SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET

Tomislav Bukovac

SIGURNOST INFORMACIJSKIH SUSTAVA

DIPLOMSKI RAD

Zagreb, 2016.

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET

Tomislav Bukovac

Matični broj:346539 - D

Studij: Informacijske znanosti - Istraživačka informatika

SIGURNOST INFORMACIJSKIH SUSTAVA

DIPLOMSKI RAD

Mentor:
Dr.sc. Krešimir Pavlina

Zagreb, listopad 2016.

Sadržaj

1. Uvod

U današnje vrijeme privatne i državne organizacije posjeduju velike količine povjerljivih informacija koje je potrebno adekvatno zaštititi kako bi se sačuvala njihova povjerljivost. Informacija se danas smatra resursom te gubitkom povjerljivosti neke informacije to ima štetno djelovanje na samu organizaciju.

U ovom radu objasniti ću glavne pojmove koji su sadržani u sigurnosti informacijskih sustava i približiti čitatelja važnosti sigurnosti informacija i informacijskih sustava.

U prvom poglavlju objasniti ću pojmove informacije i sustava koji su važni za shvaćanje informacijskih sustava. Kako je svaki informacijski sustav dio neke organizacije tj. poslovnog sustava objasniti ću što je to poslovni sustav i što je njegov informacijski sustav. Proći ću kroz povijest razvoja informacijskih sustava, njegove dijelove te vrste informacijskih sustava. Kako postoji više podjela informacijskih sustava o svakoj od njih ću reći nekoliko riječi te objasniti njihove podsustave.

U drugom poglavlju koncentrirati ću se na pojam sigurnosti i informacijske sigurnosti. Detaljno ću objasniti zašto je pojam informacijske sigurnosti važan, osobito u današnje doba. Također opisati ću tri glavna aspekta informacijske sustav, koja slobodno možemo nazvati „zlatnim“ pravilima informacijske sigurnosti.

Treće poglavlje rezervirano je za sigurnosne prijetnje informacijskom sustavu. Nabrojati ću i opisati vrste prijetnji informacijskom sustavu prema njihovom izvoru. Nabrojati ću i opisati metode napada kojima se koriste napadači te navesti neke primjere za svaku od pojedinih metoda. U nastavku rada baviti ću se zloćudnim programima jer oni danas predstavljaju najveću opasnost informacijskim sustavima. Upoznati ću vas sa programima za praćenje unosa sa tipkovnice, virusima, trojanskim konjem, napadima otimanjem sjednice, metodama prijevare phishing i pharming te distribuiranim napadima uskraćivanjem usluge.

U četvrtom poglavlju objasniti ću kako zaštiti informacijske sustave pomoću fizičkih, programskih i organizacijskih metoda zaštite informacijskih sustava. Prvo ću objasniti fizičke metode zaštite informacijskih sustava. Prikazati ću tri osnovna načina fizičke metode zaštite informacijskih sustava te za svaku nabrojati nekoliko elemenata s kojima se to postiže.

Sljedeća je programska metoda zaštite informacijskih sustava. Ovdje ću objasniti kako se informacijski sustav može zaštititi na razini operacijskog sustava, na razini korisničkih aplikacija, objasniti ću kako se kriptografija uklapa u zaštitu informacijskih sustava, kako se informacijski sustavi štite uz pomoć antispyware i antivirusnih alata te zaštitnog zida. Pojasniti ću način rada svakog od ovih programskih alata. Nastavljamo sa trećom i posljednjom metodom zaštite informacijskog sustava, a to su organizacijske metode. To su mjere koje poduzima sam poslovni sustav radi svojih potreba. Organizacijske metode imaju tri razine. Prva od njih je infrastruktura informacijske sigurnosti koja objašnjava kako se kroz komunikaciju i organizaciju unutar poslovnog sustava podiže sigurnost operacijskih sustava. Druga je kontrola pristupa koja je usko povezana sa trećom koja je outsourcing. Ove dvije metode su slične, jedina razlika je u fizičkom smještaju korisnika. Kontrola pristupa govori o sigurnosti informacijskih sustava unutar organizacije tj. objekta organizacije i kako zaštiti informacijski sustav od unutarnjih prijetnji sa treće strane dok se outsorcing koncentrira na vanjske poslovne partnere i njihov pristup informacijskom sustavu te odnos sa informacijama.

Posljednje poglavlje bavi se zakonskim aspektima informacijskih sustava. Navesti ću glavne institucije koje donose zakone i regulative o informacijskoj sigurnosti u Republici Hrvatskoj. Za svaku od njih ću navesti njihove ciljeve i zadaće kojima oni pridonose informacijskoj sigurnosti u Republici Hrvatskoj.

Cilj ovog rada je pojasniti korisniku važnost sigurnosti informacijskih sustava, a time i njegovih privatnih i povjerljivih podataka.

2. Informacija i informacijski sustavi

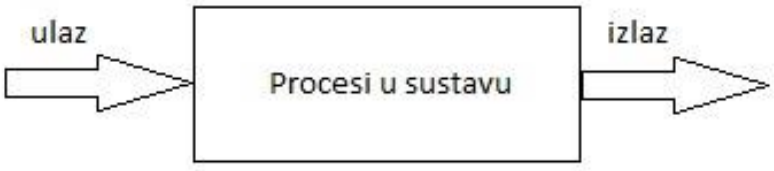
2.1. Informacija i sustav

Kako bi lakše shvatili pojam informacijskog sustava prvo ću definirati pojmove informacija i sustav.

Informacija je podatak obrađen u obliku koji je smislen njezinom primatelju i koji ima stvarnu ili percipiranu vrijednost za njegove sadašnje i buduće odluke i akcije.[1]

Informacija je organizacijski resurs i postala je presudna u današnjem svijetu visoke tehnologije, te onaj tko posjeduje pravu informaciju u pravo vrijeme ima veliku prednost. Stoga se informaciji i informacijskim sustavima pridaje tolika važnost. Informacija kao resurs je specifična jer se ona ne troši i može se upotrebljavati više puta od više korisnika. Zbog toga je bitno pohranjivati informacije jer ona može zatrebati u bilo kojem trenutku. Informacije su ključni faktor poslovnog sustava jer bez informacija nema ni poslovanja. Iz tog razloga svaki poslovni sustav ima svoj vlastiti informacijski sustav, koji mu služi da se obrađuju podaci o svim segmentima poslovanja.

Sustav je svaki uređen skup od najmanje dva elementa koji zajedno interakcijom ostvaruju funkciju cjeline.[2] Pri tome je cilj sustava transformacija različitih vrsta ulaza u izlaz. Transformacija se obavlja djelovanjem različitih procesa u sustavu, ovisno o prirodi promatranog sustava.



Slika 1. Transformacija ulaza u izlaz

[1]G. B. Davis, M. H. Olson, Management Information Systems: ConceptualFoundations, StructuraandDevelopment, McGraw- Hill, New York, SAD, 1985., str. 200.

[2]Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.13

2.2. Poslovni sustav i njegov informacijski sustavi

Nakon definicije sustava bitno je definirati i pojmove poslovnog i informacijskog sustava. To će nam olakšati daljnje razumijevanje ovog rada.

Poslovni sustav je organizacijski sustav kojeg opisuje skup informacija o prošlosti i sadašnjosti i poslovnih procesa koji ih obrađuju.[3] Poslovne sustave karakteriziraju materijalni ulazi i izlazi te informacijski tokovi. U ulaze spadaju sirovine, dokumenti, poruke, energija, a u izlaze dokumenti i proizvodi. U procesu pretvorbe ulaza u izlaze sudionici procesa mogu biti ljudi (kao izvršitelji posla), alati i razni strojevi. Postojanje informacija je osnova za obavljanje funkcija poslovnog sustava.

Svaki poslovni sustav ima svoj informacijski sustav, a uloga mu je stalna opskrba informacijama na svim razinama upravljanja, odlučivanja i svakodnevnog poslovanja. Informacijski sustavi se izrađuju po potrebama korisnika, pa ako poduzeća koja se bave različitim djelatnostima imaju različite informacijske sustave. Najvažnije komponente za svaku djelatnost i uspješno poslovanje su prikupljanje, obrada i korištenje podataka, pa tako poduzeće s dobro izgrađenim informacijskim sustavom uspješnije posluje. Ovisno o vidu poslovanja organizacije informacijski sustav može, ali i ne mora, biti podržan računalom u cijelosti ili samo određenim segmentima.

Zadaci informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje podataka svim jedinicama poslovnog sustava. Zapravo uloga informacijskog sustava jest proizvesti informaciju na temelju podataka. Podatak je logička cjelina i sama za sebe ne mora imati neko značenje. Podatak se pretvara u informaciju kada mu pridodamo neko značenje. Podaci su primjerice: Tomislav, 7, 10, Karlovac, 1987. Bilo koji od tih podataka može predstavljati bilo što, primjerice broj 7 može predstavljati 7 kilometara, 7 godina, 7 kuna i tome slično, ali kada mu se prida neko značenje tada postaje informacija. Skup prije navedenih podataka nakon organiziranja i obrade predstavlja informaciju da je Tomislav rođen 7.10.1987. godine u Karlovcu. Dakle podatak je činjenica o nečemu iz realnog svijeta, dok je informacija interpretacija podataka koja ima subjektivno

[3]Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.16

značenje za primatelja. Informacijski sustav proizvodi informacije tako da podatke obrađuje, organizira i prikazuje na način koji je razumljiv korisniku, a korisnik tako pripremljene podatke interpretira i na temelju njih donosi odluke.

