Izvori i oblici prijetnji sustavu sigurnosti informacija

Uskok, Ivan Krešimir

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studiji

Poslovanje i upravljanje

Ivan Krešimir Uskok

IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA

PREDDIPLOMSKI ZAVRŠNI RAD

Zaprešić, 2021.

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Preddiplomski stručni studiji

Poslovanje i upravljanje

Usmjerenje Menadžment u uredskom poslovanju

PREDDIPLOMSKI ZAVRŠNI RAD

IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA

Mentor:
dr.sc. Dragutin Funda, prof. v. š.

Student:
Ivan Krešimir Uskok

Naziv kolegija:
UPRAVLJANJE KVALITETOM U UREDSKOM POSLOVANJU

JMBAG studenta:
0269129323

SADRŽAJ

SAŽETAK

U modernom dobu važnost poznavanja informacijskog sustava i njegove zaštite danas je od krucijalne važnosti, stoga ne čudi kako je potreba za edukacijom sve veća. Važnost proizlazi iz toga što primjerice ugroženost informacijskog sustava neke organizacije može rezultirati negativnim posljedicama za tu organizaciju, ali i okolinu u kojoj je ta organizacija. Kako bi odabrali posebno adekvatne mjere i metode zaštite potrebno je objašnjenje svih vrsta oblika i izvora prijetnji informacijskom sustavu koje bi mogle narušiti glavne sigurnosne aspekte i uzrokovati velike neželjene financijske posljedice. Upoznavanjem sa situacijom prijetnje sustavu i raznih metoda odnosno softvera zaštite otvara se šira slika u pripremi informacijskog sustava na obranu od zlonamjernih pokušaja krađe povjerljivih informacija.

Ključne riječi: informacijski sustav, mjere i metode zaštite, sigurnosni aspekti, prijetnje, oblici i izvori prijetnji.

Title in English: Sources and forms threatening the information security sistem

ABSTRACT

In the modern age, the importance of knowledge of they information system and his protection is of crucial importance today, so we should not hear that the need for education is growing. The importance stems from the fact that, for example the threat to an organizaion's information system can result in negative consequences for the organization, but also the circumstances in which that organization finds itself. As we have selected particulary adequate measures and methods of protection, it is necessary to explain all types of forms and sources of threats to the information system that could order the main security aspects and cause major undesirable financial consenquences. Getting acquainted with the threat situation of the system and various methods, software of protection opens a broader picture in the preparations of the information system for defense against malicious attempts to steal confidential information.

Key words: Information system, protection measures and methods, theats, forms and threats, security spects.

1. UVOD

Informacijsku sigurnost zahtijevaju razne organizacije danas (vojska, bolnica, tvrtke, vlada) koje posjeduju veliku količinu povjerljivih informacija koje je potrebno zaštiti od različitih izvora i oblika prijetnji. Prijetnje se mogu podijeliti na prirodne prijetnje, namjerne, nenamjerne i oprema, kako bih se zaštitili od navedenih prijetnji potrebna nam je edukacija o zaštiti sigurnosti informacijskog sustava.

1.1 Predmet i cilj rada

U današnjem svijetu tehnologija i informatizacije postoji veliki broj javnih i privatnih organizacija koji posjeduju povjerljive informacije koje je potrebno zaštiti od zloupotrebljavanja ili krađe informacija kako bi se sačuvala njihova tajnost i povjerljivost. Gubitak povjerljivosti informacija predstavlja štetno djelovanje na organizacije, zbog toga što će se naći u teškoj poziciji negativnih radnji vezanih za protok povjerljivih informacija na neadekvatnim mjestima i vremenu. Cilj ovog završnog rada je objasniti razne oblike i izvore prijetnji informacijskom sustavu kako bi se u konačnici pospješila učinkovitost organizacije te kako bi se bilo u korak s vremenom i bilo u mogućnosti odgovoriti modernim prijetnjama i izazovima.

1.2 Izvori i metode prikupljanja potrebni informacija za rad

Izvor podataka koji su korišteni za ovaj završni rad su knjige, web-mjesta i pravni propisi. Metode prikupljanja podataka korištene su sljedeće znanstvene metode: metoda analize i sinteze, povijesna metoda, metoda deskripcije, metoda dokazivanja, metoda indukcije i dedukcije.

1.3 Sadržaj i struktura rada

Rad se sastoji od šest cjelina. U prvo cjelini prikazan je opis osnovnih pojmova (Što je informacija, sustav i informacijski sustav), povijest, podjela i vrste informacijskog sustava. Druga cjelina opisuje sigurnost informacijskog sustava koji sadrži (zakone, mjere i standarde informacijskih sigurnosti). Treća cjelina predstavlja oblik i vrste prijetnje informacijskom sustavu i kod pete cjeline imamo objašnjene moguće zaštite informacijskog sustava i kako one djeluju. Šesta cjelina predstavlja zaključak ovog završnog rada.

2. INFORMACIJA I INFORMACIJSKI SUSTAVI

Svrha ovog poglavlja je ukazati kako je za efikasno obavljanje gotovo svih modernih poslova potrebno detaljno analiziranje informacija i podataka. Neovisno o kojoj je vrsti poslova riječ, organizacije se danas služe informacijskim sustavima koji prikupljaju razne tipove podataka i posljedično ih prerađuju u informacije koje dalje koriste u poslovnim procesima. Iz navedenog je moguće zaključiti kako je informacijski sustav ključan element poslovanja, a možemo ga nazvati i okosnicom za djelovanjem u dinamičnom poslovnom okruženju. U većini slučajeva informacijski sustavi dijele iste elemente pa tako primjerice uobičajeni informacijski sustav se sastoji od sustava za obradu transakcija, sustava koji služi za podršku odlučivanju, upravljačkim izvještajnim sustavom te sustavom uredskog poslovanja što će se u nastavku ovog rada detaljnije obraditi.

2.1 Informacijski sustav

Informacija predstavlja obrađeni podatak koji nam posreduje neku novost odnosno primatelju te informacije koji je može primiti u bilo kojem obliku (audio, pisanom i vizualnom) kako bi stvorio stvarnu vrijednost za sve njegove buduće odluke. Kada spominjemo informaciju, također trebamo znati kako je ona postala u današnjem svijetu tehnologije jako bitna jer posjedovanje bitnih informacija koja donosi veliku prednost u poslovanjima. Informaciju kao podatak smo u mogućnosti koristiti više puta od strane drugih korisnika, zbog toga pohranjivanje i čuvanje podataka postaje nam od velike važnost jer nam može zatrebati u bilo kojem trenutku.

Sustav je svaki uređeni skup od najmanje dva elementa koji zajedno interakcijom ostvaruju funkcije cjelina (Klasić, Klarin, 2009). Svaki sustav ima postavljen cilj, a to predstavlja transformacije određenih ili različitih vrsta ulaza u izlaz. Transformiranje se izvršava na način drugih procesa koji se međusobno razlikuju.

Kako bi se pojasnio transformacijski odnos ulaza i izlaza u nastavku slijedi slika 1

Slika 1 Transformacija odnosa ulaza i izlaza podataka

Izvor: izrada autora prema Knežević, U., 2018, Poslovni informacijski sustavi u proizvodnim poduzećima, dostupno na: https://repozitorij.unipu.hr/islandora/object/unipu%3A2946/datastream/PDF/view , pregledano 19.6.2021.

U navedenom prikazu moguće je uočiti „ulaz“ pod kojim se podrazumijeva ulaz podatka u poslovni sustav, a njegovom preradom, transformacijom i obradom dobivamo izlazni podatak, odnosno informaciju koja je korisna za neku organizaciju.

