SIGURNOSNI ASPEKT INFORMACIJSKIH SUSTAVA

Gudac, Nenad

VELEUČILIŠTE U KARLOVCU
POSLOVNI ODJEL
SPECIJALISTIČKI DIPLOMSKI STRUČNI STUDIJ POSLOVNO UPRAVLJANJE

Nenad Gudac

SIGURNOSNI ASPEKTI INFORMACIJSKOG SUSTAVA

ZAVRŠNI RAD

Karlovac, 2019.

Nenad Gudac

SIGURNOSNI ASPEKTI INFORMACIJSKOG SUSTAVA

ZAVRŠNI RAD

Veleučilište u Karlovcu
Poslovni odjel
Specijalistički diplomski stručni studij Poslovno upravljanje

Kolegij: Informacijski sustavi
Mentor: doc. dr. sc. Ljerka Luić prof. v. š.
Matični broj studenta: 0619412031

Karlovac, ožujak, 2019.

"Ne planirati znači planirati neuspjeh."

—B. Franklin

ZAHVALA

Zahvaljujem profesorima odjela Poslovnog upravljanja na zalaganju i poticajima koje su davali nama studentima, vremenu koje su nam stavili na raspolaganje te susretljivosti i profesionalnosti.

Zahvaljujem posebno mentorici, doc. dr. sc. Ljerki Luić prof. v. š. na dinamičnim i zanimljivim predavanjima te ukazanom vremenu, savjetima, usmjerenju i pomoći tijekom pisanja ovog završnog rada.

Zahvaljujem svojim kolegama na susretljivosti i podršci tijekom mog obrazovanja, kao i svojim roditeljima i supruzi koji su uvijek pokazivali razumijevanje za moje studentske obaveze i poticali me da uvijek ustrajem i vjerujem u sebe i svoje mogućnosti.

SAŽETAK

U suvremeno doba važno je prepoznati značaj informacijskih sustava te iste štititi na prikladan način. Informacijski sustavi omogućuju i pospješuju vođenje i upravljanje poslovnim procesima. Zbog činjenice da informacijski sustavi sadržavaju mnoštvo podataka važnih za poslovanje javlja se problem zaštite istih. Kako bi se odabrale adekvatne mjere i metode zaštite, analizirane su i objašnjene moguće vrste prijetnji, napadačke metode na poslovne informacijske sustave i razne vrste zlonamjernih programa koji mogu narušiti glavne sigurnosne aspekte i uzrokovati značajne posljedice. Spoznajom mogućih prijetnji, utvrđene su i opisane adekvatne metode zaštite.

Ključne riječi: informacijski sustav, zaštita informacijskog sustava, prijetnje, mjere zaštite, upravljanje sigurnošću

SUMMARY

In the contemporary times it is important to notice the significance of information systems and protect them in a convenient way. Information systems are allowing and improving guidance and control of business processes. Due to the fact that information systems contain a variety of information of great importance for business, the problem of security is relevant. Possible kinds of threats, attacking methods on business information systems and various kinds of malicious programs which can violate main safety aspects and cause severe consequence had been analyzed to choose adequate measures and method of protection. With investigation of possible threats, adequate measures of protection have been determinated and decribed.

Keywords: information system, information system security, threats, protective measures, security management

SADRŽAJ

1. UVOD

1.1. Predmet i cilj rada

Suvremena informacijska tehnologija donosi niz prednosti kao što su brzina, točnost, pouzdanost, laka programibilnost, pogodnost obavljanja ponavljajućih poslova jer za razliku od ljudskog rada ona nikad ne griješi. Za uspješno poslovanje svake organizacije ključno je uspostavljanje informacijskog sustava koje će biti efikasan, pouzdan i nadasve siguran. Cilj rada je objasniti informacijski poslovni sustav te analizirati sigurnost takvih informacijskih sustava te prikazati prijetnje vezane za informacijske sustave i informacijsku sigurnost. Kao odgovor na te prijetnje navest će se i mjere zaštite kao način prevencije i obrane od napada na informacijske poslovne sustave.

1.2. Izvori i metode prikupljanja

Kao izvori podataka korišteni su udžbenici, web-mjesta i pravni propisi. Metode prikupljanja podataka korištene pri izradi rada su sljedeće znanstvene metode: metode analize i sinteze, indukcije i dedukcije, metoda deskripcije, klasifikacije, povijesna metoda te metoda kompilacije.

1.3. Sadržaj i struktura rada

Ovaj rad se sastoji od pet cjelina. U prvoj cjelini opisuju se osnove suvremenog informacijskog sustava, osnovni pojmovi, povijest, podjele i vrste. U drugoj cjelini razmatra se važnost informacijske sigurnosti u suvremenom poslovanju, iznose zakoni i institucije bitne za informacijsku sigurnost, te moguće prijetnje informacijskom sustavu. U trećoj cjelini obrađuju se mjere kojima je moguće zaštiti informacijski sustav od napada. U predzadnjoj cjelini iznesene su na praktičnom primjeru mjere i politika zaštite informacijskog sustava. Na kraju je iznesen zaključak.

2. UVOD U SUVREMENI INFORMACIJSKI SUSTAV

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 velika 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.

2.1. Pojmovi informacijskih sustava

Sustav je svaki uređeni skup od najmanje dva elementa koji zajedno interakcijom ostvaruju funkciju cjeline.[1] Cilj svakog sustava je zadani ulaz pretvoriti u određeni izlaz. Ovisno o kojoj se vrsti sustava radi, ta pretvorba ulaza u izlaz odvijati će se djelovanjem različitih procesa u sustavu. Ulaz predstavlja skupljene ili dodijeljene veličine koje ulaze u sustav kako bi bile procesirane, odosno kako bi se obradile da bi se dobio željeni izlaz. Proces u sustavu ili obrada ulaznih veličina predstavlja procese transformacije koji konvertiraju ulaz u izlaz, a izlaz predstavljaju transformirane veličine nastale kao produkt procesa transformacije unutar sustava.

Za razumijevanje tematike ovog rada bitno je nakon definicije sustava odrediti što je to poslovni sustav i što je to informacijski sustav. Poslovni sustav je organizacijski sustav kojeg opisuje skup informacija o prošlosti i sadašnjosti i poslovnih procesa koji ih obrađuju.[2] Poslovni sustav karakteriziraju materijalni ulazi i izlazi te informacijski tokovi pa tako u poslovni sustav ulaze sirovine, dokumenti, poruke, energija, a izlaze dokumenti i proizvodi. Sudionici u procesu pretvorbe ulaza u izlaze mogu biti ljudi kao izvršitelji posla, alati i razni strojevi. Osnova za obavljanje funkcije poslovnog sustava je postojanje informacija. 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] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.13
[2] Ibidem, str.16

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.

Informacijski sustav dio je svakog poslovnog sustava, a njegova uloga je konstantna opskrba potrebnim informacijama na svim razinama upravljanja, odlučivanja i svakodnevnog poslovanja. Svako poduzeće ima određenu djelatnost kojom se bavi pa će tako i izgradnja informacijskog sustava za svako poduzeće biti različita. Informacijski sustavi prilagođavaju se i razvijaju za realni poslovni sustav, a poslovni procesi realnog sustava temelj su za modeliranje strukture njegovog informacijskog sustava. Za svaku djelatnost i uspješno poslovanje najvažnije su komponente prikupljanje, obrada i korištenje podataka, pa poduzeće s dobro izgrađenim informacijskim sustavom uspješnije posluje. S obzirom da je već navedeno kako svako poduzeće razvija vlastiti informacijski sustav ovisno o vidu poslovanja, tako taj isti 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 radnim razinama poslovnog sustava. Ono što je zapravo uloga informacijskog sustava jest proizvesti informaciju na temelju podataka. Podatak je logička cjelina koju primamo osjetilima, a sama za sebe ne mora imati neko značenje. Informacija je skup podataka, a podatak se pretvara u informaciju kada mu je pridruženo neko značenje. 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 u skladu s svojim ovlaštenjima.

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).[3] Razinu izvođenja karakteriziraju procesi osnovne djelatnosti, a cilj informacijskih sustava na toj razini je povećanje produktivnosti rada. Upravljačka razina odgovorna je za organiziranje, praćenje uspješnosti te otklanjanje smetnji, a cilj informacijskih sustava je povećanje učinkovitosti. Cilj informacijskih sustava na razini odlučivanja jest osiguranje stabilnosti rasta i razvoja s obzirom da je ta razina odgovorna za postavljanje poslovnih ciljeva.

[3] http://documents.tips/documents/informacijski-sustavi-skripta.html

2.2. Povijest 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.[4] 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:[5]

- **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.

- **Faza mehaničke obrade podataka**

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.

- **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.

[4] Panian, Ž., Poslovna informatika za ekonomiste, Masmedia, Zagreb, 2005, str. 35.
[5] Ibidem, str. 36

- **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.

2.3. Dijelovi i načela informacijskog sustava

Da bi informacijski sustav ispunio svoje funkcije i zadatke mora biti tako izgrađen i organiziran da posjeduje sve dijelove i elemente koji su zato potrebni, a zajednički čine sređenu strukturu informacijskog sustava. Svaki informacijski sustav sastoji se od šest glavnih dijelova. To su:

1. Materijalno-tehnička komponenta (hardware) koju čine svi uređaji i sredstva namijenjeni isključivo ili pretežito obradi podataka ili informacija
2. Nematerijalna komponenta (software) je ukupnost ljudskoga znanja ugrađenog u strojeve, opremu i uređaje, koja predstavlja predmet obrade ili diktira način obrade u sustavu
3. Ljudska komponenta (lifeware) koju čine informacijski djelatnici koji sudjeluju u radu sustava kao profesionalni informatičari ili korisnici sustava pritom koristeći rezultate obrade podataka, odnosno informacija
4. Organizacijska komponenta (orgware) gdje spadaju organizacijski postupci, metode i načini povezivanja gornje tri komponente u skladnu i funkcionalnu cjelinu
5. Prijenosna komponenta (netware) koju tvore sredstva i veze za prijenos podataka na daljinu, odnosno realizacija komunikacijskog povezivanja elemenata sustava u skladnu cjelovitu informatičku (telekomunikacijsku) mrežu
6. Podatkovna komponenta (dataware) čija je svrha koncepcija i organizacija baza tj. skladišta podataka i svih raspoloživih informacijskih resursa[6]

Gore navedene komponente informacijskog sustava su u međusobnoj interakciji, pri čemu organizacijska komponenta ima ulogu sprege među njima. Za uspješno funkcioniranje informacijskog sustava potrebno je da svi ti dijelovi imaju podjednaku razinu kvalitete i međusobne usklađenosti. Njihovo povezano i međuzavisno djelovanje

[6] Dragičević, D., Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004, str. 18.

tvori jedinstveni proces transformacije ulaza u izlaze, primanja i prerađivanja sirovih podataka, njihovo obrađivanje i memoriranje, te dostavljanje oplemenjenih podataka i informacija zainteresiranim korisnicima. Međutim, u stvarnim sustavima, teško je za očekivati da će se postići potpuna usklađenost svih komponenta s obzirom na njihovu kvalitetu.

S obzirom na način koji informacijski sustavi poslovne procese mogu poduprijeti, informacijske sustave možemo podijeliti na dijelove kako slijedi:[7]

Izvršni dio – podupire izvršne procese u organizaciji. Izvršnim procesima se obavljaju poslovi temeljene djelatnosti organizacije kojima se mijenjaju stanja poslovanja. S obzirom da se bilježenje promjena stanja obavlja transakcijama, taj se dio informacijskog sustava naziva sustavom za obradu transakcija. Tri su funkcije sustava za obradu transakcija: vođenje evidencije, izrada dokumenata i izrada izvještaja.

Upravljački dio – podupire upravljačke procese u organizaciji. Ovaj dio informacijskog sustava se naziva sustavom za potporu upravljanju. On preuzima podatke iz izvršnog dijela informacijskog sustava te podatke iz vanjskih izvora da bi stvorio informacije potrebne upravljanju i odlučivanju. U stvaranju informacija koristi se različitim analitičkim, upravljačkim ili specifičnim obradama ili aplikacijama.

Komunikacijski dio – podupire procese koji omogućuju komunikaciju, suradnju i informiranje među sudionicima poslovanja. Taj se dio naziva sustavom za komunikaciju i suradnju. U funkcioniranju organizacije sudjeluje niz sudionika unutar organizacije (zaposlenici) i izvan nje (klijenti, poslovni partneri, javna administracija) koji međusobno surađuju i komuniciraju.

S obzirom na sastav informacijskih sustava, djelatnost i cilj, mogu se odrediti tri temeljna načela informacijskih sustava:[8]

- načelo efikasnosti,
- načelo ekonomičnosti i
- načelo sigurnosti.

[7] Pejić Bach, M. i dr., Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Zagreb, 2016.
[8] Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004.

Pod načelom efikasnosti se podrazumijeva pravovremenost, dostupnost i valjanost informacija. Za potrebe informacijskog sustava i kvalitetnog odlučivanja, njegovim korisnicima je od uvelike važnosti da informacija koju posjeduju sadrži navedena tri svojstva. Samo takva informacija je korisna informacija ako je korisnik zna upotrijebiti na pravi način i u pravo vrijeme.

Načelo ekonomičnosti nalaže da bi ulaganja u razvoj, održavanje i rad informacijskog sustava trebalo biti u skladu s koristima od čijeg rada imaju njegovi korisnici. S obzirom da informatička tehnologija brzo zastarijeva, a njena ugradnja, održavanje i uporaba je jako skupa prije uvođenja iste potrebno je analizirati i odrediti koje koristi i u kojoj mjeri bi korisnici imali od upotrebe takve tehnologije.

Načelo sigurnosti predstavlja odgovornost za sigurnost informacijskih sustava, te edukacija njihovih korisnika o potencijalnim prijetnjama i mjerama zaštite. Pri tome treba paziti da su mjere zaštite informacijskih sustava usklađene s ostalim mjerama organizacije, te da one neće dovesti do ugroze tuđih prava i interesa kao ni na dostupnost informacija u društvu.

Svako od navedenih načela jednako je važno u ostvarenju navedenih funkcija informacijskog sustava, a o njihovom provođenju ovisi i konačno ispunjenje željenih ciljeva.

2.4. Vrste informacijskih sustava

Mnogo je kriterija za podjelu informacijskih sustava, a oni najčešće korišteni su podjela prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija u poslovnom sustavu.

- **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 1. prikazane su vrste informacijskih sustava prema konceptualnom ustrojstvu poduzeća.

Tablica 1. 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**

Izvor: izrada studenta prema: Klarin, Klasić, 2009, str.23

Prema konceptualnom ustrojstvu poslovodstva transakcijski sustavi su vrsta informacijskih sustava namjenjena operativnoj razini, a njihova uloga je izvođenje procesa osnovne djelatnosti. Primjerice to može biti sustav kojim se evidentiraju pojedini koraci u proizvodnji. Kao rezultat izvršnog informacijskog sustava dobivaju se izvješća nužna za upravljanje i ona se pridružuju taktičkoj razini poslovanja. Informacijski sustav strateške razine poslovanja jest sustav potpore odlučivanju.

- **Informacijski sustavi prema namjeni**

Prema namjeni informacijske sustave možemo podijeliti na četiri podsustava, a to su: sustavi za obradu podataka, sustavi podrške uredskom radu, sustavi podrške u odlučivanju i ekspertni sustavi.[9]

Sustavi obrade podataka koriste se kako bi se unjeli, obradili i pohranili podaci o stanju sustava i poslovnim događajima. Podaci u ovim informacijskim sustavima pohranjuju se u bazama podataka, a do traženih podataka u bazi dolazi se uz pomoć posebnih programa za pretraživanje. Kada se podaci obrade, na temelju njih izrađuju se posebna izvješća čija je svrha pravilno izvođenje procesa osnovne djelatnosti, ali isto tako služe za upravljanje. Sustavi podrške uredskom radu dijele se u dvije kategorije. Razlikujemo sustave za podršku ljudskog komuniciranja za čiju podršku se koriste elektronička pošta, telefoniranje i slično, te drugu vrstu sustava, sustav za podršku u obavljanju administrativnih poslova. Ovaj sustav koristi pomoćni sustav za potporu rada u skupini, prezentacije i sl.