Ciljevi informacijskih sustava različiti su za različite radne razine. Najčešća podjela je na tri radne razine: razinu izvođenja (operativnu razinu), razinu upravljanja (taktička razina) i razinu odlučivanja (strateška razina).[4] U razinu izvođenja spadaju procesi osnovne djelatnosti, a cilj informacijskih sustava na toj razini je povećanje produktivnosti. Upravljačka razina odgovorna je za organiziranje, praćenje uspješnosti te otklanjanje smetnji, a cilj informacijskih sustava je povećanje učinkovitosti. Razina odlučivanja odgovorna je za postavljanje poslovnih ciljeva poduzeća i zadaća joj je osiguranje stabilnosti rasta i razvoja.

2.2.1. Povijest razvoja informacijskih sustava

Na spomen informacijskih sustava uvijek prvo pomislimo na računala, međutim poslovni sustavi mogu imati informacijske sustave bez upotrebe računala. Prema tome informacijski sustav je svaki sustav koji se koristi u poslovanju, a zadatak mu je prikupiti, razvrstati, obraditi, čuvati te rasporediti podatke i on ne mora nužno biti podržan računalom.

2.2.1.1. Faze obrade podataka

Moguće je razlučiti četiri osnovne faze u razvoju načina obrade podataka. Neke od ovih faza se i danas primjenjuju.

Faze u razvoju načina obrade podataka:

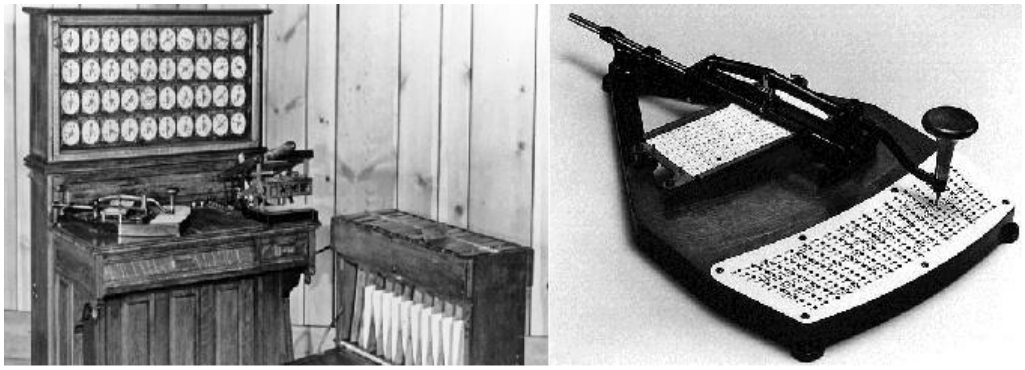
1. **Faza ručne obrade podataka**
   U ovoj fazi primjenjuje se rad ruku, medij za pohranu podataka i sredstva za pisanje po tom mediju. Medij je bio kamen u koji su se klesali simboli, papirus, glinene pločice te papir. Ovu fazu karakterizira spora obrada podataka, mala količina obrađenih podataka i upitna točnost podataka.
2. **Faza mehaničke obrade podataka**

[4]http://documents.tips/documents/informacijski-sustavi-skripta.html, 10.10.2016.

Ova faza posljedica je razvoja znanosti i tehnike. Počinje sredinom 17. stoljeća. U to doba konstruirani su prvi uređaji za obradu podataka. Glavne odlike ove faze su povećanje produktivnosti, točnosti i količine obrađenih podataka.

3. **Faza elektromehaničke obrade podataka**

   Ova faza počinje sredinom 19. stoljeća kada je vlada SAD-a raspisala javni natječaj za konstruiranjem uređaja kojim bi se što brže obradili podaci sa popisa stanovništva. Pobjedu na natječaju odnosi Hermann Hollerith s prijedlogom da nositelj podataka bude bušena kartica (Hollerith kasnije osniva poduzeće iz kojeg nastaje IBM). Za obradu podataka se upotrebljavao poseban elektromehanički uređaj. Ovime je omogućena masovna obrada velike količine podataka.



Slika 2. Tabulatorski stroj i bušena kartica

4. **Faza elektroničke obrade podataka**

   Ova faza počinje 1944. godine s razvojem ENIAC-a, koje se smatra prvim "pravim" računalom. Glavne odlike ove faze su mogućnost obrade velike količine podataka u kratkom vremenskom razdoblju sa zanemarivim brojem grešaka.

2.2.2. Dijelovi informacijskog sustava

Informacijski sustav sastoji se od 6 glavnih dijelova, od kojih je svaki potreban za odvijanje osnovnih funkcija informacijskog sustava. Glavni dijelovi informacijskog sustava i njihov opis nalaze se u tablici 1.

Dijelovi informacijskog sustava	Opis
Podaci	Ulaz koji je sustavu potreban za generiranje informacija
Hardver	Računala i njihova periferijska oprema; ulazni i izlazni uređaji, uređaji za pohranu podataka te komunikacijska oprema
Softver	Setovi instrukcija koji govore računalu kako primiti, obraditi, prikazati i pohraniti podatke i informacije
Komunikacije (mreža)	Hardver i softver koji omogućuje brzo primanje i slanje podataka i informacija u raznim oblicima (tekst, slika, zvuk)
Ljudi	Informacijski stručnjaci koji analiziraju informacijske potrebe organizacije, kreiraju informacijske sustave, održavaju informacijske sustave i popratnu opremu
Procedure	Pravila kojima se postiže sigurnost i optimalni rezultati pri obradi podataka

Tablica 1. Dijelovi informacijskog sustava (prema http://research-methodology.net/information-system-and-its-components/)

2.2.3. Vrste informacijskih sustava

Postoji mnogo kriterija za podjelu informacijskih sustava, a oni najčešći su podjela prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija u poslovnom sustavu.

2.2.3.1. Informacijski sustavi prema konceptualnom ustrojstvu poslovodstva

Razine upravljanja u organizacijskom sustavu dijelimo na operativnu, taktičku i stratešku razinu. Zbog različitih nadležnosti i zadataka pojedinih razina informacijski sustavi se razlikuju. U tablici 2. prikazane su vrste informacijskih sustava prema konceptualnom ustrojstvu poduzeća.

Ustroj poslovodstva		Vrste informacijskog sustava	
Poslovodstvo	*Strateški nivo*	Odlučivanje	**Sustav potpore odlučivanju**
Izvršno vodstvo	*Taktički nivo*	Upravljanje	**Izvršni informacijski sustavi**
Operativno vodstvo	*Operativni nivo*	Izvođenje	**Transakcijski sustavi**

Tablica 2. Vrste informacijskih sustava prema konceptualnom ustrojstvu poslovodstva (prema Klarin, Klasić, 2009, str.23)

Kao što vidimo u tablici operativnoj razini namijenjeni su transakcijski sustavi. Uloga im je izvođenje procesa osnovnih djelatnosti npr. sustav kojim se evidentiraju pojedini koraci u proizvodnji. Taktičkoj razini namijenjeni su izvršni informacijski sustavi, čiji rezultat su izvješća potrebna za upravljanje. Informacijski sustav strateške razine je sustav potpore odlučivanju.

2.2.3.2. Informacijski sustavi prema namjeni

Prema namjeni informacijski sustavi se dijele na:

- Sustave za obradu podataka
- Sustave podrške u uredskom poslovanju
- Sustav podrške u odlučivanju
- Ekspertni sustavi

Zadatak sustava za obradu podataka je unos, obrada i pohranjivanje podataka o stanju sustava i poslovnim događajima. Podaci se pohranjuju u baze podataka. Pristupa im se pomoću posebnih programa za pretraživanje baze podataka. Na temelju obrađenih podataka kreiraju se izvješća potrebna za izvođenje procesa osnovne djelatnosti, ali i za upravljanje. Područje primjene su dobro strukturirana problemska područja čiji se procesi mogu strukturalno opisati.

Sustavi podrške u uredskom poslovanju dijeli se na sustave za podršku u administrativnim poslovima (potpora za rad u skupini, prezentacije i sl.) i sustava za podršku ljudskog komuniciranja (e-mail, telekonferiranje i sl.). Primjenjuje se za dobro strukturirane ponavljajuće uredske poslove.

Sustavi podrške u odlučivanju koriste različite modele odlučivanja kojima se dobivaju informacije potrebne za odlučivanje, kao podrška pojedincu i grupi. Primjenjuje se u djelomično strukturiranim procesima donošenja odluka.

Ekspertni sustavi najčešće služe kao potpora ekspertima, te služe za potrebe konfiguriranja i dijagnosticiranja sustava. Oni sadržavaju informacije i znanja za uska problemska područja.

2.2.3.3. Informacijski sustavi prema modelu poslovnih funkcija u poslovnom sustavu

Prema modelu poslovnih funkcija informacijski sustavi se dijele na podsustave kojima su pokrivena pojedina poslovna područja. Može ih biti onoliko koliko ima i poslovnih funkcija u poduzeću. Broj im ovisi o organizaciji poslovanja poduzeća, pa tako poduzeća koja se bave istom djelatnosti mogu imati različit broj informacijskih podsustava. To mogu biti[5]:

- Informacijski podsustav (IPS) planiranja i analize poslovanja,
- IPS upravljanja trajnim proizvodnim dobrima,
- IPS upravljanja ljudskim resursima,
- IPS upravljanja financijama,
- IPS nabave materijala i sirovina,
- IPS prodaje proizvoda i usluga,
- IPS računovodstva,
- IPS istraživanja i razvoja itd.

Kako različiti poslovni sustavi nemaju isti značaj primjene informacijskih sustava razlikujemo četiri osnovna tipa informacijskih sustava. To su:

[5]Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.25

- **Operativni** informacijski sustav - o njemu ovisi uspjeh tekućeg poslovanja. U ovom slučaju informacijski sustav služi kao potpora svakodnevnom poslovanju.
- **Potporni** informacijski sustav - koristan, ali nije nužan za uspješno poslovanje poduzeća. Ovisnost funkcioniranja poduzeća o informacijskom sustavu je vrlo mala.
- **Strateški** informacijski sustav - ovaj sustav je kritičan za buduće poslovanje poduzeća. Mora omogućiti sigurnu pohranu i brzu obradu velikih količina podataka. Uspjeh poduzeća uvelike ovisi o ovom informacijskom sustavu.
- **Izgledni** informacijski sustav - može utjecati na buduće poslovanje, pa možemo reći da je ovisnost poduzeća o informacijskoj tehnologiji mala, ali je utjecaj informatike na poslovni rezultat značajan.

