa raspoloživa je za adresiranje računala na Internetu, a samo dio adresno prostora je rezerviran za lokalne mreže, i to:[15]

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Kako IPv4 pruža ograničen broj adresa koji više ne zadovoljava potrebe modernog društva, uveden je novi standard IPv6 koji pruža skoro neograničen broj adresa. Ovaj standard omogućuje zapisivanje adrese u heksadecimalnom formatu, te time znatno više adresnog prostora. Primjer IPv6 adrese: 3ffe:0501:0008:0000:0260:97ff:fe40:efab.

Kako IPv6 adrese imaju 16 byteova, korištenjem IPv6 adresiranja omogućuje korištenje 2^{128} adresa ili približno $3x10^{38}$ adresa.[16] Nasuprot njemu, IPv4 protokol je duljine 32 bita i osigurava maksimalni broj od 2^{32} različitih adresa što je oko 4,3 milijardi adresa.

[15] IP adresa, dostupno na http://mreze.layer-x.com/s030101-0.html, (20.3.2018.)
[16] Ibid.

3.5. Sustav video nadzora

Važna komponenta informacijskog sustava Zatvora u Gospiću je i sustav video nadzora koji nadzire i snima sva događanja u pojedinim dijelovima zgrade i okoline. Video zapisi se pohranjuju na tvrdi disk računala u kontrolnoj sobi, te se čuvaju minimalno trideset dana od dana snimanja.

Važnost sustava video nadzora osobito dolazi do izražaja u slučaju konflikta između zatvorenika i osoblja zatvora. Pregled pohranjenog materijala mogu vršiti voditelj smjene i načelnik Odjela osiguranja.

Uz ključne prostorije i okoliš zatvora, sustavom video nadzora je pokriveno i dvorište za šetnju zatvorenika. Iako u Zatvoru u Gospiću još nije zabilježen takav slučaj, iskustva drugih ustanova pokazuju snalažljivost kriminalaca koji sve češće koriste dronove za unošenje nedozvoljenih sredstava poput mobitela, droge i slično u krug zatvora.

3.6. Korisnici informacijskog sustava

Posebna pozornost posvećena je zaštiti od neovlaštenog iznošenja podataka iz kruga zatvora. Svi korisnici osim mrežnog administratora imaju status „običnog korisnika“ (*engl. user*), te im je u sigurnosnim postavkama onemogućena pohrana podataka na optičke medije, podatkovne kartice ili bilo koji uređaj koji se priključuje na USB ili eSATA priključak. Također je onemogućena instalacija bilo kakvog softvera ili uređaja, a ispis svih potrebnih dokumenata se izvodi na mrežnom pisaču čija je uporaba dozvoljena svim korisnicima.

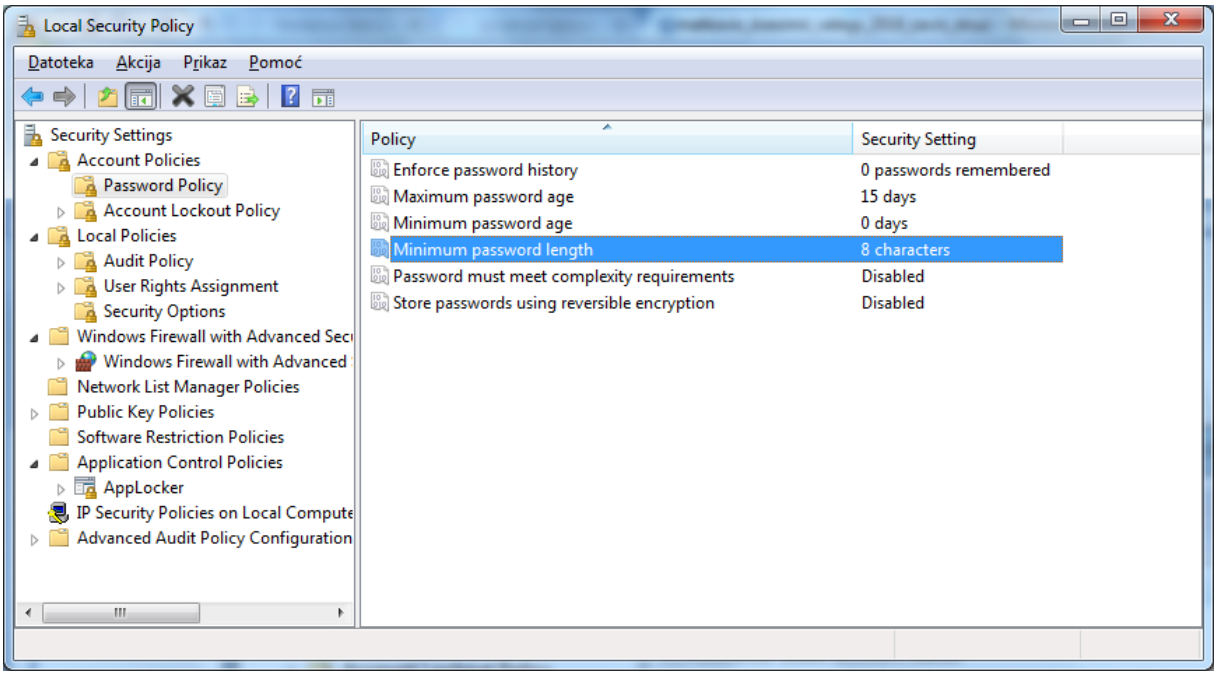
Iako svi korisnici informacijskog sustava imaju mogućnost korištenja interneta, postoje brojna ograničenja čija je zadaća svesti mogućnost ugroze sustava na najmanju moguću mjeru. Moguć je pristup samo nekolicini internetskih stranica (dnevne tiskovine, HAK, Hidrometeorološki zavod Hrvatske i slično). Onemogućeno je i slanje elektroničke pošte na privatne adrese, pa je moguća interna razmjena pošte.