Informacijski sustav predstavlja dio poslovnog sustava kojem je uloga prikupiti potrebne informacije koje su vezane za donošenje odluka i upravljanje poslovanja. Zapravo informacijski sustav ima zadatak prikupiti, obraditi, čuvati, oblikovati i razvrstavati podatke poslovnog sustava kako bi proizveo informaciju na temelju prikupljenih podataka. Podatak predstavlja jedinu cjelinu koja se pretvara u informaciju kada dobije nekakvo značenje (Pavlić, 2011). Primjer podatka: Marko 12, 01, Zagreb, 1992. Bilo koji podatak koji je naveden u primjeru može predstavljati bilo što, npr. broj 12 može se predstaviti kao 12 godina ili 12 kuna, ako mi dodamo značenje tom podatku on tada postaje informacija. Kada podatak koji smo naveli u primjeru organiziramo i obradimo tada predstavlja informaciju koja nam govori da je Marko rođen 12.1.1992 godine u Zagrebu. Na temelju primjera vidimo kako podatak predstavlja tvrdnju o nečemu iz stvarnog svijeta, dok informacija predstavlja interpretaciju podatka koja ima subjektivno značenje za primatelja poruke. Informacijski sustav zapravo upotrebljava informacije na način da ih proizvodi nakon toga obrađuje kako bi prikazao na način koji će biti razumljiv primatelju kako bi na temelju njih mogao donijeti odluke.

Ciljevi informacijskih sustava različiti su za različite radne razine. Najčešća podjela je na tri radne razine: razina izvođenja (operativnu razinu), razina upravljanja (taktička razina) i razina odlučivanja (strateška razina) (Klasić i Klarin, 2003). U razinu izvođenja možemo uvrstiti procese koji su vezani uz osnovne djelatnosti, a cilj informacijskog sustava predstavlja povećana produktivnost na toj razini. Upravljačka razina ima odgovornost za organiziranje, uspješno otklanjanje smetnji i praćenje uspješnosti. a cilj informacijskog sustava je u povećanoj učinkovitosti rada. Informacijski sustav na razini odlučivanja ima cilj osigurati razvoj zbog toga što ta razina je odgovorna za postavljanje poslovnih ideja i ciljeva.

2.2 Povijest informacijskog sustava i njegov razvoj

Kada je riječ o informacijskom sustavu taj pojam najčešće asocira na korištenje računala, no potrebno je imati na umu kako to nužno ne uvjetuje da nam je potrebno računalo za potrebe izgradnje informacijskog sustava. Informacijski sustav predstavlja svaki sustav koji se koristi poslovanju i može se izgraditi bez primjene računala i tako ostvariti prikupljanje, razvrstavanje, obrađivanje i čuvanje podataka.

2.2.1 Faze obrade podataka

Prema načinu obrade podataka tijekom povijesti razlikujemo nekoliko razdoblja: ručna obrada podataka, mehanička obrada podataka, elektromehaničke obrada podataka i elektroničke obrada podataka (Razvoj obrade podataka kroz povijest). Sve četiri navedene faze prikazuju nam kako su se kroz povijest razvijale i neke od njih se danas primjenjuju u poslovnome svijetu:

1. Faza ručne obrade podataka: predstavlja nam već sam pojam „ručne“ da u toj fazi se primjenjuje rad ruku, medij za pohranu podataka i sredstvo za pisanjem. Tada u vrijeme ručne obrade podataka mediji je predstavljao kamen na kojem su se klesali razni simboli. Ovakav način obrade podataka predstavlja spor način obrade podataka ali i dovodi do upitnosti jesu li točni podatci.

2. Faza mehaničke obrade podataka: pojavljuje se sredinom 17. stoljeća kao posljedica razvoja znanosti i tehnike koja je tada pokazala bržu, učinkovitiju i pouzdaniju obradu podataka u odnosu na ručnu obradu. Za mehaničku obradu podataka koristili su se tada računski i pisaći strojevi. Isto tako možemo naglasiti francuskog filozofa i matematičara, Blaise Pascal izradio je mehanički stroj koji je mogao relativno brzo zbrajati i oduzimati velike brojeve (Računala kroz povijest).

3. Faza elektromehaničke obrade podataka: pojavljuje se u drugoj polovici 19. stoljeća kada je raspisan javni natječaj u SAD-u za konstruiranjem uređaja kojim se podaci stanovništva mogli obraditi u što bržem i kraćem roku. Fazu elektromehaničke obrade podataka često su nazivali mehanografske ili birotehničke obrade podataka zbog pobjede Hermanna Holleritha koji je na raspisanom natječaju predložio korištenje bušenih kartica, a za njihovu upotrebu koristio se elektromehanički stroj.

U nastavku slijedi prikaz slike 2 elektromehaničkog stroja

Slika 2 Elektromehanički stroj

Izvor: preuzeto sa: Columbia University Computing History, 2001., Hollerith 1890 Census Tabulator, dostupno na: http://www.columbia.edu/cu/computinghistory/census-tabulator.html pregledano 19.6.2021

Priložena slika prikazuje elektromehanički stroj koji je izumljen od strane Hermana Hollerith u svrhu bušenja kartica s podacima iz popisa stanovništva, koji je nazvan sortiranim strojem. Elektromehanički stroj pripada prvom modernom stroju za obradu podataka koji nije obavljao aritmetičke operacije već prebrojavanje podataka.

4. Faza elektroničke obrade podataka: počinje 1944. godine s razvojem ENIAC-a (Elektronički numerički integrator i računalo) koje se smatra prvi programibilnim elektroničkim računalom. Prednosti faze elektroničke obrade podataka predstavljaju mogućnosti obrade velike količine podataka u kratkom vremenskom periodu (Povijest.hr, 2021.). Mogućnost pohranjivanja podataka i povezivanja operacija kao što su: prijenos i obrada podataka, integracija obrade, grafika, slike i zvuk. Danas se smatra jednim od najšireg načina obrade podataka Internet koji također svrstavamo u fazu elektroničke obrade podataka.

Slika 3 ENIAC računalo

Izvor: preuzeto iz članka: ENIAC programibilno računalo, 2014. dostupno na: https://www.racunalo.com/eniac-programabilno-racunalo-postalo-eksponat-u-muzeju/ 19.6.2021

ENIAC se smatrao jednim od najtežih računala ikada, njegova masa iznosila je 27 tona. On se sastojao od 70.000 otpornika, 10.000 kondenzatora, 1.500 prekidača i sadržavao je više od 18.000 vakuumskih crijeva. Oko 2.000 cijevi se zamjenjivalo svaki mjesec od strane tima šest tehničara.

2.3 Dijelovi informacijskog sustava

Dijelovi informacijskog sustava sastoje se od 6 glavnih dijelova (hardware, software, orgware, lifeware, neware, dataware) od kojih svaki predstavlja odvijanje glavnih osnovnih funkcija sustava koje ću prikazati u sljedećoj tablici zajedno sa njihovim opisima. U nastavku kroz tablični prikaz slijedi opis šest glavnih dijelova informacijskog sustava (Gospočić, 2018):

Tablica 1 Dijelovi informacijskog sustava i njegova djelovanja

Dijelovi informacijskog sustava	**Opis dijelova**
Hardware	Predstavlja komponentnu sustava koja je vezana za ostale elemente koji čine materijalnu osnovicu računala
Software	Predstavlja nematerijalni dio informacijskog sustava koji služi kao skup programa u izvedbi primanja, obrade, prikazivanja i pohrani podataka i informacija
Podatci	Ulaz koji je sustavu potreban za generiranje informacija

Lifeware (ljudi)	Predstavlja zaposlenike koji su stručnjaci kod analiziranje informacijski potreba organizacije, održavaju informacijske sustave i opremu, kreiraju informacijski sustav
Netware (komunikacija)	Povezanost elemenata i dijelova sustava u cjelinu, odnosno omogućava hardversko-softversko komuniciranje putem bržeg primanja i slanja podataka unutar mreže u raznim oblicima (slike, zvuka i teksta)
Procedura	Predstavlja skup pravila kod postizanja sigurnosti i optimalnog rješenja pri obradi podataka i informacija.

Izvor: Izrada autora prema Gospočić, Z., Analiza aplikacijskih rješenja informacijskog sustava mrežnog operatora, 2018. str. 2-3 https://zir.nsk.hr/islandora/object/fpz%3A1319/datastream/PDF/view , pregledano 19.6.2021

U prikazanoj tablici prikazana je zajednička povezanost svih dijelova informacijskog sustava, i njihova važnost za pravilno funkcioniranje kako bi ostvarili poslovne ciljeve informacijskog sustava.

2.4 Vrste informacijskog sustava

Postoji povećani broj kriterija za podjelu informacijskog sustava koji su često korišteni prema podjelama konceptualnom ustrojstvu poslovodstva, također prema namjeni ili prema modelu poslovnih funkcija.