Svakom poslovnom sustavu pripada neki informacijski podsustav te se tako ovisno o djelatnosti poduzeća može odrediti tip informacijskog podsustava. Također tako se može i ocijeniti redoslijed izgradnje informacijskog sustava. Često on započne kao potporni informacijski sustav pa prerasta u izgledni koji je važan za buduća poslovanja.

Neovisno o tipu informacijskog sustava, u njega se spremaju podaci potrebni za daljnju obradu i izvješćivanje. Upravo o kvaliteti tih podataka ovisi i kvaliteta informacijskog sustava. Kako je informacijski sustav dio poslovnog sustava, o njegovoj kvaliteti direktno ovisi i poslovanje poduzeća. Stoga kvalitetan informacijski sustav mora zadovoljiti sljedeća načela[6]:

- Informacijski sustav je model poslovne tehnologije organizacijskog sustava
- Podaci su resurs poslovnog sustava
- Temelj razmatranja prilikom određivanja podsustava su poslovni procesi kao nepromjenjivi dio određene poslovne tehnologije
- Informacijski sustav izgrađuje se integracijom podsustava na osnovi zajedničkih podataka – modularnost
- Informacije za upravljanje i odlučivanje izvode se na temelju zbivanja na razini izvođenja

[6]Brumec, J.: Projektiranje i metodike razvoja IS-a,Euro Data, Zagreb, 1996.

Informacijski sustav izrađen na primjeni navedenih načela u potpunosti zadovoljava svoju zadaću, a to je prikupljanje, obrada, pohrana te distribucija podataka svima kojima je to potrebno. Cilj postojanja informacijskog sustava je unaprijediti poslovanje i ostvariti pozitivan poslovan rezultat.

3. Sigurnost i informacijska sigurnost

Kako je tema ovog rada sigurnost informacijskih sustava potrebno je definirati i pojmove sigurnost i informacijska sigurnost.

3.1. Sigurnost

Sigurnost se može definirati kao proces održavanja prihvatljivog nivoa rizika. Kada je riječ o zaštiti informacijskih sustava i sigurnosti tada postoji nekoliko osnovnih pravila[7]:

- sigurnost je proces, skup usluga, proizvoda ili procedura te raznih drugih elemenata i mjera koje se konstantno provode
- apsolutna sigurnost ne postoji
- uz različite tehničke zaštite potrebno je razmotriti i ljudski faktor sa svim svojim slabostima

Informacija se smatra imovinom koja omogućuje normalno poslovanje organizacije i kao takvu ju je potrebno prikladno zaštititi. Taj zahtjev postaje sve važniji zbog distribuiranosti poslovne okoline, jer su u takvom okruženju informacije izložene većem broju prijetnji i ranjivosti. Bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti prikladno zaštićena.

3.2. Informacijska sigurnost

Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.[8]

Informacijska sigurnost postaje sve važnija u modernom društvu. Moderni državni i gospodarski subjekti ovise o računalnoj i komunikacijskoj infrastrukturi. To omogućuje

[7]Prema:http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustava_0.pdf

[8]http://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost

protok velike količine informacija među subjektima, ali ujedno izlaže informacije i njima pripadne informacijske sustave brojnim prijetnjama. Pod pojmom informacijske sigurnosti podrazumijeva se zaštita informacija od velikog broja prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija. Informacijska sigurnost se postiže primjenom odgovarajućih kontrola, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkcije sklopovske i programske opreme. Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, pregledavati i poboljšavati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahtjeva organizacije. Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te radi sprječavanja gubitaka cjelovitosti ili raspoloživosti samih sustava. Sigurnosne mjere uključuju mehanizme i procedure koje trebaju biti implementirane u svrhu odvraćanja, prevencije, detektiranja i oporavka od utjecaja incidenata koji djeluju na povjerljivost, cjelovitost i raspoloživost podataka i pratećih sustavskih servisa i resursa, uključujući i izvještavanje o sigurnosnim incidentima. Definiranje, implementacija, održavanje i poboljšavanje informacijske sigurnosti može biti od presudne važnosti kako bi se ostvarila i zadržala konkurentnost, osigurao dotok novca i profitabilnost, kako bi se zadovoljile zakonske norme i osigurao poslovni ugled. Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, špijunaže, sabotaže, vandalizma, požara, poplave i sl. Šteta nanesena organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge je sve prisutnija pojava. Informacijska sigurnost je jednako važna javnim i privatnim organizacijama. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Upravljanje informacijskom sigurnošću zahtjeva sudjelovanje svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan granica organizacije.

3.2.1. Aspekti informacijske sigurnosti

Tri su osnovna aspekta informacijske sigurnosti. Cilj svakog informacijskog sustava je zaštititi informacije od neovlaštenih izmjena, odnosno osigurati integritet, zaštititi informacije od neželjenog objavljivanja, osigurati povjerljivost i u konačnici osigurati dostupnost informacija ovlaštenim korisnicima. Povezanost ovih tri aspekta prikazana je na slici 3. kroz osnovni sigurnosni trokut (eng. CIA triad).

Slika 3. Osnovni sigurnosni trokut

Prvi aspekt informacijske sigurnosti je povjerljivost podataka. On podrazumijeva tajnost podataka i dostupnost podataka samo ovlaštenim osobama. Kod ovog aspekta najveća pažnja posvećena je identifikaciji i autentifikaciji korisnika.

Postoje razne prijetnje što se tiče povjerljivosti podataka. Najčešće su: hakiranje, neovlaštena korisnička aktivnost, nezaštićeno preuzimanje datoteka, lokalne mreže, trojanski konji i sl. Postoje dvije metode zaštite povjerljivosti informacija, a to su korištenje kontrole pristupa i metoda enkripcije. Kontrola pristupa vrlo je jednostavna metoda zaštite. Osobe koje su ovlaštene za pristup informacijama moći će doći do njih, a ostalim korisnicima pristup tim informacijama je onemogućen. Metoda enkripcije nešto je kompliciranija pa tako ovlašteni korisnici moraju imati tajni ključ koji im omogućuje uvid u informacije.

Drugi aspekt sigurnosti informacija je integritet. Pod integritetom smatra se da se informacije (podaci) ne mogu izmijeniti bez odgovarajućeg ovlaštenja. Odnosno onemogućuju se promjene informacija od strane neovlaštenih osoba ili neovlaštene promjene od strane ovlaštenih osoba.

Ciljevi integriteta su sprječavanje neovlaštenih korisnika da modificiraju podatke ili programe, zatim sprječavanje ovlaštenih korisnika da modificiraju podatke ili programe na nepropisan i neovlašten način i u konačnici održavanje konzistentnosti podataka i programa. Baš kao i povjerljivost, integritet se održava upotrebom kontrole pristupa i enkripcijskim

algoritmom. Način na koji se može vidjeti gubitak integriteta jest u slučaju da neovlašteni korisnik napravi bilo kakve promjene na podacima. Izvorni podaci će u ovom slučaju biti nepovratno izgubljeni. Nažalost ako neovlaštenu promjenu napravi osoba koja je ovlaštena za pristup podacima, tada nije tako lako utvrditi gubitak integriteta.

Treći aspekt informacijske sigurnosti navodi se dostupnost, a taj pojam odnosi se upravo na dostupnost podataka i informacija.

Cilj dostupnosti je osigurati korisniku prave podatke u pravo vrijeme. Danas postoje i sustavi visoke dostupnosti čija arhitektura je usmjerena na postizanje visoke dostupnosti. Važna karakteristika ovog sustava je da padom ili gubitkom jednog elementa ne gubimo cijeli sustav, već on i dalje nastavlja s radom.

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

Gledano u globalu najviše prijetnji se odnosi prvenstveno na narušavanje tajnosti informacija što je povezano s povjerljivosti. Kada je riječ o integritetu podataka, njegovo narušavanje može se dogoditi kroz neovlaštene promjene, a prekid rada sustava uzrokuje nedostupnost servisa ili podataka.

Možemo zaključiti da kako bi informacijski sustavi bili djelotvorni i sigurni u svome radu potrebno je da zadovolje sve navedene aspekte.

4. Sigurnosne prijetnje informacijskom sustavu

Informacijski sustavi izloženi su raznim vrstama prijetnji. Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti materijalna ili nematerijalna šteta. Prijetnje se mogu kategorizirati i podijeliti na razne načine ali najčešća podjela je prema vrsti prijetnji prema izvoru. Kako bi što bolje odabrali mjere zaštite potrebno je što točnije odrediti vrste prijetnji informacijskom sustavu kao i način rada potencijalno opasnih programa te njihov način infiltracije.

4.1. Vrste prijetnji

Informacijski sustavi svakodnevno su izloženi raznim vrstama prijetnji. Prema raznim istraživanjima, ustanovljeno je da je najčešća vrsta prijetnje prema informacijskim sustavima ljudski faktor, odnosno ljudska pogreška. Vrste prijetnji dijelimo prema njihovom izvoru. To su:

- Prirodne prijetnje - meteorološke nepogode, geofizičke nepogode, biološke prijetnje, astrofizički fenomeni, sezonski fenomeni itd.
- Namjerne prijetnje ljudi - neautorizirani pristup, prisluškivanje, otkrivanje podataka, sabotaža, zlouporaba ovlasti, namjerno oštećenje opreme, maliciozni programi
- Nenamjerne prijetnje ljudi - nedovoljna educiranost, nepravilno rukovanje, nemar i nepažnja, nedisciplina, nenamjerno oštećenje opreme, nenamjerno brisanje podataka
- Oprema - električni kvarovi, ispad opreme, tvorničke greške, prekid komunikacije

S obzirom na izvor prijetnje, najučestalijim se pokazao ljudski faktor koji se manifestira kao namjerna ili nenamjerna prijetnja. Prijetnje uzrokovane kvarom opreme nalaze se na drugom mjestu po učestalosti kao vrsta prijetnji informacijskom sustavu, te prirodne prijetnje na trećem. Spoznajom vrste prijetnje i analizom njena uzorka, moguće je izraditi primjerene metode zaštite te na taj način zaštiti informacijskih sustav od poznatih potencijalnih prijetnji i njihovih posljedica.