[9] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.23

Kod sustava podrške u odlučivanju primjenjuju se razni modeli odlučivanja pomoću kojih se stvaraju informacije potrebne za odlučivanje, kao podrška pojedincu i grupi.

Kao podrška stručnjacima i ekspertima za rješavanje problema poput konfiguriranja i dijagnosticiranja koriste se ekspertni sustavi. U kategoriju ekspertnih sustava mogu se ubrojati i sustavi podrške posebnim problemskim područjima, a koji se odnose na podršku učenju, podršku znanstvenom i stručnom radu ili podršku projektiranju.

Usporednim prikazom važnijih obilježja različitih vrsta informacijskih sustava prema namjeni dobiti će se slika o složenosti pojedine kategorije. Uzme li se primjerice područje primjene može se primjetiti kako su neki informacijski sustavi složeniji od drugih. Pa su tako obilježja sustava obrade podataka dobro struktuirana problemska područja čiji se procesi mogu strukturalno pratiti. Kod sustava uredskog poslovanja obilježja su dobro strukturirani ponavljajući uredski poslovi, a sustavi podrške odlučivanju obilježeni su djelomičnim strukturiranim procesima donošenja odluka. Najsloženije područje primjene je kod ekspertnih sustava čije su obilježje uska problemska područja za koja su potrebna ekspertna znanja. Skladište podataka i informacija također se razlikuje ovisno o informacijskom sustavu. Sustavi obrade podataka imaju baze podataka organizacijskog sustava, sustavi uredskog poslovanja imaju baze podataka pojedinih programskih pomagala te baze podataka o objektima, sustavi podrške odlučivanju koriste se bazama izdvojenih podataka, bazama vlastitih podataka, bazama podataka sa rezultatima obrada te bazama modela, u konačnici ekspertni sustavi koriste baze znanja. Svaki od četiri informacijska sustava ima i različitu vrstu i oblik izlaznih informacija, pa tako govorimo li o sustavima obrade podataka oni prikazuju informacije putem analitičkih i zbirnih izvješća, izvješća o greškama i porukama, te informacijama o stanjima i promjenama stanja pojedinih objekata. Sustavi uredskog poslovanja izlazne informacije prikazuju sadržajem poruka, dokumenata i ostalih objekata, a prikazuju i informacije o stanjima i promjenama pojedinih objekata uredskog sustava. Složenost u prikazu izlaznih informacija vidi se u sustavima podrške odlučivanju gdje su grafički, numerički i tekstualno prikazane informacije potrebne za donošenje odluka, a informacije su međurezultati obrada. Četvrta vrsta informacijskih sustava, ekspertni sustavi prikazuju izlazne informacije u obliku rezultata ekspertize s objašnjenjima, te ih karakterizira prikaz načina rješavanja problema.

- **Informacijski sustavi prema modelu poslovnih funkcija u poslovnom sustavu**

Treća kategorizacija informacijskih sustava je ona prema modelu poslovnih funkcija u poslovnom sustavu. Kada je riječ o takvoj kategorizaciji informacijskih sustava, oni će biti u tolikom broju koliko se poslovnih funkcija obavlja u poduzeću, dakle ovise o organizaciji poslovanja. Općenito podjela informacijskih sutava prema modelu poslovnih funkcija u poslovnom sustavu je sljedeća:[10]

- 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.

Budući da različiti poslovni sustavi imaju različit značaj primjene informacijske tehnologije, informacijske sustave može se podijeliti na četiri osnovna tipa: operativni informacijski sustav, potporni informacijski sustav, strateški informacijski sustava te izgledni informacijski sustav.

Uspjeh tekućeg poslovanja ponajprije ovisi o operativnom informacijskom sustavu. U takvom sustavu informacijski sustav služi kao potpora svakodnevnom poslu pa samim tim i funkcioniranje poduzeća ovisi o danoj informacijskoj tehnologiji. Primjer gdje se koristi operativni informacijski sustav jest trgovina.

Potporni informacijski sustav nije od velike važnosti za poslovni uspjeh poduzeća ali svakako je koristan. U takvom sustavu vrlo je mala ovisnost informacijske tehnologije, te i

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

bez nje poduzeće funkcionira sasvim solidno. Primjerice u građevinarstvu se koristi potporni informacijski sustav.

Strateški informacijski sustav od velike je važnosti za budućnost poslovanja te za poslovnu strategiju stoga je potrebno da takav sustav omogućava pohranu i brzu obradu velike količine podataka potrebnih za poslovanje.[11] Kada je riječ o takvoj vrsti poslovanja funkcioniranje poduzeća jako ovisi o primjeni informacijske tehnologije, kao i na sami poslovni rezultat poduzeća. Primjer gdje se koriste strateški informacijski sustavi je rezervacija karata za prijevoz putnika.

Izgledni informacijski sustav mogao bi utjecati na uspjeh budućeg poslovanja, pa se može reći da je ovisnost funkcioniranja poduzeća o informacijskoj tehnologiji mala, ali je utjecaj informatike na poslovni rezultat velik. Primjenu ove vrste informacijskog sustava najlakše je prikazati na primjeru osiguratelјske djelatnosti. Dakle osiguratelj može ručno izdati policu osiguranja ili obraditi štetu, ali kada je riječ o raznim izračunima premije osiguranja ili procjene rizika za određene ciljne skupine, tada je potrebno prikupiti i obraditi veliku količinu podataka. Bez korištenja informatike taj proces trajao bi predugo te bi se odrazio na rezultate poslovanja.

U principu svakom poslovnom sustavu odgovara neki informacijski sustav. Najčešće se informacijski sustavi odabiru prema osnovnoj djelatnosti samog poduzeća, jer se na taj način najlakše određuje redoslijed prioriteta pri uvođenju informacijskih sustava. Često je u poduzećima najjednostavnije najprije izgraditi potporni informacijski sustav koji s vremenom, kako raste poduzeće, prerasta u izgledni informacijski sustav. Izgledni informacijski sustav ključan je za dugoročno poslovanje poduzeća.

Budući da su informacijski sustavi dio poslovnog sustava, upravo je pravilno i uspješno integrirani informacijski sustavi jedna od glavnih komponenti čiji je rezultat uspješno poslovanje poduzeća. Da bi informacijski sustav bio uspješan, neovisno o kojoj vrsti ili tipu se radi, potrebno je da takav sustav ima dovoljne količine kvalitetnih, dobro i jednoznačno definiranih podataka koje je potrebno obraditi. Bez tako definiranih podataka nema ni kvalitetne podrške klijentima te rasta i razvoja poduzeća.

Postoji nekoliko načela koja kvalitetan informacijski sustav mora zadovoljiti:[12]

[11] http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf

[12] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.26

- 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

Poduzeće koje ima postavljen informacijski sustav 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. VAŽNOST INFORMACIJSKE SIGURNOSTI U SUVREMENOM POSLOVANJU

U razvoju visoke tehnologije danas u svijetu, organizacije sve više ovise o njihovim informacijskim sustavima. Različite prijetnje informacijskim sustavima kao što su napadi od hakera, krađe identiteta, podataka i sl. zabrinulo je javnost i poslovni svijet te ih prisililo da kao jedan od važnijih aspekata u provedbi svojeg poslovanja bude zaštita i sigurnost informacijskih sustava. Događaji zastrašivanja ukradenim ili nestalim podacima postaju sve češća pojava jer se organizacije uvelike oslanjaju na računala kako bi se pohranile osjetljive informacije vezane za njihovo poslovanje. Organizacije prikupljaju i pohranjuju velike količine informacija o svojim zaposlenicima, klijentima, raznim istraživanjima, proizvodima ili financijskom poslovanju koje se obrađuju, pohranjuju i prenose putem računalnih mreža na druga računala. Zato je jako važno ozbiljno pristupiti zaštiti i sigurnosti informacijskih sustava jer se danas vrijednost nekog poduzeća temelji na vrijednosti njegovih informacija. Dakle, informacija zapravo predstavlja konkurentsku prednost, te ako dođe u pogrešne ruke može dovesti do ugroze poslovanja, mogućih tužbi, krađe identiteta i novčanih sredstava ili čak bankrota.

Sigurnost informacijskih sustava predstavlja skup metoda i načina kojima se informacije i informacijski sustavi štite od neovlaštenog pristupa, uporabe, otkrivanja, prekida rada, promjena ili uništenja.[13] Postoje tri temeljna parametra informacijske sigurnosti:

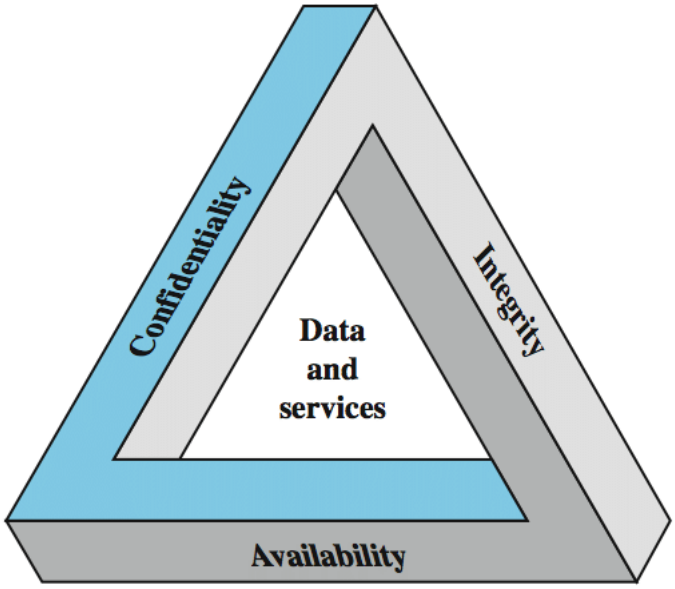
1. Povjerljivost (eng. confidentiality) – siguran pristup informaciji i informacijskome sustavu isključivo za to ovlaštenoj osobi.
2. Integritet (eng. integrity) – zaštita ispravnosti i cjelovitosti podataka i informacija.
3. Raspoloživost (eng. availability) – ovlaštenoj osobi omogućiti pravodoban i stalan pristup informacijama i informacijskome sustavu.

Navedenim parametrima mogu se priključiti i svojstva autentičnosti, neporecivosti, dokazivosti i pouzdanosti, ali mnogi autori smatraju da su ta svojstva već sadržana u osnovna tri parametra te nema potrebe za njihovim posebnim opisivanjem.

[13] Pejić Bach, M. i dr., (2016.), Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Zagreb str. 245.

Na sljedećoj slici je prikazan tzv. sigurnosni trokut (CIA triad) koji prikazuje povezanost gore navedena tri parametra.[14]

Slika 1. Sigurnosni trokut



Izvor: www.researchgate.net

Sigurnost informacijskih sustava ostvaruje se osmišljavanjem i provedbom mjera zaštite (informatičkih kontrola) koje se ugrađuju u mehanizme funkcioniranja informacijskih sustava, omogućuju njegovo neometano funkcioniranje i ublažavaju ili smanjuju informatičke rizike.

Kontrole ugrađene u rad informacijskog sustava predstavljaju skup međusobno povezanih komponenti, koje djelujući jedinstveno i usklađeno, potpomažu ostvarivanju ciljeva informacijskoga sustava.[15] Kontrole se usmjeravaju na neželjene događaje ili procese u informacijskome sustavu koji mogu nastati, odnosno biti aktivirani iz različitih razloga koji se odnose na unutarnje djelovanje informacijskog sustava ili uzroke iz njegove okoline. Kontrole se primjenjuju zato da bi se spriječili, otkrili ili ispravili neželjeni događaji ili procesi.

[14] http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[15] Spremić, M., (2017)., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 87.

Svrha informatičkih kontrola je smanjenje vjerojatnosti nastupa neželjenog događaja i smanjenje očekivanih gubitaka do kojih bi došlo kod pojave neželjenih događaja ili ostvarenja neželjenih procesa u sustavu.

Informatičke kontrole djeluju na dva načina:[16]

1. preventivnom kontrolom smanjuje vjerojatnost neželjenih događaja i/ili procesa,
2. detektivnim i korektivnim kontrolama smanjuje se veličina gubitka koji bi nastao zbog neželjenih događaja i/ili procesa.

Svaki informacijski sustav sadrži razne kontrole koje su u njega ugrađene, a koje se primjenjuju kako bi se ostvarili njegovi ciljevi te kako bi se njime učinkovito upravljalo. Kontrole što su učinkovitije i bolje osmišljene manje je vjerojatno da će informacijski sustav biti izložen nekoj prijetnji i da će se neželjeni događaj pretvoriti u rizik za poslovanje.

Informacijske kontrole razvrstavaju se prema sljedećim kriterijima:

Obzirom na način primjene razlikujemo:

- automatske kontrole i
- ručne kontrole.

Obzirom na svrhu zbog koje se poduzimaju razlikujemo:

- preventivne kontrole,
- detektivne kontrole i
- korektivne kontrole.

Obzirom na hijerarhijsku razinu njihova djelovanja razlikujemo:

- korporativne kontrole,
- upravljačke kontrole i funkcijske kontrole i
- operativne kontrole.

Obzirom na način funkcioniranja razlikujemo:

- organizacijske kontrole,
- tehnološke kontrole i
- fizičke kontrole.

[16] Spremić, M., (2017)., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 88.

Navedene kontrole se međusobno isprepliću te neke od njih se mogu uvrstiti u više različitih kategorija. Revizijom informacijskih kontrola se provjerava postoji li neka informatička kontrola i u kojoj je mjeri učinkovita.

3.1. Važeći zakoni informacijske sigurnosti

U nastojanju da se stvore uvjeti za siguran i nesmetan informacijski razvoj, posebno na području zaštite tajnosti, cjelovitosti i dostupnosti podataka, Republika Hrvatska donijela je čitav niz zakona, propisa i uredbi. Osim navedenog odnose se i na zaštitu intelektualnog vlasništva te primjeni elektroničkog poslovanja. Neki od zakona će biti samo navedeni, a relevantniji zakoni opisani.

Zakoni koji uređuju područje informacijske sigurnosti su:

- Zakon o informacijskoj sigurnosti (NN 79/2007)
- Zakon o provedbi uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage direktive 1999/93/EZ (NN 62/17)
- Zakon o elektroničkoj ispravi (NN 150/05)
- Zakon o zaštiti osobnih podataka (NN 103/03)
- Zakon o tajnosti podataka (NN 79/2007)
- Zakon o sigurnosnoj provjeri (NN 85/2008)
- Zakon o sigurnosnim službama (NN 32/02)
- Zakon o sigurnosno-obavještajnom sustavu (NN 32/02)

3.1.1. Zakon o informacijskoj sigurnosti

Najvažniji zakon koji se odnosi na sigurnost informacijskih sustava je Zakon o

informacijskoj sigurnosti kojeg je Hrvatski sabor donio 13. srpnja, 2007. godine. Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.[17] Zakon se primjenjuje na državna tijela, jedinice lokalne i područne (regionalne) samouprave i na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke, kao i na pravne i fizičke osobe koje imaju pristup ili postupaju s navedenim podacima. Zakon se sastoji od osam dijelova.
Zakonom propisane mjere i standardi informacijske sigurnosti koji se odnose na područje informacijske sigurnosti su:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podataka,
- sigurnost informacijskog sustava i
- sigurnost poslovne suradnje.