Nastavno slijedi tablični prikaz 2. koji prikazuje vrste informacijskog sustava.

Tablica 2 Vrste informacijskog sustava

Ustroj poslovodstva	**Vrste informacijskog sustava**
Poslovodstvo - *strateški nivo*	Odlučivanje **sustav potpore**
Izvršno vodstvo - *taktički nivo*	Upravljanje **izvršni informacijski sustavi**
Operativno vodstvo - *operativni nivo*	Izvođenje **transakcija**

Izvor: izrada autora prema Klasić, K., i Klarin K., 2009., str 23., Vrste informacijskih sustava prema konceptualnom ustrojstvu poslovodstva pregledano 19.6.2021

Prema prikazanoj tablici 2 na operativnom nivou odnosno razini imamo prikaz namijene transakcijskog sustava. Uloga je izvođenje procesa osnovnih djelatnosti kojima je zadatak evidentirati korake u proizvodnji. Taktička razina ima namjenu izvršni informacijski sustav, prikazom rezultata potrebna su izvješća upravljanja. Strateški dio razine predstavlja sustav potpore odlučivanja.

2.4.1 Informacijski sustav prema namjeni

Informacijski sustavi prema namjeni se dijele na četiri podsustava: sustav za obradu podataka, sustav podrške uredskom radu, sustavi podrške u odlučivanju i ekspertni sustavi. Sustav obrade podataka ima zadatak unošenja, obrade i pohrane podataka o stanju sustava i poslovnim događajima. Kod ovakvih unošenja podataka u sustav pohranjuje se u bazama podataka, a pretragom traženih podataka dolazi se uz pomoć posebnih programa za pretraživanje. Kod obrade podataka postoje posebna izvješća čija je svrha izvođenje procesa osnovne djelatnosti koji također služe za upravljanje.

Sustav podrške uredskom radu dijelimo na dvije kategorije: podrška za administrativne poslove (potpora za rad prezentacija i sl.) i podrška ljudskog komuniciranja koji obuhvaća rad sa (e-mailom ili telefoniranjem). Sustav podrške odlučivanja koristimo kroz različite metode kojima dobivamo potrebne informacije koje su potrebne za odlučivanja i kao podrška pojedincu ili grupi. Ekspertni sustav primjenjujemo kao potporu ekspertima koji ujedno služe za rješavanje problema konfiguriranja i dijagnosticiranja sustava. Ekspertni sustav odnosi se na podršku kod učenja, podršku znanstvenom i stručnom radu ili kod izrade projekata. (Klasić i Klarin, 2009.)

Prikazom najvažnijih obilježja vrsta informacijskog sustava prema namjeni prikazana je slika o složenosti pojedine kategorije. Područje primjene informacijskog sustava prikazan je kao složeniji od drugih, zbog obilježja sustava obrade podataka problemska područja prikazanih procesa mogu se funkcionalno pratiti. Kod sustava uredskog poslovanja obilježja strukturiranih uredskih poslova su relativno dobro složeni, a sustav podrške obilježen je djelomičnim funkcionalnim procesom kod donošenja odluka. Ekspertni sustav predstavlja najsloženije područje primjene čija su obilježja uska problemska područja kod kojih je potrebno imati ekspertno znanje. Skladište informacija i podataka prikazuje razliku koja je ovisna o informacijskom sustavu. Od četiri navedena informacijska sustava ima različitu vrstu i oblik izlazni informacija koji prikazuju obradu podataka putem analitičkih i zbirnih izvješća. Informacijski sustavi uredskog poslovanja imaju izlazne informacije koje prikazuju sadržaj poruka, dokumenata i ostalih objekata, također prikazanost informacija o stanjima objekata

uredskog sustava. Složenost prikaza izlaznih informacija prikazan je u sustavu podrške odluka gdje se nalazi gradački, numerički i tekstualni prikaz informacija za donošenje odluka. Ekspertni sustav spada pod četvrti informacijski sustav koji ima prikaz izlazne informacije u obliku rezultata ekspertize sa karakteriziranom načinu rješavanja problema (Bukovac, 2016).

2.4.2 Informacijski sustavi prema modelu poslovne funkcije

Model poslovne funkcije spada pod treću kategoriju informacijskog sustava kojih može biti u broju koji ovisi koliko poslovnih funkcija se obavlja u poduzeću. Model sustava prema modelu poslovne funkcije se sastoji od različitih informacijskih podsustava:

- Informacijski podsustav (IPS) planiranja i analiza poslovanja
- IPS upravljanje trajnim proizvodnim dobrima
- IPS upravljanje ljudskim resursima
- IPS upravljanje financijama
- IPS nabave materijala i sirovina
- IPS prodaja proizvoda i usluga
- IPS računovodstva
- IPS istraživanje i razvoj

Kod različitih poslovnih sustava postoje različite primjene informacijske tehnologije koja se dijeli na četiri glavna dijela (Panian i Ćurko, 2010):

1. Operativni informacijski sustav predstavlja sustav o kojem ovisi uspjeh tekućeg poslovanja. Sustav se koristi kod trgovina.
2. Potporni informacijski sustav je koristan, ali nema utjecaj na poslovnih uspjeh. U takvom sustavu prikazana je jako mala ovisnost o tehnologiji. Sustav se koristi u građevinarstvu kao potporni informacijski sustav.
3. Strateški informacijski sustav igra veliku ulogu vezanu za poslovnu strategiju budućnosti zbog primjene informacijske tehnologije koja služi za brzu obradu i velike količine podataka potrebnih za poslovanje. Strateški informacijski sustav koristi se na primjer kod rezervacije putnički karti za prijevoz.
4. Izgledni informacijski sustav predstavlja mogućnost utjecaja na uspjeh u budućnosti, također prikazuje malu ovisnost o tehnologiji, ali utjecaj informatike na poslovni rezultat je vrlo visok. Primjena ovakvog sustava najčešće se koristi kod osiguratelјeve djelatnosti zbog toga što osiguravatelj može fizički odnosno ručno izdati policu

osiguranja ili obraditi štetu, kada se radi o izračunima premije tada je potrebno prikupiti i obraditi veličinu podataka.

Kod svakog poslovnog sustava pripada neki informacijski podsustav koji ovisi o djelatnosti poduzeća kako bi odredio tip informacijskog podsustava, bilo to da se radi o trgovini, građevinarstvu, rezervaciji ili izdavanje police osiguranja. Poduzeća često izgrade potporni informacijski sustav koji s vremenom i rastom poduzeća prelazi u izgledni informacijski sustav kako bi omogućio dugoročno i uspješno poslovanje.

Kvaliteta daljnje obrade i izvještavanja podataka ovise o kvalitete informacijskog sustava. Kako je informacijski sustav postao dio poslovnog sustava njegov rezultat uspješnosti poslovanja poduzeća ovisi o kvaliteti informacija koje obradi, zato je važan informacijski sustav jer bez njega poduzeće teže postaje uspješno čak i mogućnost neuspjeha u budućnosti. Kako bi informacijski sustav bio uspješan potrebno je imati dovoljne količine kvalitetnih i definiranih poruka koje je potrebno obraditi, jer bez toga nema ni kvalitetne podrške klijentima.

Kako bi informacijski sustav bio kvalitetan i koristan poduzeću mora sadržavati i zadovoljiti nekoliko načela (Klasić i Klarin, 2009):

- Informacijski sustav je model poslovne tehnologije organizacijskog sustava
- podaci su resursi 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

Kroz navedena načela informacijski sustav ako ih sadržava i zadovoljava u potpunosti svoju zadaću, a u to spada: prikupljanje, obrada, pohrana te distribucija podataka svima kojima je to potrebno. Informacijski sustav ciljano unapređuje poslovanje i ostvaruje pozitivan poslovan rezultat.

3. SIGURNOST I INFORMACIJSKA SIGURNOST U POSLOVANJU

S obzirom da je tema ovog rada sigurnost informacijskog sustava, prije nego definiramo sigurnost informacijskog sustava, moramo znati što pojam sigurnost što predstavlja i kako ga definiramo.