4.2. Metode napada

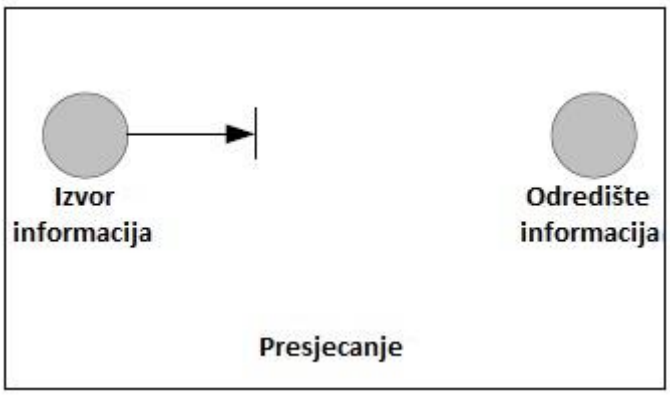
Napadi su akcije koje su usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža. Ove vrste napada se događaju prilikom prijenosa podataka unutar mreže. Postoje različite vrste napada, ali se oni generalno mogu podijeliti u četiri osnovne kategorije:

1. Presijecanje/prekidanje
2. Presretanje
3. Izmjena
4. Proizvodnja

4.2.1. Presijecanje/prekidanje

Metode napada prekidanjem onemogućuju korisniku korištenje usluge. Napadač u ovom slučaju prekida tok podatak između izvora informacija i njihovog odredišta (slika 4). Napadač kada dobije pristup korisničkoj mreži može učiniti sljedeće:

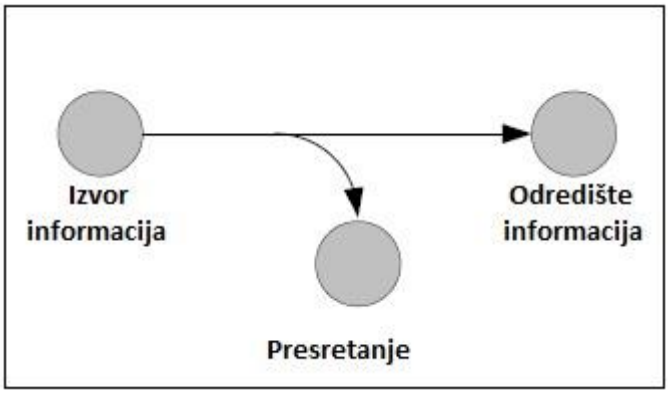
- Blokiranje prometa što rezultira gubitkom pristupa mrežnim resursima
- Prikrivanje sistemskih informacija kako se ne bi vidjela napadačeva prisutnost i eventualna mogućnost budućih napada
- Preplavljanje računala ili cijele računalne mreže s mrežnim prometom što dovodi do gašenja računala ili cijele mreže zbog preopterećenja
- Slanje štetnih podataka aplikacijama i mrežnim servisima što dovodi do njihove nestabilnosti i mogućeg prestanka rada.



Slika 4. Presijecanje komunikacije između dva korisnika

4.2.2. Presretanje

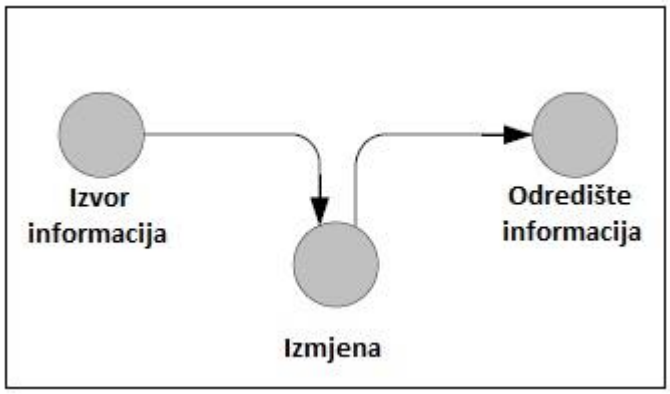
Napadi presretanjem su napadi koji se događaju posredstvom treće osobe u komunikaciji. Treća strana je u mogućnosti aktivno pratiti, bilježiti i kontrolirati komunikaciju. Napadač koji se korist presretanjem podataka, ubacuje se u komunikaciju između dvoje korisnika, te preusmjerava poruke na svoje računalo i predstavlja se kao osoba koja je u razgovoru, te pokušava izvući što je moguće više korisnih informacija (slika 5). Glavna odlika ove vrste napada je mogućnost preusmjeravanja podataka.



Slika 5. Presretanje podataka od treće strane

4.2.3. Izmjena

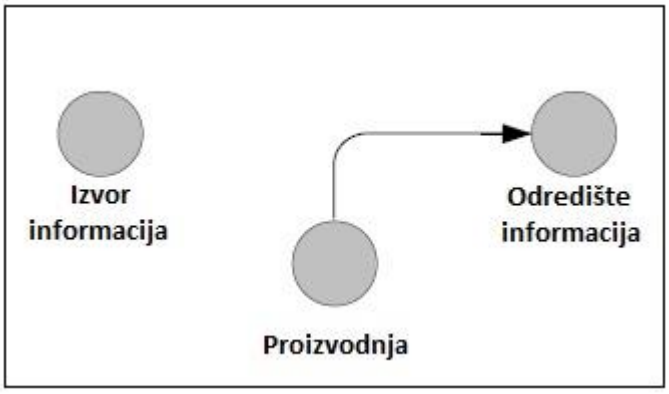
Izmjena podataka je vrsta napada kojom napadač izmjenjuje informacije između pošiljatelja i primatelja poruke. Najčešće neposredno nakon presretanja poruke, napadač bez znanja korisnika izmjenjuje njen sadržaj u svoju korist (slika 6). Ova vrsta napada je izuzetno štetna, jer korisnik može dobiti netočne informacije koje mogu štetno utjecati na poslovanje poduzeća. Najčešći slučajevi ove vrste napada su kod raznih novčanih transakcija.



Slika 6. Izmjena podataka od treće strane

4.2.4. Proizvodnja

Metoda napada proizvodnjom i umetanjem lažnih podataka osmišljena je isključivo za krađu i zlonamjerno iskorištavanje korisničkih podataka. Napadač proizvodi lažne podatke i umeće ih u korisnikovu mrežu s ciljem nanošenja štete korisniku ili krađom podataka od korisnika (slika 7).



Slika 7. Proizvodnja podataka

4.3. Zloćudni programi

Zloćudni ili maliciozni programi su zlonamjerni i štetni programski alati. To si programski alati kojima se služe napadači kako bi oštetili ili ukrali korisnikove podatke, pridobili pristup korisnikovoj mreži te zarazili i pridobili pristup drugim računalima u mreži.

Kako bi se informacijski sustavi i njegovi korisnici što bolje zaštitili važno je proučiti maliciozne programe. Važno je znati kako oni funkcioniraju, kako infiltriraju u sustav i koje su njihove posljedice. U daljnjem tekstu navedeni su najčešći napadački alati i maliciozni programi.

4.3.1. Programi za praćenje unosa znakova s tipkovnice i radne površine računala

Kao što im i ime govori programi za praćenje unosa znakova su programi koji imaju mogućnost praćenja i bilježenja svake aktivnosti korisnikovog unošenja znakova s tipkovnice i općenito rada na računalu u cilju krađe korisničkih podataka poput lozinki, pinova, brojeva kartica i sl.. Često se još nazivaju keyloggeri. Prema načinu implementacije na računalo, dijele se u dvije skupine:

- Fizički uređaji koji se implementiraju u sklopovlje računala
- Programski alati

Fizički uređaj za praćenje je veoma malih dimenzija, izgledom je sličan adapteru u koji se s jedne strane spaja tipkovnica, a s druge strane se on spaja u računalo (slika 8). Uređaj funkcionira tako da bilježi svaki pritisak tipke na tipkovnici i zabilježeni podatak sprema u svoju memoriju. Podaci se tada najčešće bežičnim putem šalju na računalo napadača. Vrlo rijetko je korišten zbog nepraktičnosti.

Slika 8. Fizički keylogger *(prema:*http://www.geekandblogger.com/detect-keylogger-software/)

Današnji programi za praćenje unosa s tipkovnice su softverskog oblika, odnosno u obliku programskih paketa koji su lako dostupni i moguće ih je besplatno preuzeti s raznih stranica. Programski tipovi programa za praćenje unosa s tipkovnice su sveobuhvatniji od fizičkih jer pri instalaciji ima mogućnost samo konfiguriranja unutar operacijskog sustava. Zadatak mu je presretanje podataka o svakom pojedinom unosu znaka s tipkovnice. Te podatke sprema u određeni, sakriveni dio memorije na računalu. Ovo je programski proces koji radi u pozadini, te ga je moguće konfigurirati tako da je u potpunosti nevidljiv korisniku. Podaci se napadaču šalju automatizmom bez znanja korisnika.

Ovo su dosta kompleksni programi kojima je najveći nedostatak bilježenje svih podataka koje korisnik unosi. Zbog toga napadač prima jako velike količine podatak od kojih neki možda i nisu bitni. Iz ovog razloga se uz programe za praćenje unosa s tipkovnice koriste i dodatni programi koji filtriraju dobivene podatke po unaprijed postavljenim kriterijima.