U zakonu su definirana središnja državna tijela za informacijsku sigurnost, a to su Ured vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava, te Nacionalni CERT koji je osnovan unutar CARNet-a. O navedenim institucijama će biti rečeno više u sljedećim poglavljima.

3.1.2. Zakon o provedbi uredbe o elektroničkoj identifikaciji i uslugama povjerenja

Zakon o elektroničkom potpisu (NN 10/02) je prestao važiti 07. kolovoza 2017. godine i zamijenjen je Zakonom o provedbi uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage direktive 1999/93/EZ koji vrijedi od 08. kolovoza 2017. godine. Regulatorni okvir u RH za usluge povjerenja poput elektroničkog potpisa je bio uspostavljen, ali nije postojao specifičan i ujednačen okvir za uzajamno i prekogranično priznavanje i prihvaćanje e-identiteta, autentifikacije i srodnih usluga povjerenja. Navedena uredba proširuje mogućnosti koje pružaju postojeći sustavi za elektroničku identifikaciju čineći ih funkcionalnima i preko

[17] http://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html

granica Europske unije.

Ovim Zakonom se utvrđuju nadležna tijela te njihove zadaće za provedbu Uredbe, određuje tijelo nadležno za akreditaciju tijela za ocjenu sukladnosti i utvrđuju prava, obveze i odgovornosti potpisnika i pružatelja usluga povjerenja. Također, propisane su i prekršajne odredbe za postupanje protivno Uredbi.

3.1.3. Zakon o elektroničkoj ispravi

U Zakonu o elektroničkoj ispravi uređuje se pravo fizičkih i pravnih osoba na uporabu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, pravna valjanost elektroničke isprave te uporaba i promet elektroničkih isprava.[18] Elektronička isprava se može definirati kao skup podataka koji su elektronički oblikovani, poslani, primljeni ili sačuvani na elektroničkom, optičkom ili nekom drugom mediju te njen sadržaj mogu biti svi oblici pisanog teksta, slike, crteži, zvuk, glazba i sl. Ima istu pravnu snagu kao i isprava pisana na papiru te se sastoji od dva neodvojiva dijela. Prvi dio je opći dio kojeg čini predmetni sadržaj isprave, te posebnog dijela kojeg čini elektronički potpis i podaci o vremenu nastajanja elektroničke isprave. Prilikom korištenja elektroničkih isprava, informacijski sustav mora imati odgovarajuću zaštitu osobnih podataka u skladu sa zakonom i propisima.

Uporaba elektroničkih isprava smatra se pravovaljanom ako su ispunjeni sljedeći uvjeti:[19]

- da sadrži podatke o stvaratelju, pošiljatelju i primatelju te podatke o vremenu otpreme i prijema,
- da kroz cijeli dokumentacijski ciklus sadrži isti unutarnji i vanjski obrazac koji je oblikovan pri njenoj izradi i koji mora ostati nepromijenjen te,
- da je u bilo kojem trenutku dostupna i čitljiva ovlaštenim fizičkim i pravnim osobama.

[18] https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi

[19] https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi

Elektroničke isprave se pohranjuju u originalnom obliku na informacijskim sustavima ili medijima koji omogućuju trajnost elektroničkog zapisa za utvrđeno vrijeme zapisa.

3.1.4. Zakon o zaštiti osobnih podataka

Zakonom o zaštiti osobnih podataka se uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj.[20] Njegova svrha je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda. Odredbe Zakona se primjenjuju na obradu osobnih podataka od strane državnih tijela, lokalne i područne samouprave te pravnih i fizičkih osoba koje obrađuju osobne podatke. Za obavljanje nadzora nad obradom osobnih podataka osnovana je Agencija za zaštitu osobnih podataka koja je odgovorna Hrvatskom saboru. Zadužena je za nadziranje provođenja zaštite osobnih podataka i ukazivanje na zloupotrebe te rješava zahtjeve za utvrđivanje povrede prava koji se odnose na zaštitu osobnih podataka.

3.2. Institucije koje djeluju na području informacijske sigurnosti

U sljedećim poglavljima će biti navedena i opisana središnja državna tijela koja djeluju na području informacijske sigurnosti te Hrvatska akademska i istraživačka mreža.

3.2.1. Ured vijeća za nacionalnu sigurnost

Ured vijeća za nacionalnu sigurnost (UVNS) je središnje državno tijelo odgovorno za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u Republici Hrvatskoj, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.[21] Mjere i standardi informacijske sigurnosti se odnose na sigurnosne provjere osoblja,

[20] https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka
[21] http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html

fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje.

Ured vijeća za nacionalnu sigurnost prati zakonitost, svrsishodnost i djelotvornost agencija, temeljem zaprimljenih izvješća te njihova usklađenost s aktima i odlukama kojima se usmjerava rad sigurno-obavještajnih agencija. Na osnovu uradaka sigurnosno obavještajnih agencija, izrađuje objedinjena i periodična izvješća te strategijske procjene za potrebe Predsjednika RH i Vlade.

U sastavu UVNS-a djeluje Središnji registar za prijam, pohranu i distribuciju informacija i dokumenata u razmjeni sa stranim zemljama i organizacijama.

3.2.2. Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela RH, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.[22] Osim navedenih zadaća obavlja poslove istraživanja, razvoja i ispitivanja tehnologija namijenjenih zaštiti klasificiranih podataka te za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava.

Standardi tehničkih područja sigurnosti informacijskih sustava primjenjuju se na sva državna tijela, jedinice lokalne i područne (regionalne) samouprave kao i na pravne osobe s javnim ovlastima koje koriste klasificirane i neklasificirane podatke.

Rad Zavoda za sigurnost informacijskih sustava uređen je Zakonom o sigurnosno-obavještajnom sustavu RH, Zakonom o informacijskoj sigurnosti te Uredbom Vlade RH o mjerama informacijske sigurnosti. Za poslove akreditacije informacijskih sustava surađuje s Uredom Vijeća za nacionalnu sigurnost, dok za poslove prevencije i zaštite te izrade preporuka i normi vezanih za sigurnost informacijskih sustava surađuje s Nacionalnim CERT-om.

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

3.2.3. Hrvatska akademska i istraživačka mreža

CARNet (Croatian Academic and Research Network), odnosno Hrvatska akademska i istraživačka mreža nastala je 1991. godine sa svrhom pospješivanja napretka pojedinca i društva u cjelini pomoću novih informacijskih tehnologija. CARNet je javna ustanova koja djeluje u sklopu Ministarstva znanosti i obrazovanja u području informacijskih i komunikacijskih tehnologija i njihovih primjena u obrazovanju u rasponu od mreža i internetske infrastrukture, preko e-usluga do sigurnosti i korisničke podrške.[23] Njegove usluge su dostupne obrazovnim ustanovama, kao što su osnovne i srednje škole, sveučilišta, znanstveno-istraživački centri i instituti, te pojedinačnim korisnicima koji uključuju učenike, nastavnike, studente, profesore, znanstvenike i zaposlenike ustanova članica CARNeta. CARNet nudi različite usluge obrazovanja i osposobljavanja, multimedije, računalne sigurnosti, internetske povezanosti, korisničke podrške itd. Standard za pristup njegovim uslugama je virtualni elektronički identitet kojim se upravlja posredstvom središnjeg sustava za autentifikaciju i autorizaciju. CARNetovi inženjeri su aktivno uključeni u testiranje novih rješenja i tehnologija te sudjeluju u raznim projektima istraživanja i razvoja. CARNet pruža usluge filtriranja sadržaja školama, izdaje poslužiteljske certifikate, provodi provjeru ranjivosti i izdaje sigurnosne preporuke.

3.2.4. Nacionalni CERT

Nacionalni CERT (Croatian national computer emergency response team) je osnovan u skladu sa Zakonom o informacijskoj sigurnosti RH. Sukladno tome, jedan od zadataka je obrada incidenata na Internetu, odnosno očuvanje informacijske sigurnosti Republike Hrvatske. CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži. Misija Nacionalnog CERT-a je prevencija i zaštita od računalnih ugroza sigurnosti javnih informacijskih sustava u RH. U okviru svog djelovanja provodi proaktivne i reaktivne mjere.

Proaktivne mjere koriste za sprječavanje ili umanjenja mogućih šteta i to prije incidenta i ostalih događaja koji mogu predstavljati opasnost za sigurnost informacijskih sustava. Na

[23] http://www.carnet.hr/o_carnetu/o_nama

web stranicama Nacionalnog CERT-a naveden je popis proaktivnih mjera, koje podrazumijevaju aktivno praćenje stanja na području računalne sigurnosti, praćenje tehnologija vezane za računalnu sigurnost, objava sigurnosnih novosti u svrhu sprječavanja šteta, edukacija šire javnosti i unaprjeđenje svijesti o važnosti računalne sigurnosti, te obuka određenih grupa korisnika.
Reaktivnim mjerama se djeluje na incidente te druge događaje koji mogu ugroziti računalnu sigurnost javnih informacijskih sustava u RH. Takve mjere podrazumijevaju: izradu i objavu upozorenja vezanih za sigurnost, prikupljanje, obrađivanje i pripremanje sigurnosnih preporuka o slabostima informacijskih sustava, objavljivanje i pohranjivanje istih u svom informacijskom sustavu, te organizacija rješavanja većih incidenata pri čemu je barem jedna strana iz RH.

3.2.5. Agencija za zaštitu osobnih podataka

U Republici Hrvatskoj je osigurana zaštita osobnih podataka svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o vjerskim i antropološkim različitostima. Taj posao obavlja Agencija za zaštitu osobnih podataka koja djeluje samostalno i neovisno o izvršnoj i zakonodavnoj vlasti od 24. listopada 1995. godine. 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. Agencija također ima trajnu zadaću podići razinu svijesti svih sudionika i svih ciljanih javnosti o važnosti zaštite osobnih podataka, o njihovim pravima i obavezama te predlaganje mjera za unaprjeđivanje zaštite osobnih podataka.

3.3. Standardi informacijske sigurnosti

Informacijski sustavi, a posebno oni koji se temelje na digitalnim tehnologijama, su dinamični te stalno podložni promjenama. Stoga, sigurnosne mjere i zahtjeve je potrebno

kontinuirano mijenjati, nadopunjavati i unapređivati kako bi se informacijski rizici zadržali na prihvatljivim razinama, a informacijski sustavi ispunjavali svoje ciljeve. Zato danas postoje opće prihvaćeni standardi i norme na međunarodnoj razini koji pokrivaju različita područja primjene informatike u poslovnoj praksi te olakšavaju poduzećima rad nad svojim informacijskim sustavima.

Najčešće korišteni okviri upravljanja informacijskom sigurnošću su:[24]

- CobiT 5,
- ISO 27001:2013,
- PCI DSS,
- US National Institute of Standards and Technology (NIST) i
- SANS Institute Critical Controls

S obzirom da standard ISO 27001:2013 predstavlja preporuke i norme koje su najrelevantnije za potrebe pisanja ovog rada isti će biti opisan u tekstu koji slijedi.

Standard ISO 27001:2013

Institucije za izdavanje standarda u području zaštite informacijskih sustava su ISO (International Organization for Standardization) i IEC (International Electrotechnical Commission). To su međunarodne organizacije za standardizaciju.

ISO/IEC 27001:2013 (Annex A) je trenutno najnovija verzija ovog standarda, a predstavlja minimalne zahtjeve i norme koje organizacija treba poduzeti da bi se uspostavio sustav upravljanja sigurnošću informacija. Sadrži 14 sigurnosnih upravljačkih kontrola, 35 sigurnosnih kontrolnih ciljeva i 133 sigurnosne kontrolne mjere. Implementacija ovog standarda omogućuje ostvarivanje najvažnijih ciljeva poduzeća na području informacijske sigurnosti. Standard je izrađen 2005. godine, a nastao je na temelju standarda BS 7799 (British Standards).

[24] M., Spremić, (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 108.

Standard se sastoji od 14 dijelova:[25]

1. Politike informacijske sigurnosti (obuhvaća smjernice i podršku uprave za informacijskom sigurnosti)
2. Organizacija informacijske sigurnosti (organizacija bi trebala postaviti ljude koji će provoditi primjerene zaštite informacija te zaštitu od unutarnjih i vanjskih prijetnji)
3. Sigurnost ljudskih resursa (dodjela potrebne razine pristupa svakom zaposleniku te između njih uspostaviti određenu razinu svijesti i primjereno ih obrazovati)
4. Upravljanje imovinom (pravilno raspolaganje informacijskih resursa i njihova zaštita)
5. Kontrola pristupa (pristup računalima, mreži i podacima mora biti pod nadzorom da bi se spriječilo neovlašteno korištenje istih)
6. Kriptografija (osiguravanje učinkovito korištenje kriptografije za zaštitu)
7. Fizička sigurnost i zaštita od utjecaja okoline (fizička zaštita računala i opreme od zlonamjernih i nenamjernih oštećenja i gubitaka)
8. Sigurnost informatičkih resursa i poslovnih operacija (mora se omogućiti sigurnost i učinkovitost rada uređaja za obradu resursa)
9. Sigurnost komunikacijske infrastrukture (uspostavljanje zaštite informacija u računalnim mrežama pri prijenosu unutar i izvan poduzeća)
10. Razvoj sustava i održavanje (osiguravanje da je informacijska sigurnost sastavni dio informacijskog sustava kroz cijeli životni ciklus)
11. Upravljanje odnosa s dobavljačima (osigurati ne otkrivanje povjerljivih podataka između poduzeća i dobavljača)
12. Upravljanje incidentima informacijske sigurnosti (sigurnosne incidente koji su se dogodili potrebno je odmah prijaviti nadležnoj ustanovi, te voditi računa o upravljanju sustavom ukoliko se sigurnosni incident dogodi)
13. Upravljanje kontinuitetom poslovanja (provođenje analize utjecaja informacijskog sustava na kontinuirano poslovanje organizacije kako bi se smanjila nastala šteta sigurnosnim incidentima)

[25] M., Spremić, (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 112.

14. Sukladnost (informacijski sustav je potrebno uskladiti sa propisanim zakonima, standardima te ugovorenim zahtjevima)

3.4. Prijetnje informacijskih sustava

Prijetnja se može definirati kao mogućnost ili namjera neke osobe da poduzme akcije koje nisu u skladu s ciljevima organizacije.[26]

Izvori prijetnji mogu biti:[27]

1. prirodni – odnose se na prirodne katastrofe, potresi, poplave i slično
2. ljudske pogreške, odnosno čimbenici unutar poslovne organizacije – obuhvaćaju prijetnje koje mogu nastati namjernim ili slučajnim pogreškama koje rade ljudi, a to su uglavnom nezadovoljni zaposlenici organizacije ili djelovanje njihovog nemara i neopreznosti (neovlaštena uporaba resursa informacijskih sustava, zaraza računalnim virusima, slučajno brisanje važnih podataka)
3. namjerno počinjenje štete ili ugroza rada informacijskog sustava – to su namjerni napadi na imovinu sustava s ciljem počinjenja izravne štete ili prekida rada sustava (napadi računalnim virusima) ili napadi s ciljem neovlaštenoga upada u sustav i počinjenja štete.
4. čimbenici iz okružja poslovne organizacije – može se odnositi na nestanak struje, terorizam, špijune, kriminalce, računalne hakere i sl.

Tablica 2. Izvori opasnosti i rizika u informacijskome sustavu

PRIRODNI	LJUDSKI namjerni	LJUDSKI pogreška
Požar	Računalni kriminalci	Brisanje podataka
Poplava	Nezadovoljni djelatnici	Nepravilno rukovanje opremom
Jaka i izravna svjetlost	Hakeri	Nestručnost
Prljavština i prašina	Teroristi	Nepažnja, nemar, neznanje

Izvor: prikaz autora prema Srića, V. i suradnici, Menedžerska informatika str. 97

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

[27] Srića, V. i suradnici, Menedžerska informatika, MEP Consult, Zagreb, 1999. str. 99.