Pojam sigurnost predstavlja proces održavanja prihvatljivog nivoa rizika, što znači da sigurnost nije proizvod ili završno stanje. Kod zaštite informacijskih sustava postoji nekoliko osnovnih pravila koje je važno naglasiti i nabrojati:

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

Poslovna organizacija treba prikladno zaštiti svoje informacije koje smatraju pod imovinom organizacije. Svaka organizacija trebala bi se zaštiti zbog toga jer se nalaze u okruženju distribuiranosti poslovne okoline i tada postaju izložene ranjivostima i većem broju prijetnji od napada. Informacija u bilo kojem obliku pohranjena uvijek treba biti prikladno zaštićena, zbog toga jer tajnost informacija i ispravnosti daje poslovanju moć prema napretku.

3.1 Informacijska sigurnost u poslovanju

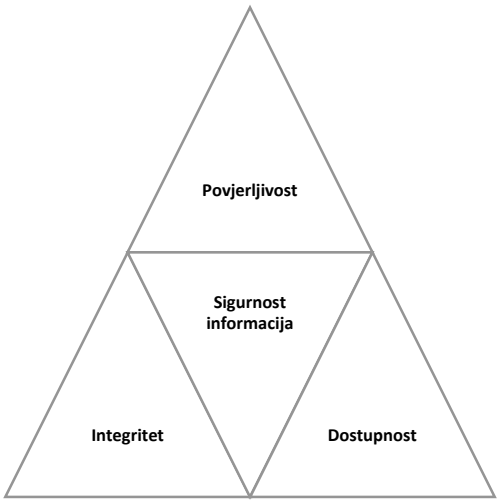
Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda (Republika Hrvatska UVNS). Informacijska sigurnost u današnjem poslovanju postaje sve važnija zbog velikih protoka količine informacija među subjektima, ali ujedno i izlaganje broju prijetnji. Kako bi se poslovanje zaštitilo od velikog broja prijetnji informacijski sustav ima postavljene ciljeve: zaštita informacija od neovlaštenog pristupa, zaštita informacija od velikog broja prijetnji u svrhu smanjenja poslovnog rizika, te osiguravanja poslovnog kontinuiteta zbog povećanja broja poslovnih prilika i povrata od investiranja. Informacijska sigurnost postiže se učinkovitom primjenom kontrola kao što su: razni procesi, procedure i sigurnosna politika. Navedene kontrole je potrebno implementirati, nadzirati, pregledavati, poboljšavati kako bi se zaštitilo i osiguralo poslovanje organizacije.

Poslovne organizacije se susreću sa mnogobrojnim prijetnjama poput: računalnih napada i prijevara, špijunaža, sabotaža, vandalizam, požar, poplava i slično, također sve češće prisutne opasnosti nanesene organizaciji u obliku zloćudnog koda, računalnih prijevara (hakiranje) i uskraćivanje usluga. Zbog takvih opasnosti kako bi se na vrijeme zaštitila javna i privatna organizacija informacijska sigurnost postaje vrlo poznat pojam, zbog toga što postoje javne i privatne računalne mreže koje je moguće dijeliti informacije i tako otežavaju kontroliranje protoka informacija. Kod informacijske sigurnosti potrebno je sudjelovanje svih zaposlenika pa čak i konzultanti izvan organizacija.

3.2 Aspekti informacijske sigurnosti

Tri glavna aspekta informacijske sigurnosti su: povjerljivost, integritet i dostupnost.

U nastavku slijedi slika 4. na kojem su prikazana tri aspekta informacijske sigurnosti.



Slika 4 Sigurnosni trokut informacija

Izvor: izrada autora prema Tyson, J., 2019., The CIA Triad, dostupno na https://blog.jamestyson.co.uk/the-cia-and-dad-triads, pregledano 19.6.2021

Povjerljivost spada u prvi aspekt informacijske sigurnosti koji se odnosi na provođenje mjera osmišljenih kako bi neovlaštenim osobama onemogućile pristup osjetljivim podatcima. Najveću pažnju ovaj aspekt posvećuje na identifikaciji i autentifikaciji korisnika. Neke od prijetnji koje se odnose na povjerljivost podataka su: hakiranje, nezaštićeno preuzimanje datoteka, lokalne mreže, trojanski konji i sl. Aspekt povjerljivosti se dijeli na kontrolu pristupa

(jednostavna metoda zaštite) i metoda enkripcije (malo složenija metoda koja predstavlja ovlaštenim korisnima tajni ključ za uvid informacija.)

Integritet spada pod brojem dva u sigurnosnoj piramidi aspekata informacijske sigurnosti koja predstavlja zaštitu na način zabrane izmjena podataka bez odgovarajućeg ovlaštenja. Također za integritet možemo reći kako on uključuje održavanje točnosti, dosljednosti i pouzdanosti podataka. Integritet podataka osigurava se na način mjera poput potrebne dozvole za datoteku i model kontrole pristupa, u koliko neovlašteni korisnik napravi bilo kakve promjene na podatcima može dovesti do gubitka integriteta. U tome slučaju izvorni podatci mogu biti nepovratno izgubljeni.

Dostupnost spada pod brojem tri aspekta sigurnosti informacija koji predstavlja upravo dostupnost podataka i informacija koje ovlaštenim osobama pružaju pristup podatcima kad god to požele. Dostupnost se može narušiti na nekoliko načina: uskraćivanjem usluga zbog gušenja na mrežnoj opremi, nemogućnost procesuiranja podataka zbog prirodnih katastrofa poput potresa, poplava ili požara. Ključni dio osiguravanja visoke dostupnosti je provođenje snažnih postupaka oporavka od katastrofe u slučaju opasnosti.

Osim navedena tri aspekta u novije vrijeme postoje razmišljanja kako bi u sigurnosni trokut trebalo ubaciti još neke aspekte, a to su dokazivost, autentičnost, neporecivost, no postoje i protivnici ove teze jer smatraju da su ova tri aspekta već uključena u osnovi sigurnosnog trokuta (Antoliš et al., 2010).

Kako bi sva tri navedena aspekta sigurnosti informacija bili učinkoviti i djelotvorni u svome radu potrebno je da zadovolje navedene aspekte.

3.3 Zakon o informacijskoj sigurnosti

Zakon informacijske sigurnosti informacija donesen je od strane Hrvatskog sabora na sjednici 13. srpnja 2007. godine gdje tim zakonom se utvrđuje pojam informacijske sigurnosti, mjere i standardi te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. Zakon informacijske sigurnosti odnosi se na državna tijela, jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svojim djelokruzima upotrebljavaju klasificirane i neklasificirane podatke. Ovaj zakon vrijedi za sve pravne i fizičke osobe koje imaju pristup klasificiranim i neklasificiranim podatcima. (NN, 2007)

3.3.1 Mjere i standardi informacijske sigurnosti

Područja informacijske sigurnosti prema članku 8. propisuju se mjere i standardi informacijske sigurnosti na pet područja (NN, 2007):

- Sigurnosna provjera – pruža osobama utvrđivanje mjera i standarda koji se služe pristupom klasificiranim podatcima koje dijelimo na „Povjerljivo“, „Tajno“ i „Vrlo tajno“. Osobe koje imaju pristup takvim podatcima dužni su ustrojiti popis osoba i registar zaprimljenih certifikata s rokovima važenja.
- Fizička sigurnost – obuhvaća informacijske sigurnosti u okviru utvrđivanja mjera i standarda za zaštitu objekata, prostora i uređaja koje sadrže klasificirane podatke.
- Sigurnost podataka – odnosi se na klasificirane i neklasificirane podatke koji se obrađuju, pohranjuju ili prenose u informacijski zaštitni sustav kako bi prešao u proces planiranja, izgradnje, uporabe, održavanja i projektiranja rada informacijskog sustava.
- Sigurnost poslovne suradnje – odnosi se na provedbu ugovora ili natječaja s klasificiranim dokumentom koji obuhvaća pravne i fizičke osobe iz članka 1. stavka 3. ovog zakona.