Najčešće ugroze informacijskih sustava dolaze zbog neznanja ili nemara samih korisnika sustava. Kako bi se negativan utjecaj korisnika sveo na najmanju moguću mjeru, svakom korisniku su dodijeljene samo one ovlasti i prava koji su nužni za obavljanje svakodnevnih zadaća. Za sigurnost cjelokupnog informacijskog sustava najveću odgovornost ima mrežni administrator koji je u zatvoru zadužen za održavanje sustava,

arhiviranje podataka, instaliranje i ažuriranje novog softvera, te sve druge radnje koju zahtijevaju administratorske ovlasti. On može određenom korisniku dati i nešto više ovlasti, ali je odgovoran za sve eventualne štete koje mogu proizaći iz takvog postupka.

Osim korisničkih profila ugrađenih u operacijski sustav, administrator sustava može modificirati bilo koji profil s ciljem smanjenja ili povećanja ovlasti korisnika. Najpreciznije se mogu definirati obveze i prava korisnika pomoću administrativnih alata u applet-u[17] *Local Security Policy* integriranomu sam operacijski sustav, što je prikazano na slikama 12. i 13.

Slika 12: Definiranje snage zaporke za korisnike informacijskog sustava



Izvor: autor rada

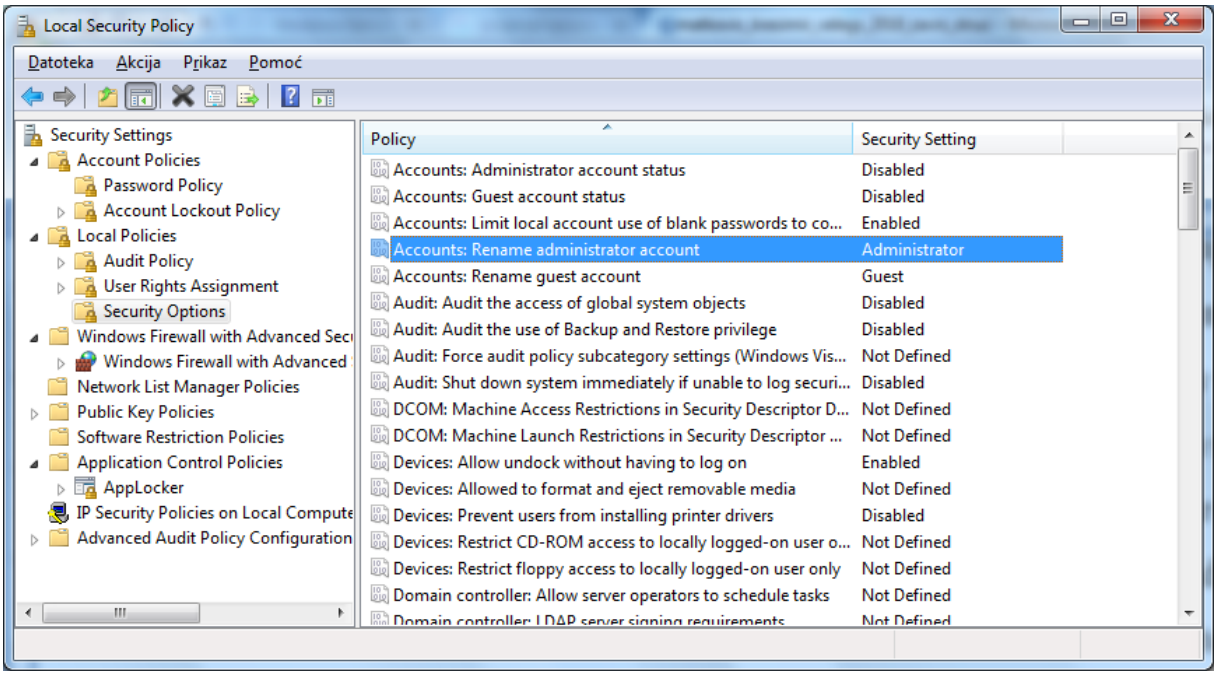
Obveza svakog korisnika je čuvanje zaporke i ostalih podataka vezanih za autorizaciju u sustavu. Kako bi osigurali što višu razinu sigurnosti, administratori često određuju najmanju dozvoljenu dužinu zaporke, te period nakon kojeg svaki korisnik mora promijeniti zaporku. Ukoliko to ne učini na vrijeme i na propisan način, korisniku biva onemogućen pristup informacijskom sustavu sve do intervencije administratora sustava.

[17] Applet je manja aplikacija (program) koji izvršava određeni dio programskog koda. U operacijskom sustavu pomoću applet-a se podešavaju mnoge postavke rada sustava (sigurnost, postavke mape, postavke štednje energije, personalizacija sustava i slično). Svaka ikona u kontrolnoj ploči (*Control Panel*) je kratica do nekog appleta.

Na slici 12. su unesene postavke da korisnik mora mijenjati zaporku svakih petnaest dana, te da zaporka mora imati najmanje osam znakova.