Svaka od navedenih prijetnji može prouzročiti velike gubitke za poslovanje ukoliko se na adekvatan način ne pristupi mjerama zaštite informacijskih sustava i njegove okoline, a njihov zajednički prikaz možemo vidjeti na tablici 2. Gubitak, kao rezultat prijetnji, može biti u materijalnom obliku koji se ogleda kao kvar ili oštećenje nekog dijela opreme, ali može se odraziti u obliku gubitka informacija koje su potrebne za poslovanje organizacije. Ipak, najvažnija posljedica može bit opasnost za zdravlje zaposlenika, a moguće i gubitak zaposlenika.

3.4.1. Prirodni izvori opasnosti informacijskih sustava

U skupinu prirodnih prijetnji spadaju meteorološke, geofizičke nepogode, sezonski fenomeni, astrofizički fenomeni te biološke prijetnje.[28]

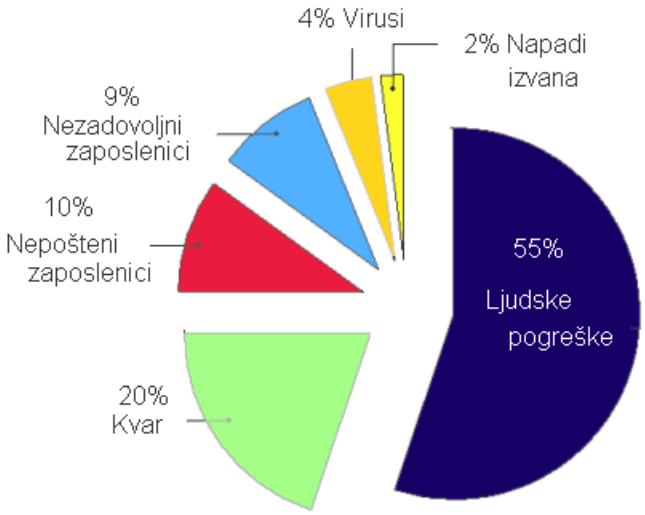
Prilikom meteoroloških nepogoda kao što su kiše, snijeg, oluje, ekstremno viskoke ili niske temperature, vjetar i sl. može doći do različitih oštećenja ili uništenja uređaja informacijskog sustava. Potresi i vulkanske aktivnosti, spadaju u geofizičke nepogode, a njihovim djelovanjem dolazi do drugih nepogoda (požari, poplave, prekid električnog napajanja, zagađenje kemikalijama), a posljedice su također velika materijalna oštećenja te prekid rada sustava. Kao i gore navedene nepogode, sezonski fenomeni imaju jednake posljedice na informacijske sustave, a predstavljaju razdoblje vremenskih ekstrema pri čemu dolazi do nepogoda u vidu uragana, tajfuna, šumskih požara i sl. Prilikom djelovanja astrofizičkih fenomena (npr. meteori) može doći do prekida satelitskih veza dok se pod biološkim prijetnjama podrazumijevaju različite bolesti koje za posljedicu imaju smanjenje radne snage. Kada je riječ o sigurnosti informacijskih sustava, veliki problem u poslovanju predstavljaju prirodne prijetnje jer na takve prijetnje čovjek nema nikakav utjecaj. Međutim, određenim mjerama moguće je učinak prirodnih nepogoda smanjiti na najmanju moguću razinu tj. minimalizirati štetu nastalu na informacijskim sustavima djelovanjem nekih od gore navedenih nepogoda.

3.4.2. Ljudske prijetnje informacijskim sustavima

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

Ljudski faktor ima važnu ulogu u postizanju što bolje sigurnosti informacijskih sustava, ali jednako tako predstavlja i prijetnju informacijskome sustavu. Takve prijetnje mogu dolaziti od zaposlenika, korisnika, klijenata, poslovnih partnera, dostavljača te kriminalnih skupina koje su povezane ili nepovezane s poslovanjem organizacije, njezinom imovinom i podacima. Prijetnje koje uzrokuju najčešće zaposlenici, ali odnose se i na ostale navedene osobe, su: neposlušnost, otkrivanje osobnih podataka, sabotaža, namjerno oštećenje imovine, zlouporaba ovlasti, neovlašten pristup imovini ili podacima te krađa imovine poduzeća.[29]

Slika 2. Prijetnje sigurnosti informacijskih sustava



Izvor: http://sigurnost.zemris.fer.hr

Gore prikazana slika 2. jasno prikazuje da najveću opasnost na informacijske sustave predstavljaju ljudi i to u vidu pogrešaka koje su nastale ljudskim djelovanjem, neposlušnim i nepoštenim radnicima. Kvarovi na informacijskim sustavima se nalaze na drugom mjestu, dok najmanju opasnost predstavljaju virusi i napadi izvana.

Jedna od najzloglasnijih prijetnji je računalni odnosno informatički kriminalitet. Pod ovim nazivom se podrazumijeva ukupnost protupravnih aktivnosti pri kojima informacijska tehnologija služi kao sredstvo činjenja i/ili objekt napada.[30] Prema procjenama američkog Federalnog istražnog ureda (FBI) tek se oko 5% informatičkog

[29] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf
[30] Panian, Ž., (2005.), Poslovna informatika za ekonomiste, Masmedia, Zagreb, str. 314.

kriminala otkrije, a samo 2% procesiranih prekršaja završi kažnjavanjem izvršitelja. Razlog tako malim postotcima su poteškoće pri otkrivanju protupravnih djela i komplikacija u dokazivanju izvršitelja.

Suvremena pravna teorija i sudska praksa prihvaćaju sljedeću opću klasifikaciju informatičkog kriminaliteta:[31]

1. manipulacija sredstvima informacijske tehnologije,
2. neovlaštena uporaba računalnih programa i povreda prava vlasništva,
3. sabotaže i računalni virusi i
4. zlouporaba parainformacijske tehnologije.

U daljnjem tekstu biti će opisani neki od napada na informacijske sustave koji su najrelevantniji za potrebe ovog rada, a dotiču se područja povrede prava vlasništva, sabotaže te krađe identiteta.

Neovlaštena uporaba računalnih programa i povreda prava vlasništva je jedan od najrasprostranjenijih oblika informatičkog kriminala. Računalni programi su autorsko djelo i podliježu načelima zaštite prava vlasništva jednako kao i pisana, likovna, glazbena i ostala djela te patenti. Neovlaštena uporaba računalnih programa podliježe zakonskim sankcijama. Za ovakvu pojavu računalnog kriminala, popularni naziv je softversko piratstvo ili gusarstvo. Softversko piratstvo u svijetu predstavlja financijski prekršaj te se za njegovo suzbijanje i kažnjavanje zauzima financijska policija, kao što je to slučaj i u Hrvatskoj.

Najčešći oblici povreda prava vlasništva računalnih programa su: kopiranje, krivotvorenje, skidanje zaštićenih programa ili njihovih dijelova s Interneta, neovlašteno iznajmljivanje u maloprodajnoj mreži, na Internetu ili putem vlastitih računala na kojima su instalirani tuđi programi. Protiv navedenih zlouporaba provode se zaštitne mjere, kao što su kriptografske, ali one povećavaju cijenu programa na tržištu, što sigurno ne ide na ruku ni proizvođačima ni kupcima programskih proizvoda. Osim što softversko piratstvo dovodi do novčanih gubitaka proizvođača, također se negativno odgleda u povećanju cijene legalnih program, smanjenju inovacija u softverskoj industriji te smanjenju ponude

[31] Ibidem, str. 315.

legalnih programa.

Sabotaže informacijskih sustava su aktivnosti usmjerene na oštećivanje, onesposobljavanje ili uništavanje informatičke opreme i podataka. Mogu se ostvarivati ručno, stvaranjem nenormalnih uvjeta rada (npr. strujni udari, povećanje temperature u radnoj okolini i sl.) ili telekomunikacijskim kanalima. Sabotaže čine teroristi među koje spadaju hakeri (eng. hacker) ili njima slično krekeri (eng. cracker). Hakeri su prijestupnici koji uglavnom putem računalnih mreža neovlašteno traže nezaštićene ili nedovoljno osigurane elemente tuđih informacijskih sustava kako bi u njih provalili i ilegalno ostvarili neku korist. Krekeri za razliku od hakera, kojima je cilj ostvariti nekakvu korist, imaju namjeru pomoću računalnih programa izazvati materijalnu ili nematerijalnu štetu vlasnicima tj. ovlaštenim korisnicima informacijskog sustava.

Napadi usmjereni na onemogućavanje rada su napadi uskraćivanjem usluge (eng. Denial of Service - DoS). Odnose se na nedopuštene aktivnosti sprječavanja ili onemogućavanja ovlaštene uporabe računalne mreže, sustava ili programa iskorištavanjem njihovih resursa kao što je procesor, memorija, propusnost mreže i sl.

Slično gore navedenom napadu postoje i raspodijeljeni napadi uskraćivanjem usluge (eng. Distributed Denial of Service - DdoS) kojima se koordinirano, upotrebom više računala napadaju određeni resursi sustava s ciljem onemogućavanja njihova rada.

Jedna od vrsta sabotaže informacijskih tehnologija su računalni virusi. To su zlonamjerni računalni programi (eng. malware) koji se odnose na širok krug softverskih prijetnji usmjerenih na počinjenje šteta ugrožavanjem računalnih mreža, računalnih i informacijskih sustava, ugrožavanjem ili krađom privatnih i povjerljivih podataka i njihovom zlouporabom. To su programi koji su najčešće tajno, bez znanja korisnika, ubačeni u sustav s namjerom ometanja ili počinjenja određene štete, odnosno s namjerom ugrožavanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija, operacijskog sustava ili nekog drugog dijela računalnoga ili informacijskog sustava programi koji se 'zakače' na aplikacijske ili sistemske programe, a imaju svojstvo razmnožavanja, uzrokuju poteškoće pri radu informatičke opreme te oštećenje ili uništenje datoteka programa i podataka.

Najčešći primjeri računalnih virusa su:[32]

[32]Srića, V. i suradnici, Menedžerska informatika, MEP Consult, Zagreb, 1999. str. 107.

- trojanski konj – predstavlja destruktivni program koji prikriva svoju pravu aktivnost predstavljajući se kao normalni program, a širi se u privitcima poruka elektroničke pošte ili unutar nekog drugog programa
- crvi – su zlonamjerni programi sastavljeni od samokopirajućeg koda koji omogućava razmnožavanje i širenje crva te koji skenira mrežu tražeći računalo s odgovarajućim propustom na kojega se može kopirati i replicirati
- ransomware – je računalna ucjena kojom se nakon neovlaštenog upada u računalo, najčešće djelovanjem računalnog virusa kojega je pokrenuo neoprezni korisnik, kriptiraju podaci koji su u njemu pohranjeni, a koji su nužni za nastavak rada ili poslovanja, pri čemu napadači traže otkupninu za njihovo dekriptiranje
- spyware – programi koji koriste resurse računala ili mreže bez znanja korisnika, a s ciljem da nadgledaju njihove navike, posebno na Internetu, o čemu šalju podatke prema određenom poslužitelju
- adware – je vrsta zlonamjernog virusa koji ovisno o sadržaju neke web stranice pokazuju reklame, ankete, nude neke proizvode i slično, a mogu sadržavati maliciozne kodove različitih namjera.

Najčešći načini širenja virusa su preko zaraženih medija (USB, disk i sl.), preko datoteka koje se šalju preko mreže, datotekama preuzetim s Interneta, datotekama koje se šire društvenim mrežama ili koje se nalaze u privitcima elektroničke pošte i sl. Ažuriranje verizja softvera i korištenje nelicenciranih programa i aplikacija također pridonose većoj opasnosti širenja zaraze.

Phishing je vrsta računalne prijevare s ciljem krađe identiteta te se odnosi se na aktivnosti kojima prevaranti i računalni kriminalci dobiju pristup povjerljivim korisničkim podacima. Načini na koje pribave te podatke su slanje lažnih elektroničkih poruka korisniku, pritom lažno predstavljajući se da bi korisnik pomislio da su poslane od strane izvornih institucija. Prevarantske poruke izgledaju veoma slično porukama legitimiranih organizacija te imitiraju njihove usluge dovodeći korisnika u zabludu da bi on otkrio povjerljive podatke. To se najčešće radi putem skočnih prozora ili poveznica iz elektroničke pošte koje vode na određene internetske stranice te se dalje prosljeđuju podaci prevarantima ili računalnim kriminalcima, a ne s institucijom s kojom korisnik misli da

komunicira.

Vishing je sličan phishingu, ali se odnosi na lažne telefonske pozive u kojima se prevaranti predstavljaju kao zaposlenici banke, internetske trgovine ili slično te pokušavaju doći do povjerljivih podataka korisnika.

Skimming predstavlja umetanje nezakonite opreme u utore bankomata koja čita i pohranjuje magnetski zapis kartice. Takva vrsta opreme može očitati podatke s kartice (broj računa) te u kombinaciji s nezakonito postavljenom kamerom otkriva prevarantima pristupne podatke pomoću kojih ima pristup sredstvima s računa.

Društveni inženjering odnosi se na navođenje i manipuliranje osoba kako bi one otkrile što više osobnih podataka. Prikupljeni podaci dalje se koriste u svrhu krađe on-line identiteta i počinjenje različitih zlouporaba.

Keyloggers su uređaji kojima se bilježi svaki udarac na tipkovnici. Oni prate i bilježe sve što korisnici upisuju preko tipkovnice, a nevidljivi su za korisnika. Ti podaci se izdvajaju i objedinjuju te šalju kriminalcima. U kombinaciji s zloćudnim programima, kriminalci brzo uočavaju podatke kao što su lozinke, brojevi kartica, računa i ostali tajni podaci te time spadaju u jedan od najzastupljenijih načina ugrožavanja privatnosti.

Man-in-the-middle napad nastaje kada napadač, koji se nalazi na kanalu između poslužitelja resursa i korisnika, pomoću zlonamjernog računalnog programa iskorištava ranjivosti mreže i zaobilazi komunikacijske protokole. Takvim napadom mu je omogućeno nadgledati sadržaj, pohranjivati datoteke i mijenjati sadržaj komunikacije.

Prisluškivači mreže su aplikacije ili dio hardvera koji iskorištavaju sigurnosne propuste u računalnoj mreži i omogućuju nadgledanje, kopiranje i promjenu sadržaja koji se prenosi. Takvim nezakonitim pristupom napadači dolaze do podataka o lozinkama na dva načina: napad grubom silom (eng. brute force attack) prilikom kojeg se nasumice isprobavaju različite lozinke, te napad pomoću rječnika (eng. dictionary attack) gdje se za neovlašteni ulaz koristi algoritam rječnika često korištenih izraza.[33]

3.4.3. Ostale prijetnje informacijskom sustavu

Osim ljudskih prijetnji i prirodnih nepogoda, možemo definirati i ostale prijetnje na informacijski sustav koje su rezultat nekih nesreća, a nisu uzrokovane ljudskim ili

[33] Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004. str. 112.

prirodnim djelovanjem. Te prijetnje su: eksplozija, prašina, poplava, gubitak električnog napajanja te elektromagnetska radijacija.[34] Eksplozije mogu nastati curenjem plina ili pojave kvarova na uređajima te predstavljaju veliku opasnost za zaposlenike i okolinu sustava. Zbog nedovoljnog održavanja uređaja, prašina koja nastaje ulazi u fizičke elemente sustava te time uzrokuje različite kvarove na istima. Poplave mogu nastati i puknućem cijevi ili neadekvatno postavljenim odvodima te prilikom takve nepogode najveći rizik predstavljaju oštećenja na elektroničkim dijelovima sustava. Prekid kontinuiteta sustava se najčešće događa zbog gubitka električnog napajanja ako ne postoji određena zaštita koja pruža sustavima nesmetan rad neovisno o napajanju. Uslijed elektromagnetskog zračenja može doći do različitih kvarova na uređajima te tako prekinuti rad informacijskih sustava.

4. MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

Sigurnost informacijskih sustava i sama zaštita podataka i informacija dobiva na važnosti tek kada su se počela primjenjivati računala u poslovnoj praksi. Tada se veća pažnja usmjerila na zaštitu informacijskih sustava te su uvedeni razni standardi vezani uz

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

rad računala i pohranjivanje te zaštitu podataka i informacija što je već izneseno u prethodnim poglavljima. Na samom začetku informatizacije, računalna oprema bila je centralizirana pa je iz tog razloga najznačajniji način zaštite bila upravo fizička zaštita. Fizička zaštita primjenjivala se iz razloga što se računalna oprema nalazila u posebnim prostorijama i objektima, a te prostorije i objekte trebalo je dobro čuvati kako bi se informacije zaštitile. Trenutak kada se širi potreba i za nekim drugim vrstama zaštite je kada se počela distibuirati oprema te kada su se podaci uključivali na internet. Tada je bilo potrebno osim fizičke zaštite uvesti i druge vrste zaštite kao što su hardversko softverska zaštita te organizacijsko administrativna zaštita, te cjelokupan sustav zaštite svesti na složeniju razinu. Uvođenjem novih vrsta zaštite informacijskih sustava naglašena je potreba izradom i primjenom raznih uputa o zaštiti podataka koje se primjenjuju u poduzećima.

Informacijska sigurnost je zaštita informacija od velikog broja prijetnji radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od investicija i poslovnih prilika. Informacijska sigurnost postiže se primjenom odgovarajućeg skupa kontrola, uključujući politike, procese, procedure, organizacijske strukture i softverske i hardverske funkcije.[35]

Prema navedenom mjere zaštite informacijskih sustava mogu se podijeliti na zaštitu na razini države, zaštitu samih podataka, programsku zaštitu, organizacijsku zaštitu, te fizičku i tehničku zaštitu. Budući da su neki načini prethodno opisani u radu poput zaštite samih podataka i informacija do zaštite na razini države te su navedeni i objašnjeni zakonski akti koji se koriste na području informacijske sigurnosti, u daljenjem radu biti će navedeni te opisani preostali načini kojima se vrši zaštita informacijskih sustava.

4.1.Hardversko softverska zaštita

Kada je riječ o hardversko softverskoj zaštiti informacijskih sustava bitno je naglasiti kako je upravo ovaj aspekt jedan od najranjivijih. Razlog tome je što u današnjici

[35] Hadjina, N. Zaštita informacijskih susava. Zagreb: FER, 2009., str 6.

jednostavnu i brzu distribuciju softvera omogućuju sve brže internet veze te činjenica da upravo računalna mreža postaje glavni medij kojim se sve to omogućuje. Budući da je razvoj softvera relativno skup potrebno ga je štititi iako to nije moguće u potpunosti. Kad tada će se pojaviti piratska verzija na internetu te neće biti potrebe za originalnim programom. Ne postoji određena metoda kojom je moguće u potpunosti zaštiti softver te se iz tog razloga upravo i pojavljuju piratske verzije nakon nekog vremena što je program izbačen na tržište. Svaki program, odnosno softver predstavlja vid zaštite podataka i korištenjem razvijenog softvera i pravilnim očuvanjem istog poduzeće postiže prednost nad konkurencijom i veću zaradu.

4.1.1. Zakonska zaštita softvera

Postoje razni načini kojima se zakonski softver može zaštititi. Razlog tome je što se softver može smatrati i kao vrstom literarnog djela te kao vrstom mehanizma koji obavlja neki koristan posao. Upravo zbog toga softver se može štititi kroz autorsko pravo, patent, te licencu.

Autor se od nelegalnog korištenja njegova djela koristi autorskim pravom, ali ne štiti se sama ideja već način prikaza neke ideje te originalna implementacija. U softverskoj industriji autorskim pravom moguće je zaštititi izvorni i izvršni kod programa, strukturu i organizaciju koda programa, dijelove ili cijelo korisničko sučelje te sve priručnike, upute i ostalu dokumentaciju u pisanom ili digitalnom obliku.[36] Softver se štiti autorskim pravom jer se vrlo jednostavno, jeftino i u kratkom roku može dobiti, a također je primjenjivo na gotovo svaki oblik softvera.

Za razliku od autorskog prava, patentom se štiti sama ideja, matematički postupci korišteni u programu te algoritmi. U softverskoj industriji patent se konkretno odnosi na svaki koristan proizvodni proces, mehanizam ili princip koji je nov, te se ne nalazi prethodno u nekom već objavljenom patentu. Što se tiče patentiranja softvera ono se smatra najmoćnijim načinom zaštite softvera ali u isto vrijeme nije ni najpametnije činiti zaštitu putem patentiranja.[37] Činjenica je da je za patentiranje potrebno i do nekoliko godina, pa to dovodi u pitanje da li se isplati patentirati neki softver koji će za par godina biti

[36] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf,

[37] http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-28.pdf,

neiskoristiv. Softver se u današnje vrijeme prebrzo razvija da bi ga se ograničilo patentiranjem. U SAD-u je moguće patentirati softver ali u Europi nije.

Licencom se određuje koliko dugo se smije koristiti neki softver, u koje svrhe se koristi te koliko računala smije taj isti softver instalirati. Softverska licenca je pravni instrument kojim se regulira korištenje, distribucija i redistribucija softvera.[38] U današnje vrijeme najčešća zaštita softvera je upravo putem neke vrste licence.

Zakonski oblik zaštite dijeli softver na nekoliko kategorija. Te kategorije su: Public domain, Open Source, Freeware, Shareware, Komercijalni softver te licencirani Komercijalni softver.[39] Razlika svakog od ovih kategorija je u razini radnji i dozvola koje krajnji korisnik ima pravo činiti s određenim softverom. Stoga je Public domain softver s kojim korisnik radi sve što želi, smije ga koristiti, umnožavati, distribuirati pa čak i prodavati, a da prethodno nije dobio odobrenje autora. Redom kako su navedene kategorije softvera sve je manje ovlasti koje krajnji korisnik ima što se tiče njegovog korištenja, distribucije, kopiranja i sl. Ono što omogućuje Open Source softver jest promjena izvornog koda i daljnja distribucija istog pod uvjetom da i takav izmjenjeni softver ostaje Open Source, a sve se distribuira pod istim licencnim sporazumom. Freeware je softver koji ne odobrava promjene, te ima posebnu licencu sa definiranim pravilima korištenja, a autor softvera zadržava autorsko pravo. Shareware softver najsličniji je Freeware-u, samo što se nakon određenog perioda za njegovo korištenje treba izdvojiti određena svota novca kako bi se takav softver nastavio koristiti. Komercijalni softver je kategorija softvera gdje korisnik ima pravo samo koristiti taj softver, a nesmije ga kopirati, mijenjati te distribuirati. Danas je najčešće korištena kategorija licenciranog komercijalnog softvera. Kako sam naziv kaže, ovim softverom dobiva se samo licenca za korištenje istog, te ga je moguće koristiti u skladu s licencnim sporazumom te zakonom o autorskim pravima.

4.1.2. Metode zaštite softvera

U pokušaju da se softver zaštiti koriste se razne hardverske i softverske metode. Pomoću tih metoda prije nego se omogući korištenje softvera potrebno je proći kroz neku vrstu autentikacije korisnika, kako bi osigurale zaštitu informacija. U daljnjem tekstu u

[38] http://www.digitconsulting.rs/index.php/licenciranje-microsoft/licenciranje/sofverska-licenca.html,

[39] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf,

kratkim crtama biti će riječi o uređaju Dongle, zaštiti pomoću instalacijskog medija, zaštiti CD-a protiv kopiranja, fiksnoj registracijskoj šifri, promjenjivoj registracijskoj šifri, serijskom broju ovisnom o hardveru te zaštiti programa pomoću registracijske datoteke.

Dongle je vrsta hardvera koji se koristi kako bi se zaštitio neki softver od kopiranja i nedopuštenog korištenja. To je zapravo uređaj koji se spaja na serijski ili paralelni komunikacijski port računala da bi se omogućilo pokretanje određene aplikacije, drugim riječima takav uređaj sadrži hardverski implementiran ključ pomoću kojega se pristupa određenoj aplikaciji. Preko određenih portova računala prema dongle-u aplikacija šalje upite i provjerava odgovore koji pristižu. Ukoliko odgovarajući dongle nije priključen aplikacija će prestati s radom jer neće dobiti potrebne odgovore u obliku šifri. Što se tiče same razine zaštite ona nije određena dongle uređajem već izvedbom aplikacije koju koristi. Razlozi zašto se u današnjici dongle uređaji ne koriste ima nekoliko, počevši od komplicirane instalacije, visoke cijene pa sve do nemogućnosti distribucije softvera preko interneta.[40]

Zaštita pomoću instalacijskog medija je zaštita kod koje se softver isporučuje najčešće na optičkom mediju, CD-RW ili DVD-RW. Na optičkom mediju se nalazi poseban prostor u kojem se nalazi brojač instalacija programa. Svaki put, nakon uspješno obavljene instalacije, stanje brojača se uveća za jedan. Nakon određenog broja instalacija, više nije moguće instalirati program s određenog medija. Kako bi zaštita bila na razini i kako bi se ona sama ispravno provodila medij mora biti što teže kopirati, a u tu svrhu je potrebno da datoteka s brojačem bude enkriptirana kako bi bilo što teže izmijeniti sadržaj. Danas se taj način zaštite zbog svoje nepraktičnosti vrlo rijetko koristi.

Nekoliko je različitih vrsta zaštite CD medija protiv kopiranja, te svi programi koji se isporučuju na CD mediju imaju takvu zaštitu. Najjosnovniji oblik takve zaštite je provjera da li se ispravan CD nalazi u CD čitaču. Iako je nemoguće razlikovati original od ilegalno kopiranog CD-a, na taj način je moguće spriječiti pokretanje programa s tvrdog diska računala. I najjednostavnijom zaštitom CD medija protiv kopiranja onemogućeno je softverskim piratima da izbace nepotrebne dijelove programa te na taj način smanje prostor koji program zauzima i objave ga na internet. Nešto kompliciranija metoda zaštite protiv kopiranja CD medija je da se na originalni CD snimi neka informacija koju nije

[40] Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011. str. 152

moguće kopirati komercijalno dostupnim softverom za kopiranje CD-a.[41]

Najjednostavniji način zaštite softvera je ugradnja programske funckije koja traži od korisnika unos određene šifre za registraciju. Iako je ta šifra uvijek ista – fiksna registracijska šifra, prednost ove vrste zaštite je u tome što takva šifra nije nužno unesena na disku već se nalazi negdje unutar programskog koda.

Promjenjive registracijske šifre nešto su složeniji način zaštite softvera, a postoje dvije grupe: serijski broj se generira iz korisničkih podataka te serijski broj se generira iz prikupljenih podataka o hardveru računala. Kada je riječ o korisničkim podacima tada se šifra generira na način da se sakupe određeni podaci o korisniku kao što su ime, adresa, naziv poduzeća i slično. U trenutku kada korisnik upiše svoju šifru, program provjerava da li se ona poklapa s izračunatom šifrom. U drugom slučaju se serijski broj generira na osnovu serijskog broja dobivenog uz kupnju softvera i prikupljenih podataka o hardveru, poput konfiguracije operacijskog sustava, serijskog broja diska i slično. U toku instalacije programa, putem prikupljenih podataka program generira jedinstveni slučajni serijski broj, a aplikacija ga šifrira i skriva u posebnu datoteku. Na taj način prilikom registracije proizvođaču softvera šalje se taj dobiveni identifikacijski kod, a on štalje odgovarajuću šifru potrebnu za instalaciju softvera. Danas se ova vrsta zaštite softvera najčešće koristi, te se uz njega vrlo često koristi zaštita putem interneta.[42]

Serijski broj ovisan o hardveru jedan je od najčešće korištenih načina hardverske zaštite računala. Kada se program instalira generira se pseudo-slučajni serijski broj računala. Pomoću aplikacije taj broj se šifrira i pohranjuje u posebnu datoteku. Kako bi se postigao jedinstveni generirani broj, serijski broj se generira pomoću serijskog broja isporučene kopije softvera te iz prikupljenih podataka o hardveru računala i konfiguraciji operacijskog sustava. Nakon što se program instalira potrebno ga je instalirati, a prilikom instalacije šifra se šalje proizvođaču softvera koji korisniku vraća šifru potrebnu za registraciju, a ona odgovara generiranom serijskom broju hardvera.

Zaštita programa pomoću registracijske datoteke ima veliku prednost zbog količine informacija koju je moguće spremiti u njih. Registracijska datoteka u velikoj većini slučajeva enkriptirana te nije moguće pročitati i promijeniti njen sadržaj. U njoj mogu biti pohranjene informacije o korisniku, ključevi za dekriptiranje enkriptiranih dijelova

[41] Ibidem str.145

[42] Ibidem str.149

izvršnog koda aplikacije, registracijskoj šifri za autentikaciju korisnika i sl. U tu datoteku također je moguće pohraniti podatke o hardveru korisnikovog računala, upravo iz tog razloga jedinstvena datoteka se koristi za svako računalo.

4.1.3. Programske mjere zaštite

Programske mjere zaštite informacijskog sustava su na razini operacijskog sustava i na razini korisničkih programa. U organizacijama se najčešće koriste višekorisnički operacijski sustavi te je za svakog korisnika potrebno odrediti područje djelovanja i razinu pristupa informacijama što se čini zaštitom pomoću zaporki. Programske mjere zaštite grubo rečeno su sigurnosna pohrana podataka, zaštita od malicioznog softvera i sustavi kriptozaštite, kao što je prikazano na slici 3. Dalje u radu u kratkim crtama biti će opisana zaštita na razini operacijskog sustava, zaštita na razini korisničke programske podrške, kriptiranje podataka u komunikaciji, antivirus alati, antispyware alati te zaštitni zid odnosno firewall.[43]

Slika 3. Načini realizacije mjera programske zaštite

[43] Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi. Zagreb : Informator, 1999. str. 109

Izvor: http://panitiaictsmktp.blogspot.hr/2012/04/computer-security-security-measure.html

Zaštita na razini operacijskog sustava uključuje višekorisnički rad na računalu. Kako bi se zaštitile informacije ovlaštenim informacijama potpuni pristup ima samo administrator, a korisnik ima pristup samo onim informacijama koje mu omogući administrator. U svrhu očuvanja sigurnosti informacija administrator svakom korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi bez problema imao pristup relevantnim informacijama i kako bi obavljao zadatke za koje je zadužen. Sukladno obujmu posla i zadacima za koje je zadužen svaki korisnik zasebno dobiva određenu razinu ovlasti. Svako računalo može imati više administratora te više korisnika, a svi suvremeni operacijski sustavi poput Windows-a, MacOs-a, Linux-a i Unix-a omogućuju upravo ovakvu razinu zaštite.[44]

Zaštita na razini korisničkih programa sljedeći je korak u sigurnosti informacija. U informacijskom sustavu potrebno je ući u određeni korisnički program putem kojega se obavljaju zadaci i aktivnosti vezani uz određenu obavezu prema organizaciji. Korisnički programi štite se kroz tri razine. Prva razina odnosi se isključivo na čitanje podataka iz baze, druga razina omogućuje unos i promijenu podataka u bazi, a treća razina uz sve to omogućuje i brisanje podataka. Kako bi se osigurala informacijska sigurnost izmjenjeni i

[44] Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi. Zagreb : Informator, 1999. str. 117.

brisani podaci ne uklanjaju se na direktan način već se pohranjuju u datoteke kojima ima pristup jedino administrator. Administrator provjerava te podatke i odlučuje da li će se oni uistinu izbrisati ili ne.