4.3.2. Virusi

Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala na način da bez dopuštenja ili znanja samog korisnika računala kopira samog sebe u

datotečni sustav ili memoriju ciljanog računalnog sustava.[9] Glavno svojstvo virusa je da se on sam širi sa jednog računala na drugo prenošenjem koda preko elektroničke pošte ili prijenosnih medija za pohranu podataka. Mogućnost zaraze virusom je još veća u slučaju da se datoteka zaražena virusom nalazi na poslužitelju.

Računalni virusi se najčešće vežu za izvršne datoteka programa i pokretanjem te datoteke pokreće se i kod virusa. Nakon instalacije datoteke virus infiltrira u servise računala i dalje nastavlja zadaću za koju je predviđen.

4.3.2.1. Osnovne vrste virusa

Postoje tri osnovne vrste virusa:

- Boot sektor virusi - kod virusa se kopira u master boot sektor i na taj način osigurava pokretanje koda pri svakom startu računala
- Programski virusi - aktivira se izvršavanjem zaražene izvršne datoteke
- Makro virusi - napisani višim programskim makro jezikom i imaju mogućnost da se samostalno kopiraju, brišu ili mijenjaju

4.3.3. Trojanski konj

Trojanski konj je maliciozni program koji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju.[10]Naziv trojanski konj nastao je po poznatoj priči o osvajanju grada Troje zloupotrebom povjerenja.

Trojanski konj funkcionira na načina da se lažno predstavlja korisniku kao neki korisni program. Kada korisnik po prvi puta pokrene instalacijsku datoteku tog programa radi instalacije pokreće se i maliciozni dio tog programa te se integrira u operacijski sustav računala. Od ovog trenutka napadač ima pristup računalu.

Trojanski konj izmjenjuje postavke na našem računalu u svrhu dobivanja potpune kontrole nad računalom. Tada je u mogućnosti ukrasti povjerljive informacije, slati ili

[9]http://www.cert.hr/malver/virusi, 02.10.20016.

[10]http://www.cert.hr/malver/trojanski_konji, 02.10.2016.

mijenjati povjerljive informacije, špijunirati aktivnosti korisnika, bilježiti utipkane sadržaje od strane korisnika itd.

Postoji nekoliko načina na koji se trojanski konj širi. To su:

- Preuzimanje zaraženog programa
- Putem elektroničke pošte
- Putem zloćudnih dinamičkih stranica
- Preko prenosivih medija za spremanje podataka

Naravno da postoje programi koji pomažu u borbi protiv trojanskog konja, ali oni su uspješni samo u borbi protiv zaraze. Ako je računalo već prije bilo zaraženo oni nam nažalost neće biti od velike koristi jer ne mogu otkriti sve promjene koje je trojanski konj učinio u sustavu.

4.3.4. Otimanje sjednice

Krađa sjednice je napadačka tehnika kojom se otima identitet drugog korisnika pri čemu je napadačeva namjera saznati identifikator koji je dodijeljen korisniku od strane poslužitelja kako bi iskoristio korisnikove privilegije za nezakonite radnje. To je izravna prijetnja koja može dovesti do otkrivanja povjerljivih informacija.

Svaki puta kada se koristimo nekim poslužiteljem on nas mora označiti nekim identifikatorom. Taj identifikator se nama prikazuje u obliku kolačića. Kolačićje znakovni niz koji se čuva u memoriji preglednika, a postavlja se od strane web aplikacije. On ima svoj životni vijek kojim je točno određeno koliko vremena određeni korisnik može koristiti usluge web aplikacije. Napadačev cilj je saznati korisnikov identifikator i poslužiti se njime kako bi dobio pristup korisnikovim podacima. Ovim putem omogućuje se krađa povjerljivih informacija, ali i nezakonite radnje koristeći korisnikove privilegije.

4.3.5. Phishing

Phishing je vrsta manipulacije kojom se koriste napadači kako bi došli do korisnikovi povjerljivih podataka. Napadač koristeći lažne poruke od korisnika pokušava dobiti informacije poput lozinki, pinova i brojeva bankovnih kartica. Najčešći oblik phishinga je preko lažnih poruka koje se šalju korisnicima. Te poruke sadržavaju poveznicu na neke

stranice zloćudnih poslužitelje. Lažne stranice su najčešće imitacija nekih pravovaljanih stranica (u najviše slučajeva stranice Internet bankarstva) te nas zahtijevaju naše korisničke podatke za pristup. Kada unesemo podatke u najviše slučajeva nam pokazuje grešku.

Postoji nekoliko metoda phishinga, a najkorištenije su:[11]

- **jednostavni zahtjev** koji najčešće dolaze elektroničkom poštom. Napadač se predstavlja kao administrator nekog sustava i moli korisnika da odgovorom na e-mail pošalje svoje korisničke podatke u sklopu nadogradnje sustava i sl.
- **lažni linkovi u e-mail porukama** koji vode korisnika na zloćudnu Web stranicu gdje se traži da upiše svoje korisničko ime i lozinku ili druge osjetljive podatke
- **lažna web sjedišta** korisnik može biti naveden kliknuti na poveznicu koji ga vodi na web poslužitelj koji korištenjem skripti, izmijeni/prekrije stvarnu adresu svog Web sjedišta i postavi legitimnu, čime obmanjuju korisnika koji misli da je na legalnoj stranici i na taj način skupljaju podatke dok ih ovaj unosi
- **lažni prozor na legitimnim web sjedištima banaka** "iskakanje" lažnog prozora sa poljima za unos povjerljivih informacija. "Popup" prozor se pojavljuje pri posjetu legitimnom web poslužitelju
- **„tabnabbing“** – jedna od novijih metoda koja koristi činjenicu da korisnici Web preglednika obično imaju otvoreno nekoliko tabova istovremeno te se jedan od neaktivnih tabova osvježi, ali sa zloćudnim sadržajem koji imitira neku legitimnu Web stranicu (računa se na nepažnju korisnika, odnosno da ne primijeti novu adresu)

4.3.6. Pharming

Iako je sličan phishingu, pharming je mnogo sofisticiranija prevara. U njegovom slučaju ne morate niti odgovarati na elektroničku poštu već samom otvaranjem pošte računalo je zaraženo. Pharming nakon otvaranja maila dopušta zarazu računala virusom ili trojanskim konjem te tada može početi krađa podataka sa računala.

Princip rada nakon zaraze je isti kao i kod phishinga. Kada se korisnik pokušava prijaviti na neke stranice npr. Internet bankarstvo virus ga prosljeđuje na lažnu stranicu (imitaciju prave) gdje korisnik unosi svoje podatke.

[11]http://www.cert.hr/phishing, 02.10.2016.

4.3.7. Distribuirani napadi uskraćivanjem usluge (DDoS)

Distribuirani napadi uskraćivanjem usluge su napadi kada više kompromitiranih sustava preplavljuje sustave nekog ciljanog sustava. Napadač se koristi sustavima koje je otprije zarazio npr. trojanskim konjem i na taj način ima ovlasti nad njima.

Napad počinje tako da napadač prvo mora zaraziti jedan sustav koji će mu biti glavni u napadu, zatim pomoću trojanskog konja širi zarazu na mnoge druge sustave kako bi preuzeo kontrolu nad njima. Sljedeći korak je slanje velikih količina paketa na ciljano računalo dok promet prema i od tog računala ne postane toliko spor da se uskrati usluga. Kao što se može primijetiti ova vrsta napada je zapravo napad na mrežnu uslugu korisnika.

Detaljan opis DDoS napada prema Šafar (2012:54):

> *„Da bi pokrenuo DDoS napad, zlonamjerni korisnik prvo mora izgraditi mrežu računala koja će se koristiti za stvaranje velikog prometa koji je potreban da bi se onemogućila usluga legitimnim korisnicima. Da bi stvorili ovu mrežu, napadači otkrivaju ranjive aplikacije ili poslužitelje. Ranjivi poslužitelji su oni koji sadrže operacijske sustave i sistemske programe s poznatim ranjivostima, ne sadrže antivirusne programe, sadrže antivirusne programe starijih inačica ili oni koji nisu ispravno konfigurirani. Napadači iskorištavaju takve ranjivosti poslužitelja kako bi dobili pristup. Sljedeći korak napadača je instaliranje novih programa (alati za izvršavanje napada) na ugrožene poslužitelje. Poslužitelji u kojima su pokrenuti takvi alati za izvršavanje napada nazivaju se zombi računala, a mogu obaviti svaki napad koji im naredi napadač. Mnogo zombi računala naziva se vojska zombija.*
>
> *Napad počinje probijanjem u slabo osigurana računala, koristeći poznate greške u standardnim mrežnim uslužnim programima te slabu konfiguraciju u operacijskim sustavima. Na svakom sustavu, nakon provale, napadač obavlja neke dodatne korake. Prvi korak je instaliranje programa kako bi se prikrila provala u sustav te kako bi se sakrili svi tragovi njegovih naknadnih aktivnosti. Na primjer, standardne naredbe za prikazivanje procesa koji su pokrenuti su zamijenjeni inačicom koja ne prikazuje procese napadača. Svi ti alati imaju zajednički naziv „rootkit“, jer nakon instalacije preuzimaju administratorske ovlasti. Tada se instalira poseban proces koji se koristi za udaljenu kontrolu računala. Ovaj proces prima naredbe preko Interneta i kao odgovor na ove naredbe pokreće napad putem Interneta prema određenoj žrtvi.*

Rezultat ovoga automatiziranog procesa je stvaranje mreže koja se sastoji od rukovoditeljskih i posredničkih strojeva. Svaki napadač mora raditi s adrese koja se najčešće ipak može povezati s njegovim identitetom. Stoga će oprezni napadač početi razbijanje sa samo nekoliko računala, a zatim ih koristiti za razbijanje više novih računala te ponavljanjem ovog ciklusa smanjiti mogućnost da bude otkriven. Vrijeme napada za napadača traje samo jednu naredbu koja pokreće pakete naredbi da svi zarobljeni strojevi pokrenu određeni napad na određeni cilj. Također, i kada napadač odluči prekinuti napad on treba poslati samo jednu naredbu.“

5. Zaštita informacijskih sustava

5.1. Fizičke metode zaštite

Fizičke metode zaštite jedna su od ključnih komponenti u cjelokupnoj zaštiti informacijskog sustava. Fizička sigurnost informacijskog sustava ugrožava se u slučajevima elementarnih nepogoda te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara.[12] Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj.