Osim ovih temeljnih postavki, moguće je definirati mnoštvo sigurnosnih postavki u odjeljku Security Options, kao što se mogućnost korištenja određenih aplikacija, dozvola pristupa pojedinim računalnim resursima poput optičkog pogona ili diska, mogućnost korištenja priključaka za vanjske uređaje (USB, SATA i slično), te mnoge druge sigurnosne postavke. Neke inicijalne sigurnosne postavke ovog odjeljka u Windowsima 7 prikazane su na slici 9.

Slika 13: Inicijalne postavke apleta Local Security Policy, odjeljak Security Options



Izvor: autor rada

Stalna edukacija korisnika informacijskog sustava je jedan od najvažnijih oblika prevencije, kad je sigurnost sustava u pitanju. Korisnicima je važno staviti do znanja važnost pridržavanja mjera zaštite sustava, kao i njihove odgovornosti za njegov rad.

4. OBLICI UGROZE INFORMACIJSKOG SUSTAVA

Sigurnost informacijskih sustava iz godine u godinu sve više dobiva na važnosti, a informacije postaju sve skuplja i traženija roba. U takvom okruženju nužno je veliku pozornost posvetiti zaštiti informacijskih sustava, te implementirati visoke standarde koji će omogućiti sigurno pohranjivanje i zaštitu podataka. Danas informacijska sigurnost podrazumijeva zaštita informacija od mnoštva realnih prijetnji s ciljem osiguranja neprekidnosti poslovanja, povećanja prihoda i smanjenja poslovnog rizika.

Svaka organizacija, pa tako i Zatvor u Gospiću, posjeduje određene resurse koji mogu biti primamljivi potencijalnom napadaču, pa ih je nužno čuvati i brinuti za njihovu sigurnost. Detekcija sigurnosnih prijetnji omogućava poduzimanje primjerenih mjera kako bi se smanjila ili u potpunosti otklonila mogućnost ugroze sustava. Svaki sustav je u određenoj mjeri ranjiv, bilo zbog nesavršenosti hardvera, softvera ili zbog slabosti, nemara i neznanja samih korisnika. Uvidjevši važnost prijetnji u računalstvu, i Microsoft je modeliranje prijetnji integrirao u sustav *Security Development Lifecycle* (SDL).[18]

Svi oblici ugroze računalne sigurnosti mogu se svesti na četiri osnovne kategorije:[19]

- malware (zlonamjerni softver),
- zlonamjerni udaljeni napadač,
- pogreške u programskom kodu,
- pogreške u konfiguraciji računala.