3.3.2 Središnja državna tijela za informacijsku sigurnost

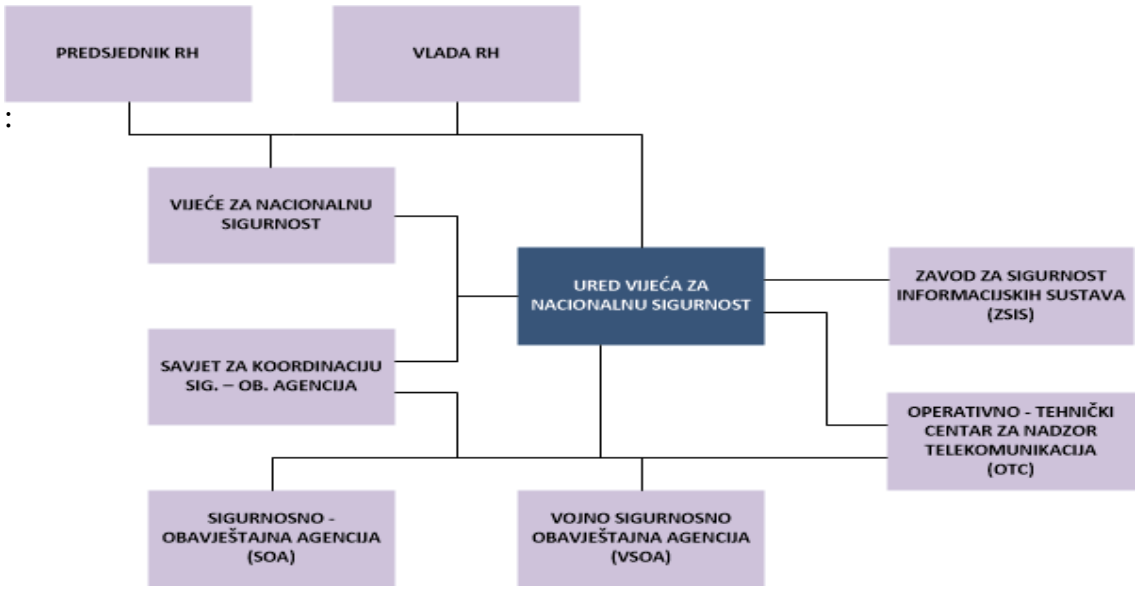
Središnja državna tijela za informacijsku sigurnost su (NN, 2007.):

- Ured vijeća za nacionalnu sigurnost
- Zavod za sigurnost informacijskog sustava
- Nacionalni CERT

3.3.3 Ured vijeća za nacionalnu sigurnost

Ured vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i donosi primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj vezan za klasificirane i neklasificirane podatke između Republike Hrvatske i stranih zemalja i organizacija (NN, 2007).

Nastavno slijedi shematski prikaz ureda vijeća za nacionalnu sigurnost i njegova podjela.



Slika 5 Ured vijeća za nacionalnu sigurnost (UVNS)

Izvor: preuzeto UVNS u sigurnosno-obavještajnom sustavu RH, 2014., dostupno na https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh, pregledano 20.6.2021

Ured vijeća za nacionalnu sigurnost zajedno sa Vladinom odlukom ima veliki utjecaj za sklapanje međunarodnih ugovora za zaštitu podataka koji su klasificirani. Osnovne zadaće institucije UVNS-a je: izvedba stručnih i administrativnih poslova Vijeća za nacionalnu sigurnost, pružanje savjetodavnih uloga za koordinaciju sigurnosne-obavještajne agencije i poslovi Predsjednika RH i Vlade RH koji imaju mogućnost nadzora nad radom sigurnosno-obavještajnih agencija i tijela sigurnosno-obavještajnog sustava. U uredu ustrojenost od strane Središnjeg registra zadužen je za prijem i distribuciju klasificiranih podataka kako bi koordinirao Sustavu registra državnim tijelima u RH (Tukić, 2018).

3.3.4 Zavod za sigurnost informacijskog sustava

Zavod za sigurnost informacijskog sustava (ZSIS) je središnje državno tijelo za tehnička područja sigurnosti i informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavka 2. ovog zakona. Početci pojave rada ZSIS-a počinje 2006. godine kada njegov djelokrug poslovanja preuzima zadaće nadziranja tehničkih kriptografskih materijala, upravljanja kriptografskom opremom te koordinacije Ureda Vijeća za nacionalnu sigurnost. Također, ZSIS

obavlja sigurnosne akreditacije informacijskog sustava u kojima se služe klasificirani podatci (NN, 2007)

3.3.5 Nacionalni CERT

Nacionalni CERT predstavlja nacionalno tijelo za prevenciju i zaštitu od računalnih prijetnji sigurnosti javnih informacija sustava u Republici Hrvatskoj. CERT proizlazi od eng. riječi (Computer Emergency Response Team) koji je osnovan u skladu sa Zakonom o informacijskoj sigurnosti u Republici Hrvatskoj. Nacionalni CERT zadužen je za obradu događaja incidenta na internetu odnosno njegova uloga je očuvanje informacijske sigurnosti u RH. Također preuzima određene korake kod čuvanja i zaštite informacijske sigurnosti prema obliku uputa, smjernica, preporuka i mišljenja koje donosi druga strana na državnim prostorima u koliko ima „Hr“ ili IP adresa locirana u državi. Nacionalni CERT ima postavljenu misiju da preventivno djeluje na zaštitu javnih informacijskih sustava prilikom pokušaja računalnog napada koji se brani na način da koristi dvije mjere, a to su proaktivne i reaktivne. Proaktivne mjere sprečavaju moguće štete ili ublažavaju koje su zadužene za nadziranje stanja na području računalne sigurnosti, kontroliranje i praćenje računalno-sigurnosnih tehnologija za prikupljanja, javno objavljivanje novih informacija u svrhu edukacija i provođenje edukativne obuke za posebne grupe korisnika. Kod Reaktivnih mjera imamo suzbijanje incidenta koji pokušavaju ugroziti informacijsku sigurnost u Republici Hrvatskoj na način da pripremaju i obrađuju sigurnosne preporuke o slabostima informacijskog sustava (Središnji portal za potrošače, 2020).

3.4 Norme informacijskog sustava

Sigurnost informacijskog sustava danas rezultira visokom razinom potrebne implementacije sigurnosti i zbog toga su određeni standardni odnosno norme. Norme predstavljaju osiguravanje pravilnog funkcioniranja informacijskog sustava u organizaciji. Najvažnije norme sigurnosti informacijskog sustava su: ISO 27001:2005 koji predstavljaju sustav upravljanja informacijske sigurnosti i ISO 27002:2013 – kodeks postupka za upravljanje informacijske sigurnosti. Kako bi se postigla kvaliteta sustava za upravljanje sigurnosti informacija potrebno je koristiti navedene norme.

ISO 27002 i ISO 27001 smatraju se jednim od glavnih međunarodnih informacijski sigurnosti predstavljeni od strane Internacionalne organizacije za standardizaciju (ISO). Primjena ovih

standarda imaju veliku ulogu zbog toga jer pružaju fleksibilnost, ne ulaze u konkretnu tehničku implementaciju i predstavljaju upravljački okvir.

Pored nabrojanih normi imamo veći broj normi koji se odnose na zaštitu sigurnosti informacijskog sustava (Bogati, 2011):