Mrežna komunikacija vrlo je osjetljiva i rizična kada je riječ o sigurnosti informacija. Budući da su u suvremenim organizacijama dijelovi poslovnog sustava prostorno dislocirani javlja se potreba za umrežavanjem računala kako bi se informacije mogle zajednički koristiti. Uključivanjem interneta u poslovanje dolazi do pojave novih rizika, a osnovni zahtjevi kojih se treba pridržavati prilikom transfera informacija su osiguranje jednosznačnosti prijenosa te onemogućenje neautoriziranog korištenja ili promjene sadržaja u prijenosu. U mrežnoj komunikaciji najčešće se kao oblik zaštite koristi kriptiranje podataka. Kriptiranje je logička promjena podataka na način da se podatci pošalju primatelju, da nitko drugi osim primatelja i pošiljatelja ne zna izvorne podatke. Kriptiranje funkcionira na temelju šifriranja podataka pomoću određenog ključa i dešifriranja podataka istim ključem. Pošiljatelj šifrira podatke dok primatelj dešifrira ukoliko oboje imaju isti ključ. Na taj način štiti se informacijski sustav na razini mrežne komunikacije.[45]

Računalni virus je računalni program koji može zaraziti druge programe tako da u njih unese kopiju samog sebe, on se može proširiti računalnim sustavom ili mrežom koristeći se ovlastima korisnika koji su zaraženi. Svaki program koji je zaražen postaje virus i tako zaraza raste. Virusi mogu biti i neki drugi štetni programi poput trojanskih konja i crva. Štete koje virusi nanose su osim navedenih i širenje mrežom, krađa korisničkih lozinki, brojeva kreditnih kartica, omogućavanje pristupa neovlaštenim osobama zaraženom računalu i sl kao što je već rečeno u prethodnim poglavljima. Kako bi se to spriječilo kao zaštita se koriste antivirusni alati. Antivirusni alati sastoje se od nekoliko programa kojima se detektiraju postojeći virusi ili se jednostavno skeniraju datoteke tražeći viruse ili se identificiraju sumnjiva ponašanja od strane kompjuterskog programa koja bi mogla pokrenuti infekciju. Antivirusni alati štite informacijske sustave tako da zaraženu datoteku odvoje od ostalih datoteka kako se virus ne bi širio dalje, brišu zaraženu datoteku ili pokušavaju popraviti datoteku uklanjajući virus unutar iste.

Antispyware alati koriste se kako bi se informacijski sustav štitio od spyware-a.

[45] Ibidem str. 133

Spyware je široka kategorija malicioznog softvera sa namjenom da presreće ili preuzima djelomično kontrolu rada na kompjuteru bez znanja ili dozvole korisnika. U današnje crijeme taj naziv koristi se za široki spektar programa koji koriste korisnikov kompjuter kako bi dobili korisne informacije za neku treću osobu. Kako bi se očuvao informacijski sustav od takvih vrsta ugroza, koriste se antispyware alati ili programi. Antispyware programi djeluju poput antivirusnih programa na način da u trenutku kada je računalo zaraženo reagiraju ili to čine na način da se periodično kontrolira računalo kojim se korisnici u organizaciji koriste. Njima se pregledava Windows Registry, datoteke operativnog sustava i instaliranih programa, kada program uoči datoteku u kojoj se nalazi spyware on je uklanja. Isto tako ako se radi o trenutnom vremenu, prati se tok podataka preko interneta te antispyware programi blokiraju aktivnosti prepoznatih prijetnji.

Da bi određeni program dobio pristup mreži ili računalu organizacije potrebno je dobiti potvrdu firewalla za to. Firewall ili zaštitni zid koristi se kako bi se smanjio rizik zaraze malicioznim kodom te na taj način protok informacija za neovlaštenu upotrebu. Funkcionira na način da pregleda informacije koje dolaze s interneta i odlaze na internet, kada prepozna informacije koje dolaze sa sumnjivih i opasnih lokacija on ih ignorira. Na taj način hakeri koji traže ranjiva računala neće moći vidjeti računalo organizacije ukoliko je zaštitni zid pravilno konfiguriran.[46]

4.2. Organizacijske mjere zaštite

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te itegriteta 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.

Postoji nekoliko razina organizacijske sigurnosti na koje je potrebno obratiti pažnju, a to su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te outsourcing. Svaka od tih razina organizacije ima jedinstveni cilj u zaštiti informacijskih sustava.

[46] Hadjina, N., Zaštita informacijskih susava. Zagreb: FER, 2009. str. 77

4.2.1. Infrastruktura informacijske sigurnosti

Cilj infrastrukture informacijske sigurnosti jest upravljati informacijskom sigurnošću unutar organizacije. Drugim riječima kako bi organizacija funkcionirala te da bi se štitile informacije potrebno je poticati multidisciplinarni pristup sigurnosti informacija pravilnom suradnjom od najviših predstavnika u hijerarhiji organizacije do najnižih koji se koriste određenim informacijama. Infrastruktura informacijske sigurnosti može se podijeliti na: [47]

- 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 managerskog tima moraju se brinuti za informacijsku sigurnost jer je to njihova poslovna odgovornost. Tim za upravljanje informacijskom sigurnošću osniva se kako bi se lakše obavljali poslovi sigurnosti informacija u organizaciji, a jedan manager je odgovoran za sve aktivnosti koje su vezane uz sigurnost počevši od pregleda i odobravanja politike informacijske sigurnosti, praćenja promjena koje mogu prijetiti informacijskoj imovini pa sve do praćenja incidenata te odobravanja postupaka kojima se postiže poboljšanje informacijske sigurnosti.

Koordinacija rada informacijske sigurnosti najpotrebnija je u organizacijama koje su velike pa se kroz tim predstavnika managera relevantinh dijelova organizacije vrše radnje vezane uz koordinaciju. To je su najčešće: dogovaranje specifičnih uloga i određenih odgovornosti za informacijsku sigurnost za cijelu organizaciju, koordiniranje i podržavanje inicijative vezane uz informacijsku sigurnost, pregled izvješća o sigurnosnim incidentima, te općenito radnje vezane uz očuvanje sigurnosti informacija na razini cjelokupne

[47] Garača, Ž., Informatičke tehnologije, Sveučilište u Splitu, Split, 2007. str. 98

organizacije.

Politika informacijske sigurnost treba pružiti općenito vodstvo za dodjelu sigurnosnih uloga i odgovornosti u organizaciji. Glavni cilj jest da su sve odgovornosti informacijske sigurnosti jasno određene. Iz tog razloga najveća pažnja se usmjerava na identifikaciju i jasno definiranje dijelova imovine te sigurnosnih procesa pridruženih svakom pojedinom sustavu, zatim treba odrediti tko je odgovoran za pojedini dio imovine ili sigurnosni proces te je taj dogovor potrebno dokumentirati. U konačnici je potrebno dokumentirati te definirati razine ovlasti.

Proces autorizacije organizacijskih cjelina koje susjeluju u obradi bitan je kada se uvodi novi organizacijski dio u poslovanje, tada manageri zaduženi za informacijsku sigurnost moraju autorizirati namjenu i korištenje tog dijela organizacije, trebaju se provoditi kontrole hardvera i softvera posebice ako se za rad koriste osobna računala gdje je potrebno kontrolirati i autorizirati rad jer primjena osobnih računala može biti vid ranjivosti organizacije.

Svaka organizacija trebala bi imati i određene specijaliste koji će davati savjete za informacijsku sigurnost. Specijalisti informacijske sigurnosti posjeduju uravnotežene analitičke vještine i poslovnu sposobnost. Njihova uloga je provoditi kontrolu informacija i sigurnosti protoka informacija, te kada je to potrebno provoditi istrage, mjere i kontrole potrebne da se očuva informacijska sigurnost. Sve organizacije nemaju svoje savjetnike za informacijsku sigurnost pa tu ulogu preuzima osoba koja je najviše upoznata sa stanjem u organizaciji i njenim radom.

Kada je riječ o suradnji među organizacijama u ulozi informacijske sigurnosti potrebno je ograničiti razmjenu informacija kako se ne bi dogodilo da one dođu do neovlaštenih osoba. Suradnja je bitna sa zakonodavnim i koordinativnim tijelima, pružateljima informacijskih usluga te telekomunikacijskih operatera. Neovisni pregledi efikasnosti informacijske sigurnosti bitni su kako bi se utvrdilo vrši li se pravilno sigurnosna politika u organizaciji. Za takve preglede zadužena je unutarnja nadzorna funkcija, neovisni manager ili vanjska organizacija koja je specijalizirana za takve preglede i čiji članovi posjeduju potrebne vještine i iskustva. Uloga osoba zaduženih za kontrolu je pregledavanje implementacije dokumenata o politici informacijske sigurnosti te odgovornosti za istu.[48]

[48] Ibidem str. 111

4.2.2. Sigurnost pristupa treće zainteresirane strane

Kada je za potrebe poslovanja potrebno uključiti i treće osobe logično je da će organizacija uključiti posebne mehanizme kontrole kako bi se održala potrebna razina sigurnosti organizacijskih jedinica. Kako bi se osigurala sigurnost informacija koriste se i procjene rizika te se kontrolni mehanizmi ugovaraju s trećom stranom koja ima doticaj s informacijama.

Kod pristupa danog trećoj strani bitno je razlikovati i identificirati rizik koji se pojavljuje kod tog pristupa. Postoje dvije vrste pristupa: fizički te logički pristup. Fizičkim pristupom omogućava se trećim stranama pristup uredima, prostorijama s računalnom opremom i ormarima za pohranu, dok se logički pristup odnosi na pristup bazama podataka štićene organizacije te informacijskim sustavima.[49]

Radi vrste i obujma poslovanja organizacije treće strane dobivaju pristup informacijama. Omogućavanjem pristupa informacijama treće strane u dogovoru s organizacijom pristaju na kontrolne mehanizme koje će provoditi organizacija kako bi se smanjio rizik neovlaštenih upotreba informacija. Tek kada se potpiše ugovor treće strane mogu dobiti potrebne informacije potrebne za rad. Treće strane mogu biti čistači, dobavljači, zaštitari, usluge omogućene kroz outsourcing, privremeno zaposleni studenti, razni konzultanti, osoblje koje se brine o hardveru i softveru, partneri i sl.[50]

4.2.3. Outsourcing

Outsourcing se može definirati kao korištenje vanjskih poduzeća i pojedinaca za obavljanje pojedinog posla. Sukladno s definicijom outsourcinga, cilj organizacije je održati sigurnost informacija u slučaju kada je obrada istih povjerena nekoj drugoj organizaciji. Kada se ugovara posao outsourcing-a bitno je kao i s ostalim trećim stranama sklopiti neku vrstu ugovora kojim se kontrolni mehanizmi, procjena rizika i sigurnosni postupcim provode kako bi se spriječilo neovlašteno korištenje informacija u organizaciji. Ugovorom o outsourcing-u zadani su određeni uvjeti odnosno zahtjevi kojih se treba držati

[49] Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb : Sinergija - nakladništvo, 2001, str. 178

[50] Spremić, M., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, 2017, str. 84

prilikom obavljanja određenog posla za organizaciju. Stavke koje takav ugovor može sadržavati su:[51]

- 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 outsourcing-u
- Pravo na nadzor

Glavna prednost outsourcinga je da se organizacija može usredotočiti na svoju osnovnu aktivnost dok i razvoj poslovnih procesa, jer su sporedni poslovi dani drugoj organizaciji koja obavlja to za njih. Naravno da je u ovakvom obliku rješavanja poslova potrebna itekako visoka razina kontrole i zaštite informacijskih sustava.

4.3. Fizičke mjere zaštite

Fizičke mjere zaštite se uz ostale mjere zaštite koriste kako bi se očuvala sigurnost informacijskih sustava. Fizička sigurnost ugrožava se u slučajevima elementarnih nepogoda, poplave, potresa i požara 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. Fizička sigurnost može se smatrati osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj. Cilj fizičke sigurnosti je spriječiti ne autorizirane pristupe računalnom sustavu, zaštititi integritet podataka koji se pohranjuju na računalo, u slučaju raznih nepogoda spriječiti oštećenje ili gubitak podataka te spriječiti krađu podataka s računalnih sustava.

[51] Ibidem, str. 93

4.3.1. Prijetnje fizičkoj sigurnosti

Nekoliko je grupa prijetnji koje su već bile spomenute u prethodnim poglavljima. Prirodne nepogode su prva kategorija prijetnji fizičkoj sigurnosti, a karakteristika im je na na takve prijetnje čovjek ne može utjecati. Budući da će se prirodne nepogode dogoditi u svakom slučaju, uloga čovjeka je određenim mjerama spriječiti gubitak informacija potrebnih za poslovanje te općenito omogućiti nastavak neprekidnog rada informacijskog sustava. U skupinu prijetnji fizičkoj sigurnosti u vidu prirodnih nepogoda ubrajamo:[52]

- Meteorološke nepogode – razne padaline, vjetar, oluja jako niske ili visoke temperature na informacijski sustav mogu djelovati tako da se izgubi ili degradira komunikacija te uništenje samih uređaja gdje informacije mogu biti pohranjene
- Geofizičke nepogode – potresi i vulkanske aktivnosti izazivaju požare, poplave, ispuštanje raznih štetnih tvari, kemikalija i plinova te dolazi do prekida napajanja.kao i kod meteoroloških nepogoda i kod goefizičkih nepogoda jednake su prijetnje i rizici.
- Sezonski fenomeni – uništenje uređaja ili gubitak te degradacija mrežnih komunikacija mogu biti uzrokovani i ekstremnim vremenom kao što su uragani, šumski požari i slično.
- Astrofizički fenomeni – utjecaj sunčanih fenomena te meteora također može dovesti do gubitka ili degradacije satelitskih veza te time naštetiti sigurnosti informacijsih sustava.
- Biološke snage – radna snaga je potrebna za očuvanje informacijskog sustava, a razne bolesti mogu uzrokovati smanjenje broja sposobne radne snage za obavljanje određenog posla.

Druga kategorija prijetnji su ljudske prijetnje jer upravo zaposlenici, korisnici, klijenti, poslovni partneri, dobavljači i ostale osobe koje imaju doticaj s imovinom i podacima organizacije čine informacijsku sigurnost ranjivom svojim namjernim ili slučajnim

[52] Antoliš, K.,et al, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010. str. 205

potezima. Zaposlenici uzrokuju razne prijetnje, a one su:[53]

- Neposlušnost – ona dovodi do prosvjeda ili štrajka te u takvim situacijama može doći do oštećenja opreme i uređaja potrebnih za rad ali se isto tako mogu ozlijediti sami zaposlenici.
- Otkrivanje osjetljivih podataka – zbog nepravilnog rukovanja ili zbog nepoštivanja sigurnosne politike organizacije.
- Sabotaža – predstavlja namjerno narušavanje rada sustava i ispravnosti uređaja te je potrebno uvesti mjere kako bi se taj čin spriječio
- Nenamjerno oštećenje imovine – nepravilno i nedovoljno educirani zaposlenici mogu oštetiti uređaje ili dio neke druge imovine, pa je stoga potrebno poraditi na njihovoj edukaciji da bi se takve prijetnje mosle svesti na minimum
- Zlouporaba ovlasti – javlja se kada se zaposlenici ne pridržavaju pravila poslovanja i svojih ovlasti, može se dogoditi da prekomjereno koriste imovinu organizacije ili istu iznose van prostora za koji nije namjenjena
- Neovlašten pristup podacima ili imovini – zaposlenik mora prema ugovoru o povjerenju poštivati upotrebu povjerljivih informacija
- Krađa – zaposlenik namjerno otuđuje dio imovine organizacije

Osim ljudskih prijetnji i prirodnih nepogoda postoje i ostale prijetnje fizičkoj sigurnosti izazvane nekim nesrećama. Takve nesreće mogu biti razne eksplozije, prašina, gubitak električnog napajanja, elektromagnetska radijacija, poplave uzrokovane nekim kvarom. U svakom slučaju sve prijetnje mogu prouzročiti velike gubitke, stoga je potrebno uspostaviti određene mjere zaštite kojima će se informacijski sustavi zaštititi.