Najčešći motiv koji potiče napadača na ugrozu nekog informacijskog sustava je pribavljanje vrijednih informacija. Napad može biti izveden od strane neke osobe, a može biti i rezultat djelovanja specijaliziranog zlonamjernog softvera. Zlonamjerni softver (*engl. malicious software*) je zloćudni softver namijenjen instalaciji na računalo bez znanja njegovog korisnika. U zlonamjerni softver spadaju:[20]

- virusi,
- crvi,
- trojanski konji,

[18] Centar informacijske sigurnosti, Modeliranje sigurnosnih prijetnji, dostupno na https://www.cis.hr/files/dokumenti/CIS-DOC-2012-05-049.pdf (16.1.2018.), str. 4

[19] Radić, Branimir, Sigurnosne računalne prijetnje, 2012., dostupno na http://www.srce.unizg.hr/arhiva_weba/sistemac2015/fileadmin/user_root/seminari/Srce-Sys-Seminari-Sigurnosne_racunalne_prijetnje.pdf (5.2.2018.), str. 10.

[20] CERT, Zlonamjerni softver, dostupno na http://www.cert.hr/19795-2/malver/, (25.3.2018.)

- spyware,
- zlonamjerni adware,
- crimeware,
- scareware,
- keyloggeri,
- rootkitovi.

Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala tako da se bez znanja korisnika kopira u datotečni sustav ili memoriju računala. Virusi se brzo šire s jednog računala na drugo putem interneta, privitaka u e-mail porukama ili prijenosnih medija poput prijenosnog diska, CD, DVD ili USB diska.

Osnovne vrste virusa su:

- boot sektor virusi su oni virusi koji kopiraju svoj kod u MBR (engl. Master boot sektor) i tako se pokreću pri svakom startu računala,
- programski virusi koji se pokreću pri izvršenju zaražene datoteke,
- makro virusi su napisani programskim makro jezikom, te mogu mijenjati dokumente.

Crvi su maliciozni programi koji sami sebe umnožavaju i šire se putem mreže. Kod njih nije nužno postojanje domaćinske datoteke za svoj rad. Crvi su samostalni programi i šire se bez interakcije korisnika. Koriste računalnu mrežu kako bi se širili s jednog računala na drugo.

Trojanski konji su oblik zlonamjernog softvera koji se lažno predstavlja kao koristan kako bi ga korisnik izvršio. Može izmijeniti pojedine dijelove operacijskog sustava kako bi on prikazivao oglase s ciljem ostvarivanja novčane koristi. Ponekad trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom, pa tada može raditi sljedeće radnje:[21]

- koristiti zaraženo računalo kao dio „botnet“ mreže,
- ukrasti vrijedne informacije,
- instalirati drugi zlonamjerni softver,
- slati, primati i mijenjati datoteke,
- bilježiti pritisak na tipke (kao keylogger),
- špijunirati aktivnosti korisnika zaraženog računala,

[21] CERT, O virusima, dostupno na http://www.cert.hr/virusi/, (23.3.2018.)

- koristiti resurse zaraženog računala,
- rušiti zaraženo računalo itd.

Spyware je namijenjen prikupljanju informacija i preuzimanje kontrole nad računalom korisnika bez njegova znanja. Ova vrsta zlonamjernog softvera se obično ne replicira. Iskorištava zaražena računala za komercijalnu dobit, poput prikazivanja pop-up reklama, krađu podataka ili preusmjeravanje internetskih adresa na druge stranice.[22]

Crimeware je zlonamjerni softver koji pomaže u obavljanju kriminalnih radnji putem računala, a uključuje:[23]

- krađu identiteta,
- ucjene,
- krađu podataka,
- slanje elektroničke pošte bez znanja korisnika.

Krajnji cilj ovog softvera je stjecanje nepripadajuće imovinske koristi kriminalnim radnjama.