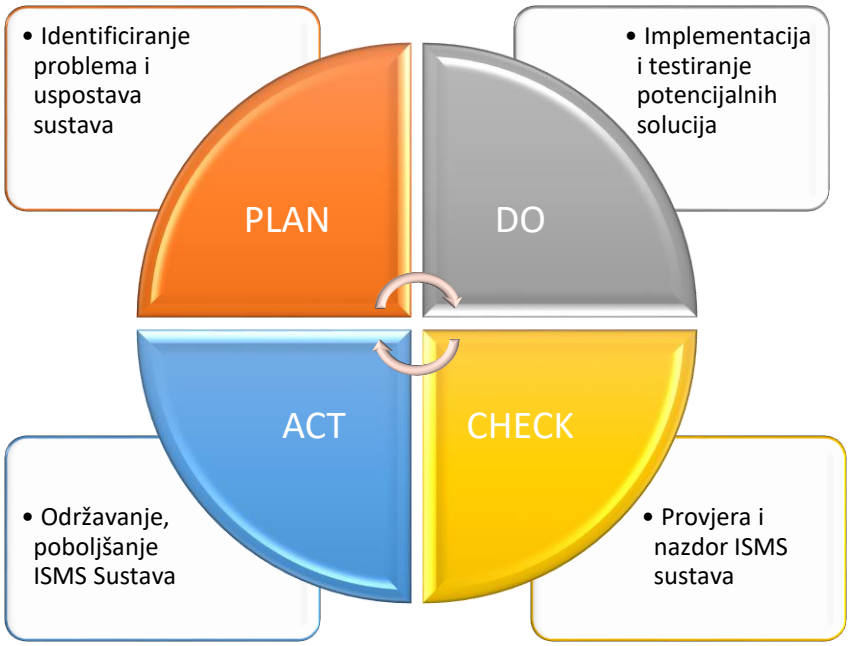
- ISO 27000 – koristi se unutar ISO 27000 serije standarda
- ISO 27000:2006 – (ISMS sustav upravljanja informatičkom sigurnosti)
- ISO 27002:2013 – Kodeks postupka za upravljanje sustava informacijske sigurnosti
- ISO 27003 – Vodič implementacije ISMS-a
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti
- ISO 27006:2007 – Zahtjevi za postupkom analize i certificiranja standarda
- ISO 27007 – Uputa za analizu ISMS-a
- ISO 27011 – Upute za uspostavu ISMS u telekomunikacijskom sektoru
- ISO 27031 – Specifikacija za ICT odjel za pripremljenosti poslovne neprekinutosti rada
- ISO 27032 – Upute za Cyber – sigurnost
- ISO 27033 – Upute za mrežnu sigurnost
- ISO 27034 – Upute za sigurnost aplikacija
- ISO 27799 – Sigurnosni sustav u zdravstvu

Nakon prikazane cijele serije standarda ISO 27000 detaljniji opis skupine ISO 27001 i ISO 27002 slijedi u nastavku zbog toga jer te dvije skupine su najvažnije za sigurnost informacijskog sustava.

3.4.1 ISO 27001 – Sustav za upravljanje informacijske sigurnosti

ISO 27001 spada pod međunarodnu normu koja je vrlo bitna sustavu za upravljanje informacijske sigurnosti kako bi omogućila procjenu rizika i implementaciju kontrola zbog očuvanja cjelovite, povjerljive i raspoložive informacijske imovine. Ona se smatra primjenjiva na sve vrste djelatnosti odnosno organizacije koje posjeduju informacijsku imovinu. Kod uspješnosti provođenja zadataka norme ISO 27001 potrebno je upotrebljavati procesni pristup za razumijevanje sigurnosnih zahtjeva organizacije koja ima cilj uspostaviti na području informacijske sigurnosti.

Nastavno slijedi slika 6 norme koja je uspješno provela svoje zadatke kako bi imala svoj model PDCA (Plan, DO, Check i Act).



Slika 6 Prikaz PDCA modela

Izvor: izrada autora prema: Otterlo van S., 2017, Information security and PDCA, dostupno na https://ictinstitute.nl/pdca-plan-do-check-act/, pregledano 20.6.2021

Prikazani model PDCA sastoji se od četiri koraka:

1. Plan – Prije same promjene potrebno je napraviti plan odnosno zapisati unaprijed postavljene aktivnosti koje želimo prikazati i upotrijebiti kako bi zapravo došli do zaključka efekt promjena. Odnosno zadaća plana se odnosi na postavljanje ciljeva, politike ISMS-a, procesa i procedura za poboljšanje informacijske sigurnosti.
2. Do – predstavlja korak postavljanja implementacije i rada ISMS kontrola i procedura.
3. Check – Nakon izvršene promjene potrebno je provjeriti učinak procesa, kontrola i postavljenih ciljeva koji su pripremljeni za izvještavanje ISMS sustava.
4. Act – Korak djelovanja koji obuhvaća poduzimanje preventivnih mjera na temelju dobivenih rezultata revizije uprave i ostalih relevantnih informacija kako bi se poboljšala situacija ISMS sustava (Horvat, 2017).

   Prema PDCA modelu koji je oblikovan od strane ISMS-a postoje četiri glavne faze sustava upravljanja informacijskom sigurnosti koje spadaju pod definiranu normu ISO 27001. Kod koraka Plan on služi kako bi isplanirali detaljno postavljene ciljeve za

informacijsku sigurnost i imao zadatak da izabere posebne sigurnosne mjere. Kod koraka „Do“ sve što je isplanirao prije te faze dolazi do provođenja. Kod PDCA modela njegov ciklus kružnog pokreta se nikad ne prekida zbog toga što četiri koraka navedenih u modelu moraju se odvijati kružno i neprekinuto kako bi ISMS pravilno funkcionirao.

ISO 27001 ima potrebnu i obaveznu dokumentaciju koju propisuje kroz sljedeće:

- Opseg sustava upravljanja informacijske sigurnosti
- Politika ISMS-a
- plan obrade rizika
- izvještaj procjene rizika
- izvještaj primjenjivosti
- načela sigurnosti sustavnog inženjeringa
- procedura upravljanja incidentima
- sve ostale dokumente ovisno o odabranim sigurnosnim mjerama

Navedene dokumentacije ovise o veličini organizacije i njihovoj količini potrebne dokumentacije kao npr. kod manje organizacije zahtjev dokumentaciji je manje u odnosu nego kao kod većih organizacije kojima je potrebno više od nekoliko stotina dokumenata u svom ISMS-U.

3.4.2 ISO 27002 – Kodeks postupka za upravljanje sustava informacijske sigurnosti

ISO 27002 predstavlja normu koja je zadužena za opisivanje posebnih mjera zaštite ISO 27001. Njezin naziv je bio ISO/IEC 17799 gdje je naziv preuzet iz dijela BS 7799 standard „Code of Practice for Information Security Managment“. Naziv ISO 27002 promijenio se u srpnju 2007. godine kada je dobio naziv ISO/IEC 27002 koji je zastupao međunarodnu osnovu za upravljanje i razumijevanje informacijske sigurnosti koji se proteže kroz 11 domena sigurnosne kontrole. Te navedene domene protežu se kroz 39 kontrolnih ciljeva i 133 kontrola povezanih sa upravljanjima, identificiranjem i smanjenje niza prijetnji od svakodnevnih izlaganja (Bogatti, J. 2011 godina). Razlika između ISO 27001 i ISO 27002 je u količini detalja koji su posvećeni zadanim sigurnosnim mjerama (Horvat, 2017).

U nastavku slijedi tablični prikaz izrađen 2013. godine koji prikazuje razliku između verzije ISO 27002:2005 i ISO 27002:2013.

Tablica 3 ISO 27002:2005 i ISO 27002:2013

ISO 27002:2005	**ISO 27002:2013**
Sigurnosna politika	Pružanje smjernica upravljanja i podrške
Organizacija i informacijske sigurnosti	Organizacija i informacijske sigurnosti
Upravljanje imovinom	Zaštita ljudskih potencijala
Zaštita ljudskih potencijala	Upravljanje imovinom
Zaštita okoliša	Kontrola pristupa
Kontrola pristupa	Kriptografija
Stjecanje informacijskog sustava	Fizička zaštita i zaštita okoliša
Upravljanje incidentima informacijske sigurnosti	Operativno osiguranje
Usklađenost	Sigurnost komunikacija
	Odnosi s dobavljačima
	Upravljanje incidentima informacijske sigurnosti
	Informacijski sigurnosni aspekti upravljanja kontinuitetom poslovanja
	Usklađenost

Izvor: izrada prema autoru Praxiom Research Group Limited, 2018, dostupno na https://www.praxiom.com/iso-27002-overview.htm, pregledano 20.6.2021

Verzija koja je nastala 2007. godine u novijoj verziji 2013. godine ima nekoliko novih izmjena, a najbitniji izmjenu se desila u verziji ISO 27002:2013 potpuno uklanjanje zadatka procjene i obrade rizika. Nova verzija ISO 27002:2013 ima 114 kontrola u odnosu na prošlu verziju koja je imala 133 i možemo naglasiti kako se broj domena povećao na broj 14. Tablica 3. prikazuje promjene koje su se dogodile između ISO 27002:2007 i ISO 27002:2013 kao npr. kod novije verzije dodana su područja „Odnosi s dobavljačima“. Kako je navedeno u podatcima iznad da je broj domena narastao sa 11 na 14 bez obzira na njegov rast cjelokupna struktura se smanjila, jer posebna kontrola se vodi za pojedine probleme i kontrole koji taj dio obuhvaća.