4.3.2. Područja zaštite

Radi li se o fizičkoj zaštiti informacijskih sustava tada je potrebno štititi ne samo pojedino mjesto na kojem se povjerljive informacije nalaze, već i cijelu okolinu kako bi što teže bilo doprijeti do određenih informacija. U tu svrhu postoji zaštita okoline, zaštita recepcije, zaštita prostorija, zaštita same opreme zatim kontrola pristupa i sl. Zaštita

[53] Ibidem, str. 209

okoline od prvi je korak koji treba poduzeti kada se štiti informacijski sustav. Najšire gledano ukoliko se ne može ući u određeni prostor gdje se informacija nalazi nije moguće ni ugroziti sigurnost informacijskog sustava. Kada je riječ o fizičkoj zaštiti tada u svrhu očuvanja informacijskog sustava postoje ograde ili zidovi koji štite okolinu organizacije te time brane pristup i uvid u ono što se događa u samoj organizaciji. Najbitniji dio te tog područja su ulazi i izlazi koje je potrebno više nagledati pomoću kamera, postavljanja lokota tako da pristup imaju samo osobe s ključem te postaviti zaštitare kako bi se utvrdilo tko ima pristup, a tko ne. Kao preventiva kriminalitetu i radi sigurnosti informacija okolina se štiti kroz CDTED dizajn (Crime prevention through environmental design) koji predstavlja multidisciplinarni pristup odvraćanja kriminalnog ponašanja kroz dizajn okoliša. Dizajnom okoliša daje se do znanja što spada u javno, a što u privatno vlasništvo te je na taj način lakše identificirati sumnjive prijestupnike.[54]

Kod većine organizacija na samom ulasku u objekt nalazi se neka vrsta recepcije odnosno mjesto na kojem se obavljaju određeni administrativni poslovi te gdje je moguće dobiti razne informacije. Rad na recepciji potrebno je kontrolirati na način da važni dokumenti ne stoje na vidiljvim mjestima dostupnim svima koji se nalaze u objektu, zatim je potrebno zaštititi rad na računalu tako da je usmjeren da klijent ne vidi što zaposlenik radi na njemu i slično. Osim ove vrste fizičke zaštite informacija na recepciji moguće je postaviti i kamere kako bi se vršio bolji nadzor, razne prekidače za slučaj opasnosti te alarme. Zaposlenik također mora paziti na svoj rad i ne napuštati radno mjesto dok nije spremio povjerljive informacije na za to predviđeno mjesto i onesposobio rad za neovlaštene osobe.

Prostorije sa skupocjenom opremom ili važnim poslužiteljima također treba zaštititi u skladu s namjenom informacija u tim prostorijama. Najčešće se to radi na način da su postavljene kamere, protupožarni i protuprovalni alarmi, razni prekidači za zaposlenike u slučaju opasnosti te općenito implementacijom sustava protiv neovlaštenog ulaska u određenu prostoriju.

Zaštita opreme smatra se najvažnijim aspektom fizičke zaštite informacijskog sustava, ali joj nije usmjerena dovoljna pažnja u obliku načina zaštite. Radi se o tome da se svaka oprema odnosno uređaj vrednuje po svojim karakteristikama i namjeni stoga je razina zaštite različita za različiti uređaje ili opremu. Većinom ta zaštita podrazumijeva samo

[54] Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011, str. 84

zaštitu primjerice osobnog računala na kojem zaposlenik radi ili zaštitu poslužitelja no potrebno je obratiti pažnju i na ostalu opremu. Primjerice staviti prijenosne medije s informacijama na sigurno mjesto, uništavanje starih medija na pravilan i siguran način, zaključavanje uređaja i sl.

Kontrola pristupa važna je kada je riječ o fizičkoj zaštiti informacija. Nju karakterizira nemogućnost ulaska u objekt osobama koje nemaju odobrenje za to. Najčešće se primjenjuje kontrola pristupa na način da se zaposle zaštitari ili druge osobe koje će kontrolirati tko ima pristup, a tko ne. Osim tog načina kontrola pristupa provodi se putem mehaničkih sredstva i tehničkih sredstva. 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 kontrola pristupa provodi a u suvremeno doba to se pametne kartice za kontrolu pristupa, skeniranje otiska prsta, šarenice oka ili pak prepoznavanje glasa.

Navedena područja fizičke zaštite informacijskih sustava kontroliraju se i pomoću EPS (electronic physical security). EPS je integrirana primjena brojnih elektroničkih sustava za sigurnost kao što su: sustavi za detekciju požara, automatski sustavi za suzbijanje plinova, sustavi za nadzor, sustavi za kontrolu pristupa, sustavi za detekciju upada, adekvatna oprema za zaštitare te sustavi za opremanje okoline i prostorija.[55]

4.3.3. Elementi za postizanje fizičke sigurnosti

Prethodno u radu su navedene prijetnje fizičkoj sigurnosti informacija te područja koja se štite kada je riječ o sigurnosti informacijskih sustava. U ovom dijelu rada biti će opisani elementi koji se koriste za postizanje fizičke sigurnosti od alarmnih sustava, rasvjete, zaštitara, nadzornih kamera, uređaja za kontrolu pristupa, sustava za zaključavanje prostorija i opreme te sustava za praćenje i otkrivanje lokacije.

Kako bi se upozorilo korisnike i zaposlenike u organizaciji o nekom nastalom problemu koriste se alarmni sustavi. Alarmnim sustavima daju se vizualna ili zvučna upozorenja o stanju sustava ili novonastalom problemu. Alarmnih sustava ima nekoliko vrsta ovisno o

[55] Ibidem, str. 109

namjeni:[56]

- Alarmi za sigurnost - alarmi za dojavu prirodnih nepogoda i izvanrednih situacija poput radijacije
- Alarmi u Q&M sustavima (operation and maintenance) – služe za slanje obavijesti o lošem radnom stanju sustava kojeg nadzire
- DCS sustavi(distributed control manufactoring system) –obavještavaju osoblje o važnim događajima, najčešće se koriste u kemijskim i nuklearnim labaratorijima
- Vremenski alarmi – aktiviraju se u trenutku kada je to odredila osoba koja ga je aktivirala
- Alarmi protiv provala – u slučaju provale pomoću njih obavještava se policija, najčešće su to tihi alarmi da ne bi zbunili provalnika.

Važnost alarma je vrlo velika kada je riječ o zaštiti informacijskih sustava jer se upotrebom alarma pravovremeno detektiraju uljezi i reagira se u trenutku. Negativna strana alarma je to što je moguće da se aktiviraju i kada za to nema potrebe. Primjerice protupožarni alarmi aktiviraju se detekcijom dima. Dim se može stvoriti i pušenjem cigarete i ako se protupožarni alarm nalazi u blizini i detektira dim može zaključiti da prijeti požar, a to zapravo nije slučaj. U svakom slučaju pravovremeno reagiranje alarma dovodi do toga da se pravovremeno informacije štite i time omogućava očuvaje sigurnosti informacijskog sustava.

U svrhu podizanja fizičke sigurnosti informacija može se koristiti i rasvjeta. Rasvjeta omogućava preglednost prostora i pruža sigurnost korisnicima i zaposlenicima u organizaciji. Rasvjeta može biti periodična, odnosno konstantna na način da se pali u zadanom vremenskom intervalu i gasi preko dana primjerice. Na taj način se omogućava drugim elementima fizičke zaštite – alarmima da svoju ulogu obavljaju besprijekorno. Osim određenih vremenskih intervala kada je rasvjeta uključena, postoji i aktiviranje i deaktiviranje rasvjete putem senzora te se na taj način štedi elekrična energija.

Elementi fizičke zaštite informacijskih sustava su već spominjani zaštitari. Zaštitari su posebno obučeni zaposlenici koji su educirani za pružanje zaštite vlasništva, dobra i osoba neke organizacije. Posao zaštitara je spriječiti bilo koje radnje vezane uz kriminal i općenito štititi organizaciju od opasnih radnji. Prilikom zapošljavanja zaštitari najčešće

[56] Hadjina, N., Zaštita informacijskih susava. Zagreb: FER, 2009, str. 143

prolaze određene testove kojima se mjere njihove sposobnosti i sukladno vrsti posla njihove reakcije. Zapošljavanjem zaštitara uvelike se pospješuje sigurnost informacijskih sustava jer svojim prisutstvom zaštitar ulaže povjerenje zaposlenicima te strah razbojnicima. Njegova uloga je patrolirati, obilaziti objekte kako bi se uvjerio da nema prijetnji, zatim provoditi kontrolu na ulazu u objekt te pravilno reagirati u slučaju opasnosti kako bi očuvao i zaštitio informacijski sustav.

Nadzorne kamere još su jedan element fizičke zaštite informacijskih sustava. Njima se kontrolira određeno stanje u organizaciji, oprema, uređaji, zaposlenici i slično. Nadzornih kamera ima nekoliko vrsta te namjena istih ovisi o tome što se nadzire i koliko je potrebno određenu poslovu situaciju i objekt štititi. Bez obzira o kojoj vrsti nadzornih kamera je riječ one održavaju fizičku sigurnost tako da:[57]

- Sprječavaju zločine
- Omogućavaju praćenje prijevoza opreme
- Pružaju mogućnost kontrole prilaska objektima
- Omogućuju identifikaciju osoba na ulazu
- Omogućuju praćenje aktivnosti zaposlenika i posjetitelja

Danas se najviše koriste IP (Internet Protocol) nadzorne kamere, koje se omogućuju preko internetske veze te je moguć stalni pregled stanja u organizaciji gdje su kamere postavljene.

Uređaji za kontrolu pristupa jedni su od važnijih zaštita pristupa objektu, tj. dozvole pristupa (ulaza/izlaza) ovlaštenim osobama ili zaposlenicima. U današnje vrijeme postoji nekoliko načina na koje se kontrolira pristup i time štite informacije. Pristup se može kontrolirati putem pametnih kartica za identifikaciju korisnika i zaposlenika, zatim identificiranjem osobe kroz otisak prsta, šarenicu oka, glas ili crte lica. Prema načinu na koji se korisnik sustava identificira razlikuju se fizičko i ponašajno prepoznavanje. Fizičko prepoznavanje odnosi se na oblik tijela, otisak prsta, prepoznavanje lica, geometriju ruke, šarenice oka i sl. Ponašajno identificiranje odnosi se na ritam, hod ili boju glasa zaposlenih ili korisnika.

Kako bi se fizički osigurala neka prostorija najčešće se koriste sustavi za zaključavanje prostorija da bi informacijski sustav ostao netaknut i siguran. Sustavi za

[57] Ibidem, str. 163

zaključavanje su mehanički ili elektronički uređaji u funkciji lokota. Prostorije se ovisno o razini zaštite zaključavaju pomoću ključa, kartica, lozinki ili njihovom kombinacijom. Osnovna namjena sustava za zaključavanje je spječavanje fizičkog pristupa nekom dobru ili imovini, a mogu se koristiti na vratima, prozorima, ormarićima ili uređajima. Prijetnje koje se javljaju kad je ovaj element u funkciji zaštite su provale, no uz odgovarajuću kombinaciju s alarmima ili primjenom elektroničkog lokota otežava se razbojništvo te se čuva sigurnost informacija.

Uz uređaje za zaključavanje prostorija postoje i uređaji za zaključavanje opreme. Baš kao i uređaja za zaključavaje prostorija i uređaja za zaključavanje opreme ima nekoliko vrsta od onih koji omogućuju fizičko zaključavanje kabela do onih koji ne zahtjevaju nikakve posebne utore na uređaju te u konačnici elektronička rješenja koja sadrže i alarmne sustave. Dakle postoji sistem koji se koristi za spajanje uređaja za zaključavanje kabela. Obično se na metalnom kablu nalazi neka vrsta lokota koja se ključem ili određenom kombinacijom može otvoriti. Bez ključa ili kombinacije ne može se kabel izvaditi prisilno te ostaje vidljiv trag namjere za otuđivanjem uređaja, pa time i informacija koje se nalaze na njemu. Osim putem kabla, alternativa su i mehanizmi zaključavanja za koje nije potreban poseban utor, pa se to čini primjerice preko priključka za pisač te imaju posebne vijke za osiguravanje na mjestu. Nešto nezgodniji način zaključavanja prijenosnog računala je s držačima koji sadrže neku vrstu lokota, a obuhvaćaju cijelo računalo te su pričvršćeni za nepomički objekt. Najjednostavni način na koji se zaključava oprema je putem pohranjivanja u za to predviđene ormariće.[58]

Sustavi za praćenje i otkrivanje lokacije nešto su sofisticiraniji od prethodno spomenutih elemenata za postizanje fizičke sigurnosti. Budući da se u uređajima poput prijenosnih računala ili raznih drugih prijenosnih medija nalazi velika količina povjerljivih informacija bitno je dobro paziti na njihovu sigurnost. S obzirom da bi šteta bila puno veća od one materijalne prirode, razni uređaji koji se koriste u poslovanju organizacije osigurani su na način da su u njih ugrađeni sustavi za praćenje i otkrivanje lokacije, a uloga im je detektirati krađu te otkriti položaj ukradenog uređaja ili druge opreme. Većina sustava za praćenje i otkrivanje lokacije funkcionira na principu internetske veze. Kada se prijavi krađa, ukoliko na prijenosnom računalu postoji takav sustav i ako je računalo u funkciji te na internetu, vlasniku/korisniku prijenosnog računala stižu podaci o tome gdje je računalo

[58] Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011, str. 133

locirano, slike osobe koja trenutno koristi otuđen uređaj, te se provodi tzv. tajno šifriranje svih podataka koje korisnik prethodno označi za tu namjenu. Ovisno o sustavu koji je ugrađen u otuđen uređaj razlikovati će se i povratne informacije koje dobiva korisnik o lokaciji svog uređaja.

Sve vrste zaštite informacijskih sustava jako su važne za očuvanje informacija, te nije dovoljno da se provodi samo jedna vrsta zaštite, već je potrebno koristiti kombinaciju fizičkih, organizacijskih, softversko – hardverskih mjera zaštite informacijsih sustava. suvremena poduzeća prepoznaju tu važnost te u svrhu učinkovitosti poslovanja te veće konkurentnosti koriste što veći broj mjera zaštite informacija u raznim kombinacijama ovisno o djelatnosti koju određena organizacija obavlja.[59]

[59] Ibidem, str. 151

5. SIGURNOSNI PLAN ZAŠTITE INFORMACIJSKIH SUSTAVA NA PRIMJERU INSTITUTA ZA HRVATSKI JEZIK I JEZIKOSLOVLJE

U daljnjem tekstu opisan je sigurnosni plan zaštite informacijskog sustava u praktičnom primjeru. Institut za hrvatski jezik i jezikoslovlje da bi što kvalitetnije zaštitio svoj informacijski sustav odlučio se internim aktom sustavno rasčlanitit problem zaštite informacijskog sustava te definirati ključne aspekte zaštite, načine pristupa zaštiti i odgovorne za njihovu provedbu. Što će biti izneseno u ovome poglavlju. Ključna stvar pri provođenju sigurnosne politike zaštite informacijskoga sustava jest da se u svakome trenutku točno zna tko je zadužen za obavljanje određenoga zadatka te tko odgovara za određeni segment opreme, odnosno računalnoga programa. Potrebno je, stoga bilo raspodijeliti zaduženja, obrazovati korisnike te oformiti stručna tijela za upravljanje sigurnošću. Djelatnici koji se u radu koriste računalima podijeljeni se na korisnike i davatelje informatičkih usluga.