Scareware je zlonamjerni softver koji se širi prijevarom ili plašenjem korisnika. Pri inficiranju se korisnika lažno uvjerava da mu je računalo zarazio virus i da za rješenje problema treba preuzeti antivirusni program koji je zapravo lažni. Ponekad se korisniku nudi i lažna nadogradnja softvera.[24]

Keylogger je namijenjen praćenju pritisnutih tipki na računalu. Ovakav softver se može koristiti za kontrolu zaposlenika ili kontrolu aktivnosti djece na računalu. U praksi se najčešće koristi za krađu povjerljivih podataka (zaporki, brojeva kreditnih kartica, PIN-ova itd.). Najčešći načini širenja keylogger softvera su:[25]

- u e-mail privitcima,
- otvaranjem datoteka na P2P mrežama,
- preko web preglednika,
- preko drugog zlonamjernog softvera.

[22] CERT, O adware/spyware softveru, dostupno na http://www.cert.hr/adware/, (23.3.2018.)
[23] CERT, O crimeware softveru, dostupno na http://www.cert.hr/crimeware/, (23.3.2018.)
[24] CERT, O scareware softveru, dostupno na http://www.cert.hr/scareware/, (23.3.2018.)
[25] CERT, O keylogger softveru, dostupno na http://www.cert.hr/keyloggeri/, (23.3.2018.)

Rootkit napadaču omogućuje udaljenu administrativnu kontrolu nad računalom, a obično ga je teško uočiti. Do zaraze može doći na mnoge načine i na mnogo razina:[26]

- na aplikacijskoj razini – rootkit napada korisničke aplikacije na zaraženom računalu,
- na razini sistemskih biblioteka –rootkit napada sistemske biblioteke mijenjajući njihov izvršni kod,
- na razina operacijskog sustava, kad se rootkit ubacuje u jezgru operacijskog sustava, gdje ih je vrlo teško otkriti jer djeluju na istoj razini kao i operacijski sustav koji upravlja računalom,
- na razini upravitelja virtualnim strojem, gdje zaobilazi operacijski sustav i vrlo teško ga je otkriti,
- na razini hardvera, kad rootkit izvršni kod ugrađuje u upravljačke programe hardvera,

U novije vrijeme su najčešći rootkitovi koji djeluju na razini operacijskog sustava, gdje ih je teško otkriti i gdje mogu biti prisutni godinama.

Kako je računalna sigurnost već desetljećima globalni fenomen, na nacionalnim razinama su osnovane ustanove i organizacije koje se bave pitanjima računalne sigurnosti. U Republici Hrvatskoj djeluje CERT (*engl. Computer Emergency Response Team*), organizacija koja se bavi računalno-sigurnosnim incidentima, te preventivno djeluje s ciljem podizanja računalne sigurnosti informacijskih sustava na višu razinu.

Kako je internet globalna mreža, problemi računalne sigurnosti ne poznaju granice, pa mnoge nacionalne organizacije ostvaruju dosta dobru suradnju s drugim državama. Mjerodavnost pojedine organizacije temelji se na korištenju njene domene ili IP adresnog prostora.

Hrvatski CERT kontinuirano provodi proaktivne mjere s ciljem prevencije incidenata, te reaktivne mjere čija je zadaća ublažavanja eventualnih šteta nastalih tijekom trajanja incidenta. U području svog djelokruga CERT provodi sljedeće proaktivne mjere:[27]

- praćenje stanja računalne sigurnosti i davanje obavijesti s ciljem sprečavanje šteta zbog ugroze računalne sigurnosti širih razmjera,

[26] CERT, O rootkit softveru, dostupno na http://www.cert.hr/rootkitovi/, (23.3.2018.)
[27] CERT, O nacionalnom CERT-u, http://www.cert.hr/onama/, (20.3.2018.)

- kontinuirano praćenje novih tehnologija i informiranje javnosti o značajnim promjenama,
- informiranje javnosti o računalnoj sigurnosti putem dokumenata, preporuka i uputa,
- podizanje svijesti kod širokog kruga korisnika o važnosti računalne sigurnosti,
- informiranje i edukacija javnosti putem raznih promidžbenih akcija,
- provođenje edukativnih akcija za točno određene skupine korisnika.

Ukoliko je već došlo do značajnije ugroze računalne sigurnosti, CERT provodi sljedeće reaktivne mjere:[28]

- na temelju spoznaja o incidentu objavljuje sigurnosna upozorenja, te ih distribuiraju cjelokupnoj javnosti ili određenoj ugroženoj skupini korisnika,
- izdaje sigurnosne preporuke o slabostima u informacijskim sustavima,
- svojim djelovanjem olakšava iznalaženje najboljih rješavanja s ciljem ublažavanja posljedica incidenta,
- provodi druge mjere čiji je cilj otklanjanje posljedica ugroze informacijskih sustava.