Cilj fizičke sigurnosti je spriječiti neautorizirane pristupe računalnom sustavu, zaštititi integritet podataka koji se pohranjuju na računalo, spriječiti oštećenje ili gubitak podataka u slučaju raznih nepogoda te spriječiti krađu podataka s računalnih sustava.

5.1.1. Zaštita okoline

Fizička zaštita okoline informacijskog sustava objedinjuje sve mjere i metode potrebne za zaštitu od utjecaja nepovoljnih vanjskih čimbenika na informacijski sustav. Kod zaštite okoline informacijskog sustava prvenstveno se misli na okolinu organizacije.

Tako su prva mjera postavljanje ograde oko objekta koji je u vlasništvu organizacije. Ponekad se postavljaju i zidovi jer oni smanjuju i vidljivost na područje organizacije. Na ovaj način se sprječava prilazak osoba objektu te zahtjeva najava.

Sljedeći element koji je potrebno osigurati su ulazi i izlazi. To uključuje:

- Postavljanje lokota
- Postavljanje zaštitara
- Postavljenje kamera
- Postavljanje alarmnih sustava

[12]http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf

5.1.2. Zaštita opreme

Zaštita opreme smatra se najvažnijim aspektom fizičke zaštite informacijskog sustava. Svaki uređaj se vrednuje po svojim karakteristikama i namjeni stoga je razina zaštite različita za različiti uređaj ili opremu. Većinom ta zaštita podrazumijeva samo zaštitu osobnog računala ili zaštitu poslužitelja. Razlog tome je jer ovi uređaji sadrže najviše podataka, no potrebno je obratiti pozornost i na ostale uređaje i opremu. Primjerice odlagati prijenosne medije s informacijama na sigurno mjesto, smještaj uređaja na sigurna mjesta, uništavanje starih medija na pravilan i siguran način, zaključavanje uređaja i sl.

Poslužitelji predstavljaju važan aspekt za poslovanje svake organizacije stoga je njihova sigurnost jako bitna. Oni sadržavaju važne informacije i koriste se svakodnevno. Stoga prvi način zaštite poslužitelje je da se jedan poslužitelj ne koristi za svakodnevne poslove nego da se svakodnevni poslovi odvoje od poslužitelja. Drugi način osiguranja poslužitelja je smještanje u posebne odvojene prostorije kojima će se kontrolirati pristup. Također treba osigurati i pravilno smještanje unutar tih prostorija kako bi se spriječilo pomicanje poslužitelja unutar prostorije u slučaju elementarnih nepogoda poput potresa.

Osnovni način zaštite osobnih računala je educiranje zaposlenika. Ako zaposlenik pravilno i sigurno koristi računalo smanjuje se rizik od raznih prijetnji. Važno je definirati pravila u obliku sigurnosne politike koja će definirati pravilno korištenje osobnih računala kao i postupanje u slučaju kvara ili nezgode. Također treba definirati i zaštitu od krađe, špijunaže i drugih ljudskih prijetnji. Načini na koje se možemo zaštititi od kraše su postavljanje kabela za zaključavanje ili instalacijom sustava za praćenje na računalo. Kako bi se zaštitili od zlonamjernog rukovanja računalom potrebno je zaključati računalo kada se ne koristi. Također važan aspekt sigurnosti osobnih računala je smještaj unutar radnog prostora. Računala trebaju biti smještena tako da niti jedan zaposlenik nema pristup podacima drugog zaposlenika.

5.1.3. Kontrola pristupa

Kontrola pristupa ima veliku važnost kada je riječ o fizičkoj zaštiti informacija. Karakterizira je ograničenje pristupa određenim prostorima i računalnim resursima unutar sustava. Fizička kontrola pristupa se najčešće ostvaruje pomoću drugih osoba (zaštitara, stražara ili

recepcionara), putem mehaničkih sredstava (lokoti, brave) ili tehnološkim sredstvima. Kontrola pristupa nije ista za zaposlenike i korisnike u organizaciji stoga se za svakog posebno određuje koje su im ovlasti. Najčešće se na samom ulazu u objekt identificiraju korisnici i posjetitelji kako bi se umanjila mogućnost zlouporabe pristupa unutrašnjosti objekta ili nekim dijelovima informacijskih sustava. Postoje mnogi načini na koje se provodi kontrola pristupa. Ovisno o razini moguće prijetnje i vrijednosti uređaja i informacija formira se adekvatna kontrola pristupa uz pomoć raznih elemenata za postizanje fizičke sigurnosti, poput:

- Posebnih magnetnih kartica
- Nadzora infracrvenim kamerama
- Identifikacije skeniranjem otiska prsta ili šarenice oka
- Identifikacije prepoznavanjem glasa
- Alarmnih sustava

Posebne megnetke

5.2. Programske metode zaštite

5.2.1. Zaštita na razini operacijskog sustava

Zaštita na razini operacijskog sustava je osnovni stupanj zaštite. On uključuje administratore sustava i korisnike tj. zaposlenike u organizaciji. Administrator sustava ima pristup svim povlaštenim informacijama te dodjeljuje razinu ovlasti pojedinim korisnicima. Administrator svakom korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi imao pristup relevantnim informacijama i kako bi obavljao svoje radne zadatke. Svako računalo može imati više administratora te više korisnika.

Same lozinke ujedno mogu biti i slaba točka zaštite sustava, ali zbog ljudskog faktora. Ovo su osnovne greške koje ljudi rade u vezi s lozinkama:

- Koriste se jednostavne ili slabe lozinke
- Ista lozinka se korisni na više računa
- Lozinke se pohranjuju na računala
- Lozinke se zapisuju na papiriće
- Lozinke se dijele sa drugim korisnicima

Kako bi spriječili ove pogreške, a s time i pad sigurnosti informacijskog sustava postoji nekoliko pravila za lozinke:

- Maksimalni vijek trajanja lozinke
- Minimalna duljina lozinke
- Potreba kompleksnosti
- Pregled povijesti lozinki

Maksimalni vijek trajanja lozinke određuje da se lozinka mora mijenjati nakon određenog vremena. Minimalna duljina zahtijeva da lozinka ne bude kraća od zadanog broja znakova. Potreba kompleksnosti zahtjeva da se koristi kombinacija malih i velikih slova, brojeva i posebnih znakova, dok pregled povijesti lozinki onemogućava da postavimo istu lozinku, nego zahtjeva njenu izmjenu. Pridržavanjem ova četiri pravila osigurat ćemo sigurnost korisničkih podataka, a time i informacijskog sustava.

5.2.2. Zaštita na razini korisničkih programa

Sljedeći korak u zaštiti informacijskih sustava je zaštita korisničkih programa. Nakon što pomoću korisničkog imena i lozinke uđemo u sustav tj. radnu površinu, pokreće se program kojim se obavlja određena aktivnost u informacijskom sustavu. Korisnički programi se štite na način da se pojedinim korisnicima dodaju ovlasti te ako određuju funkcije koje mogu obavljati u programu. Postoje tri razine ovlasti:

- Prva razina - samo čitanje iz baze podataka
- Druga razina - izmjena postojećih podataka u bazi i dodavanje novih podataka
- Treća razina - brisanje podataka iz baze

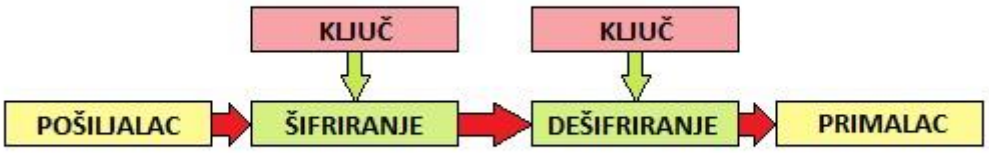
Kako bi se organizacija zaštitila od zlonamjernog korištenja ovlasti radnika postoji još jedan korak povećanju sigurnosti informacijskog sustava. Naime, svi podaci koji se mijenjaju ili brišu spremaju se u posebne direktorije u sustavu kojima pristup ima samo administrator. Tek kada on odluči da podaci nisu potrebni oni se trajno brišu iz sustava.

5.2.3. Kriptografija

Kako organizacije danas nisu centralizirane nego su prostorno dislocirane javlja se potreba za umrežavanjem računala kako bi se informacije mogle svugdje koristiti. Komunikacija između lokacija se odvija preko interneta, a to donosi nove prijetnje. U ovom

procesu mora se osigurati jednoznačnost prijenosa i onemogućiti neautorizirano korištenje ili promjena podataka. Kako bi se omogućila sigurna komunikacija i promet podacima koristi se kriptiranje podataka tj. kriptografija. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.[13]

Kriptiranje funkcionira tako da pošiljalac šifrira podatke pomoću unaprijed dogovorenog ključa te ih onda šalje preko komunikacijskog kanala. Primalac zatim pomoću tog istog ključa dešifrira dobivene podatke kako bi dobio izvorni podatak. Za nekoga tko prisluškuje kanal ti podaci ne znače ništa bez ključa jer vidi samo šifru ne originalni podatak. Princip funkcioniranja možemo vidjeti na slici 9.