Uvedeno je da pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- svu računalnu opremu koja se nalazi u prostorima Instituta
- administratore informacijskih sustava te pripadajuću tehničku službu
- korisnike, među koje spadaju zaposlenici, vanjski suradnici, volonteri i studenti
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže. Tako je definirano da svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Dužnosti korisnika su:

- pridržavanje pravila prihvatljivoga korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike
- izbor kvalitetne zaporke i njezina povremena promjena
- prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi.

Navedeno je da su korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To podrazumijeva da, ako ne postoji automatski sustav stvaranja sigurnosnih kopija, sami moraju izrađivati sigurnosne kopije. Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

Kada postoji više korisnika koji rabe određenu aplikaciju za obradu podataka, primjerice računovodstveni program, radi poboljšanja sigurnosti jedna osoba imenuje se glavnim korisnikom. U navedenome primjeru voditelj računovodstva bio bi glavni korisnik. Dok zaposlenici koji unose podatke odgovaraju za vjerodostojnost tih podataka, glavni je korisnik odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podatcima i za mjere sprečavanja izmjene podataka od strane ne autoriziranih osoba. Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih inačica, traži ugradnju sigurnosnih mehanizama itd.

Davateljima usluga smatraju se profesionalci koji se brinu o radu računala, mreže i informacijskih sustava. Ugovoreni davatelj informacijskih usluga za Institut za hrvatski jezik i jezikoslovlje je CS Computer Systems d.o.o. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

U Institutu za hrvatski jezik i jezikoslovlje ne postoji imenovani specijalist za sigurnost, već su članovi Službe za izdavaštvo i računalnu podršku odgovorni za koordinaciju korisnika s davateljem informatičkih usluga.

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući se istodobno o funkcionalnosti i sigurnosti. Svako računalo mora imati imenovanoga administratora, koji odgovara za instalaciju i konfiguraciju softvera. Ako napredni korisnici žele sami administrirati svoje osobno računalo, trebaju potpisati izjavu o

tome, nakon čega za njih vrijede sva pravila za administriranje računala. Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpa prema preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima. Posebnu pozornost administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štititi od neovlaštena pristupa. Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti. Administratori su dužni prijaviti incidente tehničkoj službi te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ako je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNetovu CERT-u. Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Kako bi ih Institut obvezao na poštivanje tih pravila, davatelji usluga potpisuju Izjavu o čuvanju povjerljivih informacija.

Djelatnik zadužen za upravljanje mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala. Ako je podržan rad na daljinu, kada se primjerice djelatnicima dopušta da s kućnoga računala ažuriraju podatke, mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove, s obzirom na mogućnost da ga koriste ne autorizirane osobe, članovi obitelji i slično. Povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove. Spajanje gostujućih računala na mrežu, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri podrazumijeva poštivanje institutskih pravila koja se odnose na sigurnost i zaštitu podataka. Ne dopušta se da oni po svom nahođenju priključuju računala na mrežu ustanove zbog opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnoga prometa, prikupljanja informacija itd. Institut može odrediti priključna mjesta, primjerice u određenim uredima, gdje je dopušteno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se s tog segmenta mreže dopre do ostalih računala u ustanovi. Institutska bežična mreža zaštićena je na način da se ne može bilo tko priključiti i služiti se njome te snimati promet. To se postiže metodama enkripcije i autentifikacije uređaja i korisnika.

Korištenje ilegalnoga softvera predstavlja povredu autorskoag prava i

intelektualnoga vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Institut zadužuje administratore za instaliranje softvera i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.

Prostor u ustanovi dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni te prostor u koji pristup imaju samo skupine zaposlenih, ovisno o vrsti posla koji obavljaju. Računalna oprema koja obavlja kritične funkcije, nužne za funkcioniranje informacijskoga sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dopušten samo ovlaštenim osobama. Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, što znači da električne instalacije moraju biti izvedene kvalitetno, da se koriste uređaji za neprekidno napajanje, a po potrebi i generatori električne energije. Treba predvidjeti i druge moguće probleme, poput poplava, požara i slično te poduzeti mjere da se oprema i informacije zaštite te da se osigura njihov što brži oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Ugovorom se regulira pristup vanjskim tvrtkama, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu treba obvezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla. Institut može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.
Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran videonadzor. Ako se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podatcima, Institut može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Instituta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Institut. Institut zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ako nisu na popisu ovlaštenih djelatnika.

Institut dijeli svu opremu u grupe prema zadaćama: Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.). Intranet je privatna mreža Instituta, a čine je

poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže. Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).

U prostorijama Instituta nalazi se i oprema CARNeta ili Ministarstva znanosti i obrazovanja, koja je dana na korištenje Ustanovi. Institut održava popis sve računalne opreme, s opisom ugrađenih komponenata, inventarnim brojevima itd. Institut se brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Manirom dobroga gospodara oprema se čuva od oštećivanja i otuđenja. Institut je dužna osoblju CARNeta dopustiti pristup opremi u vlasništvu CARNeta koja se nalazi u Institutu.

Za fizičku sigurnost opreme odgovoran je rukovoditelj Instituta. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu. Sva oprema koja se iznosi izvan prostorija Instituta podložna je provjeri kako bi se utvrdilo ima li oprema koja se iznosi potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

Kako bi se sačuvali podatci u slučaju nezgoda, poput kvarova na sklopovlju, požara ili ljudskih pogrešaka, potrebno je redovito izrađivati pričuvne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporučuje se izrada više kopija koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima. Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nezgoda. Povremeno se provjerava upotrebljivost pričuvnih kopija podataka te se izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na pričuvnoj opremi.

Institut zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim računalima te nad načinom korištenja računala. Nadzor se smije provoditi radi:

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

Nadzor smiju obavljati samo osobe koje je Institut za to ovlastio. Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No, u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi te se one mogu koristiti u stegovnom ili sudskom postupku.

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Instituta i priključena je u mrežu CARNet, na sav instalirani softver te na sve mrežne servise. Pravila su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Korisnici su dužni pomoći osobama zaduženima za nadzor informacijskih sustava tako što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora. Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni specijalistima za sigurnost pomagati pri istrazi. Pristup uključuje:

- pristup na razini korisnika ili sustava svoj računalnoj opremi
- pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Instituta, ili oprema Instituta služi za njezin prijenos
- pristup radnom prostoru
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Instituta

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu se mogu uskratiti prava korištenja CARNetove mreže i njezinih servisa.
Uz pravila nadvedena u Općoj sigurnosnoj politici po potrebi i u posebnim slučajevima primjenjuju se posebna pravila definirana pratećim dokumentima. Prateći protokoli pisani su kao upute za rješavanje konkretnih problema i mogu se mijenjati prema potrebi.

Prosječan korisnik nerijetko smatra kako se ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. No, kompromitiranjem jednoga osobnog računala u lokalnoj mreži ili jednoga korisničkog računa na poslužitelju napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Stoga je svaki korisnik dužan izborom zaporke i njezinom povremenom promjenom doprinositi zaštiti cijeloga sustava. Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dekriptirati jednostavne zaporke, dok u isto vrijeme većina ljudi ne može pamtiti složene zaporke od osam i više znakova. Svi zaposlenici Instituta za

hrvatski jezik i jezikoslovlje, suradnici i studenti koji se u svome radu služe računalima dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućuju.

Osim pravila za korištenje zaporki, djelatnicima je iznesen i mogući problemi u korištenju elektroničke pošte. Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-poštom u Institutu za hrvatski jezik i jezikoslovlje zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.

Protokol koji se koristi za prijenos elektroničke pošte, SMTP (Simple Mail Transport Protocol), nije od samog početka dizajniran da bude siguran. Dodatne probleme katkad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.

- Poruke putuju kao običan tekst te ih je lako presresti i pročitati ili čak izmijeniti njihov sadržaj.
- Lako je krivotvoriti adresu pošiljatelja tako da nikada niste sigurni tko vam je zapravo poslao poruku.
- Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.

Poruke namijenjene jednoj osobi lako se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi:

- (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki
- nemarom sudionika, koji ne traži dopuštenje za prosljeđivanje poruke
- slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply)

Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bi se primatelja obvezalo na diskreciju. U slučaju sigurnosnoga incidenta istraga

može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Institut se obvezuje čuvati povjerljivost takvih poruka, ali to ne može jamčiti ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke mora se tražiti dopuštenje njezina autora. Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje se može izložiti tužbi ne samo sebe, već i Institut.

Zbog svega nabrojenoga korištenje elektroničke pošte smatra se rizičnom djelatnošću te se korisnici obavezuju na pridržavanje određenih pravila koja su navedena niže:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite. Pridržavajte se netikete, pravila pristojnog ponašanja na Internetu, službenu email adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.
- Nije dopušteno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom te na taj način podliježe propisima o autorskome pravu i intelektualnome vlasništvu. Nitko nema pravo poruke koju su poslane njemu osobno proslijediti dalje bez dopuštenja autora, odnosno pošiljatelja.
- Sve poruke pregledat će automatska aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Ustanova zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke koje su dio poslovnoga procesa treba arhivirati i čuvati propisani vremenski

period kao i dokumente na papiru

Pri zapošljavanju novog djelatnika, rukovodilac će zatražiti od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa. Pri prestanku radnoga odnosa, rukovodilac je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkoga računa.

Pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike, volontere i studente koji imaju otvoren korisnički račun na poslužitelju Instituta.

Protiv korisnika koji ne poštuju ova pravila Institut može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Također uveden je i protokol po pitanju antivirusne zaštite. Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka. Nove generacije virusa izuzetno su složene i opasne, sposobne da prikriju svoju nazočnost, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na internet te otvoriti kriptiran kanal do čijeg računala kako bi hakeri preuzeli kontrolu nad njim. Stoga zaštita od virusa više nije stvar osobnog izbora, već obveza Instituta, administratora računala i svakog korisnika. Institut za hrvatski jezik i jezikoslovlje propisuje da je zaštita od virusa obvezna i da se provodi na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika.

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju s centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika. Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ako iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti sistemskog inženjera. Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu te na taj način izazove štetu bit će stegovno kažnjen.

Svaki zaposlenik ili suradnik Instituta za hrvatski jezik i jezikoslovlje dužan je

prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd. Incident se prijavljuje administratoru ili korisničkoj službi Instituta. Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema. Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima. Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr.

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedopušten način, mogu izlistati sadržaj korisničke mape, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (npr. dokumenata ili poruka e-pošte). Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom ustanove, uz poštivanje sljedećih pravila:

- Istragu provodi jedna osoba, ali uz nazočnost svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne načine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije se načini kopija zatečenog stanja (npr. na vanjsku memoriju, CD…), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd).
- Dokumentira se svaka radnja tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- U istrazi se napiše izvještaj kako bi u slučaju potrebe mogao poslužiti kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se tako da im pristup imaju samo ovlaštene osobe.
- Institut može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Svrha je istrage da se odredi uzrok nastanka problema te da se iz toga izvuku zaključci o tome kako spriječiti ponavljanje incidenta ili se barem bolje pripremiti za slične

situacije. Ako je uzrok sigurnosnom incidentu bio ljudski čimbenik, protiv odgovornih se mogu poduzeti sankcije. Institut može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili pristup podatcima. Ako je incident izazvao zaposlenik vanjske tvrtke, Institut može zatražiti od vanjske tvrtke da ga ukloni s popisa osoba ovlaštenih za obavljanje posla na Institutu. U slučaju teže povrede pravila sigurnosne politike Institut može raskinuti ugovor s vanjskom tvrtkom.

Ovakvim internim aktom institut je imao namjeru dodatno utjecati na djelatnike ne bi li oni na taj način spoznali važnost i njihov utjecaj na sigurnost informacijskog sustava instituta.

6. ZAKLJUČAK

U današnjem poslovanju informacijski sustavi se smatraju sastavnim dijelom poslovanja. Svaki poslovni sustav se sastoji od niza informacija potrebnih za poslovanje kojima upravlja informacijski sustav. Prikupljanjem i obradom podataka postiže se temelj za donošenje odluka koji utječu na cjelokupno poslovanje.

Ovim radom se željelo prikazati osnove za uspostavu i zaštitu informacijskog sustava. Činjenica je da postoji određena razina opasnosti za sustav pogotovo u suvremenom poslovanju pa organizacije moraju biti toga svjesne i biti spremne na reakciju protiv mogućih prijetnji.

Postoji mnogo vrsta informacijskih sustava, najšira podjela je na informacijske sustave prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija. Samim time što je toliko podjela, a još više podjela unutar tih glavnih vidi se važnost funkcioniranja tog dijela u poslovnom sustavu. Odabirom pravog i odgovarajućeg informacijskog sustava za poslovanje bitno utječe na cjelokupno poslovanje neke organizacije, ali je potrebno konstantno provjeravati rad sustava radi održavanja prihvatljive razine rizika.

Modernizacijom i informatizacijom poslovanja sigurnosni rizik se povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi konkurentnost poslovne organizacije.

Zanemareni sustav informacijske sigurnosti, u smislu ne kontroliranja problema sigurnosti, vrlo lako može postati žrtvom napada. Sigurnost sustava bi se trebala periodično kontolirati, tražiti načine kako sustav učiniti još sigurnijim, otpornijim te implementirati dodatne sigurnosne kontrole koje savjetuju stručnjaci za informacijsku sigurnost.

U Republici Hrvatskoj postoji velik broj zakona, pravila, procedura kojima se upravlja informacijskom sigurnošću, ali su zaposlenici slabo odnosno nedovoljno educirani pa se informacije ne štite na prikladne načine. To se u novije vrijeme pokušava promjenit internim aktima poduzeća ili institucija kao što je prikazano u praktičnom primjeru te bi to

u budućnosti trebalo doprinjeti edukaciji zaposlenika i korisnika u važnost odgovornog ponašanja u pristupu aspektima informacijske sigurnosti na koji oni mogu utjecati.

LITERATURA

Knjige i udžbenici:

1. Antoliš, K.,et al, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010.
2. Bocij, P. I dr., Business Information Systems; Technology, Development & Management for the e-business, 2006.
3. Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004.
4. Garača, Ž., Informatičke tehnologije, Sveučilište u Splitu, Split, 2007.
5. Hadjina, N., Zaštita informacijskih susava. Zagreb: FER, 2009.
6. Klasić, K., Klarin, K., Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009.,
7. Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb : Sinergija - nakladništvo, 2001.
8. Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011.
9. Pejić Bach, M. i dr., Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Zagreb, 2016.
10. Spremić, M., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, 2017.
11. Srića, V. i suradnici, Menedžerska informatika, MEP Consult, Zagreb, 1999.
12. Srića, V. i dr., Uredsko poslovanje: Strategija i koncepti automatizacije ureda, Sinergija, Zagreb, 2003.
13. Šehanović, J., Hutinski, Ž., Žugaj, M., Informatika za ekonomiste, Tiskara Varteks, 2002.

Internet izvori:

1. http://azop.hr/prava-ispitanika/detaljnije/zastita-osobnih-podataka
2. http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/dongle.html
3. http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html
4. http://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html
5. http://www.carnet.hr/o_carnetu/o_nama
6. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf
7. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf
8. http://www.digitconsulting.rs/index.php/licenciranje-microsoft/licenciranje/sofverska-licenca.html
9. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-28.pdf
10. http://www.pfri.uniri.hr/~tudor/materijali/Informacijski%20sustavi,%20baze%20podataka.html
11. http://www.unizd.hr/Portals/1/Primjena_rac/Poseban_program/Predavanja/sigurnost_predavanje.pdf
12. https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka
13. https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
14. https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
15. https://www.zsis.hr/default.aspx?id=13

POPIS SLIKA

POPIS TABLICA