Iz svega navedenog može se zaključiti da je ljudski faktor najčešći uzrok ugroze sigurnosti informacijskih sustava. Stoga je stalna edukacija svih korisnika sustava ključna za njegovu sigurnost.

U protekloj godini CERT je zaprimio 732 prijave o računalnim incidentima,[29] a vrste incidenata i trend u odnosu na 2016. godinu prikazani su na slici.

[28] Ibid.
[29] CERT, Godišnji izvještaj nacionalnog CERT-a za 2017. godinu, http://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf, (23.3.2018.), str. 16

Slika 14: Računalni incidenti u 2017. godini

TIP INCIDENTA	BROJ	TREND
Web defacement	370	▲
Phishing URL	127	▼
Phishing	59	▲
Malware URL	42	▼
Spam	29	▲
Nedozvoljena mrežna aktivnost	28	▲
Spam URL	26	▲
Bot	20	▲
Ostale vrste napada i zlouporabe	12	▲
DoS	10	▼
Malware domain	4	▲
Ostala kompromitirana računala	3	▼
C&C	2	–
UKUPNO	732	▲

Izvor: CERT, Godišnji izvještaj nacionalnog CERT-a za 2017. godinu, http://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf, (23.3.2018.), str. 16

5. ZAKLJUČAK

Za bilo koju djelatnost u modernom društvu nužno je imati mnoštvo informacija koje trebaju biti točne, pouzdane i pravovremene. Stoga je kvalitetan informacijski sustav nezaobilazan dio svake ozbiljne organizacije. Informacije su nužne za analizu dosadašnjeg poslovanja, uvid u trenutne zahtjeve i potrebe, kao i za planiranje budućih poslovnih poteza. Stoga je zadaća svakog informacijskog sustava prikupljanje, obrada, distribucija i arhiviranje podataka.

U modernom društvu informacije imaju sve veću vrijednost, te su kao takve često na meti mnogih kriminalaca. Motiv za neovlašten pristup i krađu podataka može biti stjecanje imovinske koristi, ali i želja za nanošenjem štete nekoj instituciji. Stoga je briga za sigurnost podataka jedna od važnih sastavnica svakog informacijskog sustava.

Do ugroza informacijskog sustava najčešće dolazi zbog ljudskog čimbenika, bilo zbog nemara, neznanja ili nekog drugog razloga. Stalna edukacija korisnika informacijskog sustava, te praćenje i dokumentiranje svih oblika ugroze znatno smanjuju mogućnost nastanka štete zbog gubitka ili neovlaštenog pristupa podatcima.

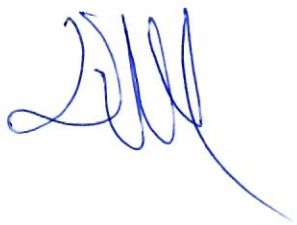
Nekvalitetan hardver i softver također mogu znatno utjecati na sigurnost informacijskog sustava, osobito ako računala na kojima su pohranjeni podatci imaju pristup internetu a ne posjeduju kvalitetnu hardversku i softversku zaštitu. Izloženost virusima i drugim oblicima malicioznog softvera predstavlja veliku opasnost za informacijski sustav. Svakodnevno ažuriranje antivirusnog softvera i operacijskog sustava, kao i softvera za obradu podataka znatno smanjuju opasnost od gubitka podataka.

Zatvor u Gospiću kao specifična institucija ima mnoge sigurnosne izazove, te je na svim korisnicima informacijskog sustava velika odgovornost za sigurnost podataka. Poslovanje Zatvora se odvija na tri lokacije, te je nužna svakodnevna razmjena podataka među njima. Također je nužna i razmjena podataka s Ministarstvom pravosuđa, a kako se za komunikaciju koristi javna mreža (internet), nužna je dodatna zaštita u obliku vatrozida i virtualne privatne mreže. Na taj način se znatno umanjuje mogućnost neovlaštenog pristupa podatcima i mogućnost krađe, neovlaštene izmjene ili uništavanja podataka.