4. PRIJETNJE SUSTAVU SIGURNOSTI INFORMACIJA

Informacijski sustav u današnjem svijetu su izloženi mnogobrojnim različitim vrstama prijetnji. Različite vrsta izvora prijetnji mogu biti: prirodne prijetnje, namjerne prijetnje, nenamjerne prijetnje, oprema. Zbog navedenih izvora prijetnji sigurnost informacijskog sustava i sama zaštita podataka dobiva danas na važnosti. Prilikom samog početka informatizacije postajala je fizička zaštita iz razloga što su se tada računala nalazila u posebnim prostorijama i tada je potrebna bila fizička zaštita informacija. Prilikom pojave interneta širi se i potreba za drugim vrstama zaštite kao što je hardversko-softverska zaštita i administrativna zaštita.

4.1 Vrste prijetnji

Kako se informacijski sustav razvio kroz razdoblja, danas postoje razne vrste prijetnji informacijskom sustavu koji zahtjeva zaštitu. Postoje prijetnje prema njihovom izvoru, a one mogu biti:

- Prirodne prijetnje – kod prirodnih prijetnji spadaju prirodne nepogode, biološke prijetnje, sezonski fenomeni.
- Namjerne prijetnje – neautorizirani pristup, prisluškivanje, sabotaža, namjerno oštećivanje imovine, zlouporaba vlasti
- Nenamjerne prijetnje ljudi – nedovoljna educiranosti, nepravilno rukovanje, nemar i nepažnja, neadekvatna organizacija, nenamjerno oštećenje
- Oprema – električna neispravnost i kvarovi, prestanak napajanja, prekid komunikacije i zračenje

Navedeni izvor prijetnji prikazuje ljudski faktor koji proizlazi kao namjerna ili nenamjerna prijetnja informacijskom sustavu koja je puno više učestalija od prirodnih prijetnji. Kod prijetnje opreme (električna neispravnost i kvarovi) ona spada pod drugom učestalom prijetnjom informacijskom sustavu te prirodne spadaju na zadnjem mjestu zbog svoje rijetkosti. Poznavanjem vrste prijetnje i analiziranjem njezinoga uzroka dolazi se do mogućnosti pripreme metode zaštite informacijskog sustava od potencijalnih prijetnji i njihovih posljedica (Bukovac, 2016).

4.2 Metode napada na sustav sigurnosti informacija

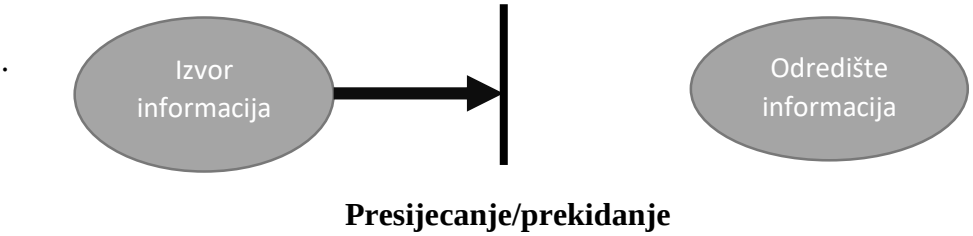
Napad predstavlja akciju ugrožavanja sigurnosti informacija, računalnog sustava i mreža. Navedene vrste napada se pojavljuju prilikom prijenosa javnih ili tajnih podataka unutar mreže. Kod metode napada na sigurnost informacija možemo raščlaniti 4 osnovne kategorije napada:

1. Metoda napada prekidanjem/presijecanje
2. Metoda napada presretanjem
3. Metoda napada izmjene
4. Metoda napada proizvodnje

4.2.1 Metoda napada prekidanje/presijecanje

Pojavljivanje ove metode napada događa se u trenutku kada korisniku napadač pokušava prekinuti tok podataka između izvora informacija i njenog odredišta.

U nastavku slijedi prikaz 7 metoda u kojem je prikazana metoda napada presijecanja.



Slika 7 Metoda prekidanja informacije između dva korisnika

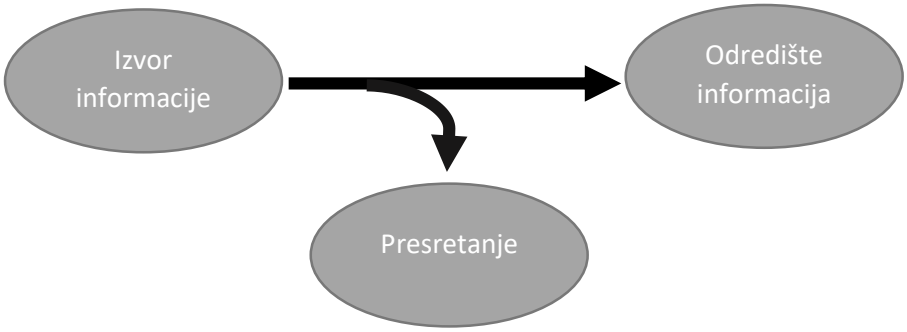
Izvor: izrada autora prema Bursać, Đ., 2015 str. 7 Sigurnosni aspekti baza podataka dostupno na: https://zir.nsk.hr/islandora/object/unipu:129/preview, pregledano 20.6.2021

Prikazana slika pruža detaljan uvid kako izgleda presijecanje izvorne informacije do njenog odredišta prekinuto od strane napadača. Također kada napadač dobije pristup korisničkoj mreži ima mogućnost blokiranja prometa mrežnim resursima, sakrivanje svog identiteta i prisutnosti, slanjem štetnih podataka aplikacijama i mrežnim serviserima što dovodi do nestabilnost rada.

4.2.2 Metoda napada presretanjem

Presretanje predstavlja napad koji se odnosi na povjerljivost podataka koji se događa pod sredstvom treće osobe u komunikaciji. Napadač treće strane ima mogućnost praćenja, bilježenja i kontroliranje komunikacije.

U nastavku slijedi prikaz slike 8 metoda napada presretanja.



Slika 8 Metoda napada presretanja

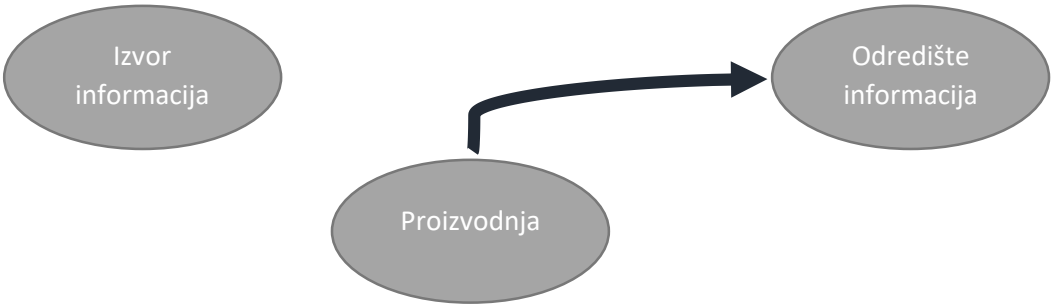
Izvor: izrada autora prema Bursać, Đ., 2015 Sigurnosni aspekti baza podataka, str.7 dostupno na: https://zir.nsk.hr/islandora/object/unipu:129/preview, pregledano 20.6.2021

Detaljno prikazana slika metode napada presretanja prikazuje kako napadač (presretanje) ubacuje se između dva korisnika (izvor – odredište informacije), te poruke koje je presreo i prikupio na svome računalu predstavlja se kao osoba koja pripada tome razgovoru. Nakon predstavljanja te osobe u razgovoru, sljedeći cilj mu je izvući što je više moguće korisnih informacija.

4.2.3 Metoda napada izmjene

Izmjena predstavlja napad na integritet koja po svojoj prirodi je aktivan napad. Metoda izmjene podataka predstavlja napad koji izmjenjuje podatke ili pristupna prava i često ostaje neprimjetan, zbog nepažnje (Mijatović, 2019).

U nastavku slijedi prikaz slike 9 koja prikazuje metodu napada izmjene od strane napadača.