Slika 9. Kriptografija

5.2.4. Antispyware

Kako bi shvatili što je antispyware prvo ćemo definirati spyware. Spyware je široka kategorija malicioznih programa, to su najčešće špijunski programi koji pokušavaju zaraziti korisnikovo računalo kako bi sa njega uzeli što više privatnih i povjerljivih informacija te ih proslijedili nekoj drugoj strani (napadač).

Antispyware su programski alati koji pomažu pri blokiranju infekcija od spywarea ili bilo kakove druge vrste malicioznih programa. Oni prate dolazni podatkovni promet poput elektroničke pošte, web stranica, spremljenih datoteka i sprječavaju infekciju računala spyware programima.

[13]https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, 01.10.2016.

Važno je napomenuti da se antispyware alati jako često ažuriraju od strane proizvođača kako bi bili u mogućnosti zaštititi sustav od najnovijih spyware programa.

5.2.5. Antivirus

Antivirusni program je softverski alat koji je dizajniran za zaštitu računala i računalne mreže od računalnih virusa. Antivirus pregledava dolazni podatkovni promet i skenira sadržaj. U slučaju da primijeti prisutnost virusa odmah reagira upozoravajući korisnika te čeka upute za daljnje radnje. Nakon otkrivanja virusa korisnik može zaraženu datoteku izbrisati, prebaciti u karantenu ili ignorirati upozorenje.

Antivirusni program funkcionira tako da uspoređuje dijelove koda dolaznog prometa tj. podataka sa kodovima svih poznatih virusa iz njegove baze podataka. Svaki virus ima specifičan dio koda koji se u bazi podataka virusa naziva potpis.

Osim praćenja dolaznog promete antivirusni program provjerava i sve datoteke koje korisnik otvara. Iako se otvaranje datoteka čini trenutačno ono to nije. Prije otvaranja datoteke antivirusni program uspoređuje njen kod sa potpisima virusa u bazi podataka. U slučaju da se dio koda poklopi sa potpisom virusa izdaje upozorenje korisniku.

Osim običnih i izvršnih datoteka antivirusni program provjerava i komprimirane datoteke jer je virus možda pohranjen u njima te word dokumente za mikro viruse. Također antivirusni programi imaju funkciju heurističkog skeniranja, što znači da osim uspoređivanja potpisa s bazom potpisa virusa oni provjeravaju programe po ponašanju, jer ako se program čudno ponaša postoji mogućnost zaraze.

Antivirusni programi se ažuriraju na dnevnoj bazi pa je važno omogućiti ažuriranja na računalu kako bi ono bilo zaštićeno od najnovijih virusa. On je barijera između korisnikove sigurne privatne mreže i nesigurnih mreža poput interneta.

5.2.6. Zaštitni zid

Zaštitni zid je mrežni sigurnosni sistem koji kontrolira dolazni i odlazni promet po određenim sigurnosnim pravilima. Prema tim pravilima odlučuje dali će dopustiti podatkovni promet ili ga blokirati. On može biti softverskog ili hardverskog tipa.

Zaštitni zid sprječava neželjen pristupa korisnikovom računalu na način da identificira i sprječava komunikaciju preko riskantnih portova. Portovi su komunikacijski kanali po kojima računalo komunicira sa vanjskim mrežama. Računala komuniciraju preko mnogo poznatih portova i zaštitni zid dopušta tu komunikaciju bez korisnikovog znanja. Npr. Internet stranice se otvaraju preko porta 80. Drugim riječima zadaće zaštitnog zida je identifikacija i blokiranje prometa po nesigurnim komunikacijskim kanalima.

Osim otkrivanja sigurnih komunikacijskih kanala zaštitni zid može otkriti čudna ponašanja u dolaznom prometu. Napadači se znaju koristiti sigurnim kanalima kako bi skenirali ranjive portove na korisnikovom računalu. Taj proces ima svoj uzorak koji zaštitni zid prepoznaje i odmah blokira komunikaciju.

5.3. Organizacijske mjere zaštite

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu.[14]

Postoji nekoliko razina informacijske sigurnosti. To su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te outsourcing. Svima njima je cilj zaštita informacijskog sustava.

[14]Šehanović, J., Hutinski Ž., Žugaj M., Informatika za ekonomiste, Tiskara Varteks, 2002, str.237

5.3.1. Infrastruktura informacijske sigurnosti

Zadaća infrastrukture informacijske sigurnosti je upravljati informacijskom sigurnošću unutar organizacije.

Infrastruktura informacijske sigurnosti može se podijeliti na[15]:

- Tim za upravljanje informacijskom sigurnošću
- Koordinacija rada informacijske sigurnosti
- Dodjela odgovornosti za informacijsku sigurnost
- Proces autorizacije organizacijskih cjelina koje sudjeluju u obradi
- Savjeti specijalista o informacijskoj sigurnosti
- Suradnja između organizacija
- Neovisni pregledi efikasnosti informacijske sigurnosti

Svi članovi tima moraju se brinuti za sigurnost informacijskog sustava. U organizacijama se čak i osnivaju timovi koji su odgovorni za vođenje brige o sigurnosti informacijskog sustava. Na taj način se svakodnevno poslovanje odvija puno brže. Najčešće se odabire jedna osoba (menadžer) koji kontrolira tim i vodi zabilješke o svim incidentima, odobrava nove politike sigurnosti te prati promjene koje mogu prijetiti sigurnosti informacijskog sustava.

Formiranje ovakvih timova s jednim menadžerem na čelu olakšava komunikaciju na razini cijele organizacije, jer se formiraju i timovi menadžera raznih odijela. Oni analiziraju sve incidente, koordiniraju inicijative i donose nove sigurnosne politike koje poboljšavaju sigurnost informacijskog sustava na razini cijele organizacije.

5.3.2. Sigurnost pristupa

Zbog normalnog funkcioniranja organizacije potrebno je zaposliti i treće strane. U ovom slučaju to podrazumijeva čistače, zaštitare, dobavljače, privremene zaposlenike itd. S njima valja ugovoriti mehanizme kontrole kako bi se održala sigurnost informacijskih sustava. Ta sigurnost će se održati kontrolom pristupa treće strane tako da će oni imati dozvoljen pristup samo prostorima koji su im potrebni za obavljanje njihovih dužnosti.

[15]https://www.scribd.com/doc/17094401/50/Kontrola-pristupa, 28.07.2016.

Postoje dvije vrste pristupa:

- Fizički pristup
- Logički pristup

Fizički pristup omogućuje trećoj strani pristup prostorijama i objektima organizacije dok logički pristup omogućuje pristup bazama podataka.

Kao sredstvo za fizičku kontrolu pristupa danas se koriste pametne kartice. Svakom zaposleniku ili vanjskom djelatniku se izdaje pametna kartica koja u svojem sklopovlju sadrži podatke sa ovlastima te osobe. Kada se ulazi u prostoriju ona se mora provući kroz skener koji čita te podatke i prema tome odlučuje može li ta osoba ući ili ne. Podaci o osobi se tog trenutka sa skenera šalju u bazu podataka kako bi se kasnije ako je potrebno moglo vidjeti tko je i kada ušao u prostorije. Također pametne kartice mogu služiti i za pristup računalima, ako korisnik za to ima ovlasti. U tom slučaju su korisnički podaci spremljeni na sklopovlju kartice.

Logički pristup se kontrolira izdavanjem korisničkih računa od strane administratora sustava. Administrator daje ovlasti korisniku i prema njima on ima samo mogućnost čitanja, dodavanja i izmjene podataka ili i brisanja podataka.

5.3.3. Outsourcing

Outsourcing možemo definirati kao korištenje vanjskih poduzeća i pojedinaca za obavljanje pojedinog posla.[16] Sukladno tome, cilj organizacije je održati sigurnost informacija u slučaju kada je njihova obrada povjerena nekoj drugoj organizaciji.

Iako se u ovom slučaju obrada informacija neće odvijati u našem poduzeću i dalje treba osigurati njihovu sigurnost. Važno je neku vrstu ugovora s outsourcing poduzećem kojim se provode kontrolni mehanizmi, procjena rizika i sigurnosni postupci kako bi se spriječilo neovlašteno korištenje informacija u organizaciji. Ugovorom o outsourcingu zadani su određeni

[16]http://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/, 28.07.2016.

uvjeti odnosno zahtjevi kojih se treba držati prilikom obavljanja određenog posla za organizaciju. Stavke koje takav ugovor može sadržavati su[17]:

- Načini kojim se udovoljava zakonskim rješenjima
- Vrste sporazuma koji se ugovaraju kako bi obje strane bile svjesne svojih sigurnosnih odgovornosti
- Načini na koje se provjerava i održava integritet te povjerljivost poslovne imovine
- Fizičke i logičke kontrole kojima se organizacija koristi kako bi ograničila pristup informacijama koje su dostupne samo ovlaštenim korisnicima
- Načini dostupnosti podataka u slučaju katastrofe
- Razina fizičke sigurnosti primjenjiva na opremu danu u outsourcingu
- Pravo na nadzor

Osnovna prednost outsourcinga je da se organizacija može usredotočiti na svoju osnovnu aktivnost i razvoj poslovnih procesa, jer su sporedni poslovi dani drugoj organizaciji koja obavlja to za njih.

[17]https://www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava, 28.07.2016

6. Zakonski aspekti sigurnosti informacijskih sustava

Kako je područje informacijske sigurnosti jako široko postoje zakonski aspekti kojih se organizacije moraju pridržavati. Također postoje i institucije koje prate da se ti zakoni uredno provode. U ovom poglavlju reći ću nešto o institucijama informacijske sigurnosti u Republici Hrvatskoj, te o samoj zakonskoj regulativi vezanoj za informacijsku sigurnost.