Bez obzira na stupanj edukacije i osposobljenosti korisnika informacijskog sustava, oni su i dalje glavni oblik njegove ugroze. Stoga su u svakom sustavu koji ima pristup javnoj mreži nužne restrikcije koje će onemogućiti namjernu ili nenamjernu ugrozu

sustava. U Ministarstvu pravosuđa, u čiju nadležnost spadaju i svi zatvori, pristup lokalnih računala internetu odvija se posredstvom tzv. *proxy servera* koji omogućuju pristup samo određenim mrežnim stranicama poput dnevnog tiska, HAK-a i slično. Ovi poslužitelji uz ograničenje pristupa omogućuju i skrivanje IP adresa lokalnih računala, čime se znatno otežava pristup računalu izvan lokalne mreže.

Značajna mjera koja osigurava zaštitu informacijskog sustava je i dodjela odgovarajućih prava i ovlasti svakom korisniku sustava. Korisnik koji je prijavljen kao obični korisnik (*engl. user*), bez administrativnih ovlasti, ne može svojim aktivnostima znatno utjecati na stabilnost operacijskog sustava, niti može dodavati ili uklanjati pojedine aplikacije. Na taj način se znatno smanjuje mogućnost softverske pogreške, kao i mogućnost štete nastale zbog neovlaštenog upada korisnika izvan lokalne mreže.



LITERATURA

1. CARNet, Logiranje NAT prometa, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-06-160.pdf, (15.3.2018.
2. CARNet, TLS protokol, dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-03-257.pdf, (17.3.2018.)
3. Centar informacijske sigurnosti, Modeliranje sigurnosnih prijetnji, dostupno na https://www.cis.hr/files/dokumenti/CIS-DOC-2012-05-049.pdf (16.1.2018.)
4. CERT, Godišnji izvještaj nacionalnog CERT-a za 2017. godinu, http://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf, (23.3.2018.)
5. CERT, O adware/spyware softveru, dostupno na http://www.cert.hr/adware/, (23.3.2018.)
6. CERT, O crimeware softveru, dostupno na http://www.cert.hr/crimeware/, (23.3.2018.)
7. CERT, O keylogger softveru, dostupno na http://www.cert.hr/keyloggeri/, (23.3.2018.)
8. CERT, O rootkit softveru, dostupno na http://www.cert.hr/rootkitovi/, (23.3.2018.)
9. CERT, O scareware softveru, dostupno na http://www.cert.hr/scareware/, (23.3.2018.)
10. CERT, O virusima, dostupno na http://www.cert.hr/virusi/, (23.3.2018.)
11. CERT, Zlonamjerni softver, dostupno na http://www.cert.hr/19795-2/malver/, (25.3.2018.)
12. Ćurko, Katarina, Skladište podataka - sustav za potporu odlučivanju, 2001., dostupno na https://hrcak.srce.hr/file/45126, (14.1.2018.)
13. Jakupović, Alen, Utjecaj oslonjivosti informacijskog sustava na poslovne organizacije, Zbornik Veleučilišta u Rijeci, 1(1), 165-178. 2013., dostupno na https://hrcak.srce.hr/103341 (14.1.2018.)

14. Klasić, Ksenija, Zaštita informacijskih sustava u poslovnoj praksi, Sigurnost: časopis za sigurnost u radnoj i životnoj okolini, 49(1), 37-47. 2007., dostupno na https://hrcak.srce.hr/11861 (10.2.2018.)
15. Pavlić, Mile, Informacijski sustavi, Zagreb, Školska knjiga, 2011.
16. Pralas, Toni, Računalne mreže – OSI referentni model, dostupno na https://sysportal.carnet.hr/node/352, (12.3.2018.)
17. Pralas, Toni, Računalne mreže – adresiranje, dostupno na https://sysportal.carnet.hr/node/393, (12.3.2018.)
18. Radić, Branimir, Sigurnosne računalne prijetnje, 2012., dostupno na http://www.srce.unizg.hr/arhiva_weba/sistemac2015/fileadmin/user_root/seminari/Srce-Sys-Seminari-Sigurnosne_racunalne_prijetnje.pdf (5.2.2018.)
19. Sviličić, Boris, Kraš, Antun, Zaštita privatnosti računalnog sustava, Pomorstvo, 19(1), 275-284. 2005., dostupno na https://hrcak.srce.hr/3962 (10.2.2018.)
20. Šimović, Vladimir, Uvod u informacijske sustave, Zagreb, Golden marketing – Školska knjiga, 2010.

POPIS SLIKA