6.1. Institucije informacijske sigurnosti u RH

Uz mnogobrojne zakone za informacijsku sigurnost u RH postoje i institucije koje provode te zakone. Nabrojati ćemo o objasniti područje djelovanja četiri glavne institucije na području informacijske sigurnosti. To su:

- Nacionalni CERT
- Ured vijeća za nacionalnu sigurnost
- Zavod za sigurnost informacijskih sustava
- Agencija za zaštitu osobnih podataka

6.1.1. Nacionalni CERT

Nacionalni CERT osnovan je u skladu 2009. godine u skladu sa Zakonom o nacionalnoj sigurnosti. Zadaća mu je obrada incidenata na internetu, ali samo ako se jedna od strana nalazi u Hrvatskoj.

U okviru svog djelovanja Nacionalni CERT provodi proaktivne i reaktivne mjere. Proaktivne mjere su one kojima Nacionalni CERT djeluje prije događanja incidenta u svrhu njegovog sprječavanja ili ublažavanja. To su[18]:

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti
- kontinuirano praćenje računalno-sigurnosnih tehnologija
- javno objavljivanje novih informacija u svrhu edukacije najšire javnosti
- provođenje detaljne edukativne obuke za specifične grupe korisnika

Reaktivne mjere su one kojima se djeluje na incident. To su[19]:

[18]http://www.cert.hr/onama, 15.10.2016.

- izrada se i distribucija sigurnosnih upozorenjana osnovu prikupljenih saznanja,
- prikupljanje, obrada i priprema sigurnosnih preporuka o slabostima u informacijskim sustavima
- koordinacija rješavanja značajnijih Incidenata u koje je uključena barem jedna strana iz Republike Hrvatske

Valja napomenuti da Nacionalni CERT iako je nadležan za sigurnost i zaštitu od incidenata nije nadležan za kažnjavanje i pokretanje kaznenih prijava. Nakon otkrivanja incidenta prijavu podnosi nadležnim tijelima u RH.

6.1.2. Ured vijeća za nacionalnu sigurnost

Ured vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost, koji koordinira, usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj.[20] Zadaća ureda vijeća za nacionalnu sigurnost je[21]:

- osigurava i nadzire uvođenje mjera i standarda za zaštitu klasificiranih podataka,
- koordinira i usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje
- akreditira sastavnice Sustava registara RH za razmjenu međunarodnih klasificiranih podataka te izdaje certifikate za fizičke i pravne osobe za pristup nacionalnim, NATO i EU klasificiranim podacima

[19]http://www.cert.hr/onama, 15.10.2016.

[20]http://www.uvns.hr/hr/hr/o-nama/uvodna-rijec, 15.10.2016.

[21]http://www.uvns.hr/hr/koje-tijelo-je-odgovorno-za-koordinaciju-nacionalne-i-medjunarodne-sigurnosne-politike, 15.10.2016.

6.1.3. Zavod za sigurnost informacijskih sustava (ZSIS)

Zavod za sigurnost informacijskih sustava je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Oni obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kripto materijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.[22]

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

Zavod za sigurnost informacijskih sustava zadužen je za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima i njihovo trajno usklađivanje s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.

6.1.4. Agencija za zaštitu osobnih podataka

„Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o zaštiti osobnih podataka.

Zaštita osobnih podataka u Republici Hrvatskoj te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj uređuje se Zakonom o zaštiti osobnih podataka.

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Glavni zadaci Agencije za zaštitu osobnih podataka su učinkovito djelovanje na ispunjavanje svih prava i obaveza iz područja zaštite osobnih podataka koje se Republici Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe, povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka vezano za primjenu propisa koji su obuhvaćeni zakonskim okvirom zaštite osobnih podataka u Republici Hrvatskoj uz odgovarajuću primjenu mjera informacijske sigurnosti.

[22]https://www.zsis.hr/default.aspx?id=13, 15.10.2016.

Misija Agencije za zaštitu osobnih podataka je uspješno izvršavanje nadzora nad provođenjem propisa o zaštiti osobnih podataka, te omogućavanje ostvarivanja tog prava svakom pojedincu u Republici Hrvatskoj, praćenje razvoja na tom području, te predlaganje mjera za unaprjeđenje zaštite osobnih podataka.''[23]

[23]http://azop.hr/djelatnost-agencije, 15.10.2016.

7. Zaključak

Za uspješan rad svakog poslovnog sustava potrebne su informacije koje moraju biti točne i dostupne u pravo vrijeme. Informacija se danas smatra najbitnijim resursom poslovanja neke organizacije i zbog toga su bitni kvalitetno razvijeni informacijski sustavi.

Svaki informacijski sustav je dio nekog poslovnog sustava i on je taj koji prikuplja, razvrstava, obrađuje, čuva, oblikuje i raspoređuje podatke po jedinicama poslovnog sustava. Kada se spominje informacijski sustav svi obično pomisle na računala i rad s računalima, ali oni ne moraju biti povezani. Podaci su se obrađivali i prije izuma računala u ručnom dobu obrade podataka. Ta ista metoda se i danas ponegdje koristi.

Gledajući na važnost informacijskih sustava i prijetnje prema informacijskom sustavu lako je razumjeti zašto je njegova sigurnost bitna stavka u poslovanju organizacije. Kako bi informacija bila korisna i osigurala rast i dobit poduzeće ona mora imati integritet, biti dostupna i povjerljiva. To su tri aspekta na kojima je zasnovana informacijska sigurnost. Informacijskoj sigurnosti pridaje se još veća važnost kada se u obzir uzmu silne fizičke i programske prijetnje informacijskom sustavu.

Kako bi se osigurala njegova sigurnost od različitih vrsta zloćudnih programa poput virusa, trojanskog konja i programa za praćenje unosa sa tipkovnice, tipova prijevare i računalnih napada postoji nekoliko metoda zaštite informacijskih sustava. Prva od njih je fizička metoda koja regulira fizički pristup dijelovima informacijskog sustava. Sljedeća je programska metoda koja koristi programske alate i metode kako bi se zaštitio informacijski sustav. Tu spadaju razni alati poput antivirusnih i antispyware programa, kriptografija podataka, uvođenje administratora sustava i dodjeljivanje korisničkih podataka i ovlasti korisnicima. Treća metoda je organizacijska i ona govori o komunikaciji i organizaciji samog poslovnog sustava sa svrhom čim lakšeg održavanja sigurnosti informacijskog sustava.

Zbog postojanja raznih regulativa i zakona o sigurnosti informacijskih sustava, moraju postojati i institucije koje osiguravaju sigurnost informacija. To su Nacionalni CERT, koji se bavi prijetnjama samo ako je domena ili IP adresa iz RH, Ured za nacionalnu sigurnost koji je središnje državno tijelo za informacijsku sigurnost u RH, Zavod za sigurnost informacijskih

sustava koji je glavno tijelo za obavljanje poslova u tehničkim područjima u RH te Agencija za zaštitu osobnih podataka koja se isključivo bavi zaštitom podataka građana RH.

Cilj ovoga rada bio je prikazati važnost informacija koje su dostupne u pravo vrijeme imaju integritet i pravovaljane su za organizacije i njihov uspjeh u poslovanju. Također upoznati korisnika sa prijetnjama sigurnosti njegovog računala, a time i privatnih podataka, te uputiti na neke metode zaštite računala.

Literatura

Knjige

1. Antoliš, K.,etal, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010.
2. G. B. Davis, M. H. Olson, Management Information Systems: ConceptualFoundations, StructuraandDevelopment, McGraw- Hill, New York, SAD, 1985
3. Hadjina, N., Zaštita informacijskih sustava. Zagreb: FER, 2009.
4. Klasić, K., Klarin, K., Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009.,
5. Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011.
6. Šehanović, J., Hutinski, Ž., Žugaj, M., Informatika za ekonomiste, Tiskara Varteks, 2002.

Članci

7. Klasić, K. Zaštita informacijskih sustava u poslovnoj praksi.// SIGURNOST, Vol.49 No.1 Travanj 2007.
8. Šafar, L. Sigurnost Web aplikacija (diplomski rad), Zagreb, Prosinac 2012.

Internet

9. http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustava_0.pdf, 26.07.2016.
10. http://www.unizd.hr/portals/1/Primjena_rac/Brodostrojarstvo/predavanje_6.pdf, 29.07.2016.
11. http://croz.net/usluge/sigurnost-informacijskih-sustava/, 03.10.2016.
12. https://www.fer.hr/_download/repository/SkriptaZaStudente2009-12%5B1%5D.pdf, 25.07.2016.
13. http://www.unizd.hr/Portals/1/Primjena_rac/Poseban_program/Predavanja/sigurnost_predavanje.pdf, 25.07.2016.

14. http://autopoiesis.foi.hr/wiki.php?name=KM+-+Tim+55&parent=NULL&page=Obrada%20podataka, 24.07.2016.
15. https://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 23.07.2016.
16. http://www.columbia.edu/cu/computinghistory/census-tabulator.html, 20.07.2016.
17. https://hr.wikipedia.org/wiki/Informacijski_sustavi, 15.07.2016.
18. http://www.cert.hr/onama, 15.10.2016.
19. https://www.zsis.hr/, 15.10.2016.
20. http://www.uvns.hr/hr, 15.10.2016.
21. http://azop.hr/, 15.10.2016.
22. http://autopoiesis.foi.hr/wiki.php?name=KM+-+Tim+37&parent=NULL&page=Sigurnost%20informacija, 24.07.2016.
23. https://www.techopedia.com/definition/25830/cia-triad-of-information-security, 09.10.2016.
24. http://documents.tips/documents/1-poslovni-informacijski-sustavi.html, 28.07.2016.
25. https://www.scribd.com/document/99898166/Informacijski-sustavi, 21.07.2016.
26. http://documents.tips/documents/informacijski-sustavi-skripta.html, 10.10.2016
27. http://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/, 28.07.2016.
28. https://www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava, 28.07.2016.
29. https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, 01.10.2016.