Slika 9 Metoda napada izmjene

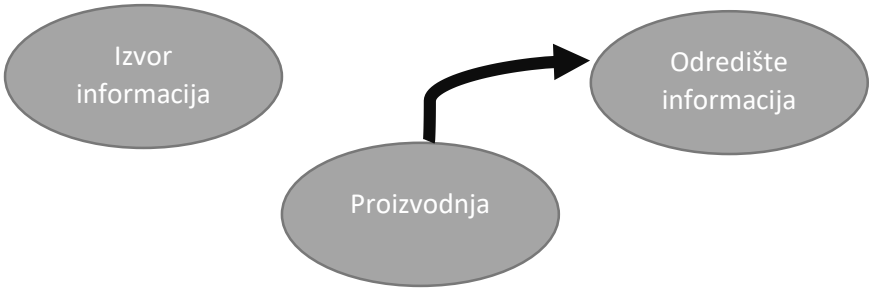
Izvor: izrada autora prema Bursać, Đ., 2015 Sigurnosni aspekt baza podataka, str 8. dostupno na: https://zir.nsk.hr/islandora/object/unipu:129/preview, pregledano 20.6.2021.

U gore navedenom prikazu 9. prikazan je način metode izmjene gdje napadač izmjeni informacije bez znanja korisnika između pošiljatelja i primatelja poruka kako bi došao do željenog sadržaja u svoju korist. Ovaka tip napada jako je opasan zbog dobivanje netočnih informacija koje mogu štetno utjecati na poslovanje organizacije. Najčešći tip ovakvih napada koristi se kod novčanih transakcija.

4.2.4 Metoda napada proizvodnje

Navedena metoda napada proizvodnje naziva se još i lažno prikazivanje gdje napad se vrši nad autentičnosti. Odnosno umetanje lažnih podataka zbog krađe korisničkih podataka s ciljem nanošenje štete korisniku (Mijatović, 2019).

U nastavku slijedi prikaz 10 metoda napada proizvodnjom.



Slika 10 Metoda napada proizvodnjom

Izvor: izrada autora prema: http://svarog.nubl.org/wp-content/uploads/2019/06/Doc.-dr-Marijan-Mijatovi%C4%87-ZA%C5%A0TITA-I-SIGURNOST-INFORMACIJSKIH-SUSTAVA.pdf , pregledano 20.6.2021.

Prikaz slike objašnjava napad proizvodnje tako što napadač (proizvodnja) proizvodi lažne podatke i ubacuje ih u korisnikovu mrežu kako bi mogao ukrasti ili zlonamjerno iskoristiti korisničke podatke, i tako nanijeti štetu korisniku.

4.2.5 Zloćudni programi informacijskog sustava

Zloćudni program ili malware predstavlja štetan programski alat kojim se služe napadači kako bi oštetili korisnika ili ukrali njegove podatke, pridobili pristup korisnikovoj mreži i drugim računalima koje se nalaze u mreži. Informacijski sustav kako bi se zaštitio od zloćudnih programa postoje razni maliciozni programi koje je potrebno dobro proučiti kako bi zaštitili informacije.

4.2.6 Keystroke logger program za praćenje unos znakova

Keystroke logger je program koji napravljen za praćenje unosa znakova i bilježi svaku aktivnost koju korisnik provede na računalu, također se naziva „Keylogger“. Korisniku kojem je postavljen keylogger predstavlja opasnost od krađe njegovih lozinki, pinova, brojeva kartica i slično. Keylogger program se dijeli na 2 kategorije:

- Fizički uređaj koji se nalazi u već sklopljenom računalu odnosno njegovim komponentima
- Programski alati koji se nalaze na računalu skinuti ali sakriveni

Fizički uređaj za praćenje unosa znakova s tipkovnice izgledom je sličan adapteru koji s jedne strane spaja tipkovnicu, a druga strana spaja u računalo. Keylogger fizički uređaj funkcionira na način da svaki put kada se pritisne tipka na tipkovnici on sprema informaciju u svoju memoriju, nakon čega korisnik koji je ugradio keylogger može zatražiti spremljene podatke (Conry-Murray i Weafer, 2005).

U nastavku slijedi prikaz fizičkog uređaja Keystroke logger na slici 11.

Slika 11 Fizički uređaj za praćenje unosa znakova na tipkovnici

Izvor: preuzeto sa https://www.detective-store.com/hardware-keylogger-keygrabber-wifi-premium-2gb-ps2--125.html 20.6.2021

Prethodno prikazan je keylogger fizički uređaj, ali postoji i softverski keylogger koji funkcionira na isti način kopiranja i praćenja unosa tipkovnice od strane korisnika kojem je podmetnut keylogger. Keylogger softverski danas je jednostavno i besplatno skinuti na Internet stranicama koji je puno lakši pri instalaciji na korisnikovo računalo bez njegovog znanja. Softverski način rada je taj da kopira unos s tipkovnice, te ih sprema na određeni sakriveni dio memorije na računalu. Kada se on uključi odnosno aktivira on postaje potpuno nevidljiv korisniku bez obzira što je upaljen u pozadini računala. Nakon procesa prikupljanja podataka putem softverskog keylogger napadaču se šalju podatci bez znanja korisnika.

4.2.7 Virusi

Računalni virus je softverski program koji na primjer ako ga otvorite ili reproducirate možete zaraziti računalo na način da bez vašeg dopuštenja korisnik računala kopira samog sebe u memoriju ciljanog računalnog sustava. Računalni virus ima zadatak uništiti ili oštetiti računalo na način nekontrolirane radnje, brisanjem podataka sa računala ili ukrasti osobne podatke (Conry-Murray i Weafer, 2005).

Početak računalni virusa počeo se širiti preko disketa, no kada se pojavio Internet uvjeti postaju bolji za prijenos virusa. Računalo se može zaraziti preko dva načina: korištenjem tuđih CD, DVD ili USB-a, putem datoteka i preko elektroničke pošte koja je razmijenjena putem internetske usluge.

4.2.7.1 Vrsta virusa

Postoje dvije kategorije virusa: prva kategorija virusa je osnovna podjela virusa na Crv („Worm“), Trojanski konj, Backdoor, Dialer, Hoaw, Spyware i postoji druga kategorija virusa koja se odnosi na njihov način funkcioniranja koja je detaljno opisana u sljedećem naslovu. (CERT, 2010)

4.2.7.2 Prva kategorija osnovne vrste virusa

Kod prve kategorije osnove vrste virusa poznajemo:

- Crv ili na eng. „Worm“ je program koji kopira samog sebe u drugim datotekama poslan od strane kontakta. Računalna mreža programu Crv pruža mogućnost daljnjeg razmnožavanja na drugim korisničkim računalima. Funkcioniranje programa radi na način taj da kada se računalo inficira crvom on briše svoju prvobitnu kopiju i uvijek se nalazi negdje na mreži, svaki svoj trag briše i zbog toga naziva se još „Rabbit“ jer stalno bježi uokolo mrežom.
- Trojanski konj poznajemo pod pojmom kao virus, ali on nije virus već oblik zlonamjernog programa koji pod lažnim programom koristi se kako bi ga korisnik aktivirao odnosno dozvolio korisniku da ga se instalira na računalo. Funkcija trojanskog konja na računalu jeste ta da kada ga se instalira on pokušava dobiti potpunu kontrolu nad računalom u svrhu krađe informacija, slanja i špijuniranja. Trojanski konj najčešće napada preko: zaraženog programa, elektroničke pošte, prenosivi mediji za spremanje podataka i web stranica (Contry-Murry i Weafer 2005).
- Backdoor je vrsta zlonamjernog programa koji poriče svakodnevne provjere autentičnosti pristupa na sustav računala. Njegova funkcija je da poput daljinskog upravljača odobrava resursima unutar računala ili programa kao što su npr. baze podataka ili poslužitelji podataka omogućava napadačima da pokradu informacije ili inficiraju korisnikovo računalo u svrhu napada na njegovu web stranicu. Najčešći napadi Backdoora je najčešće u kombinaciji sa Trojanskim konjom.
- Dialeri su programi na mreži koji se najčešće instaliraju prilikom klika na stranici npr. „Kliknite ovdje ako želite smršaviti 10 kg u 3 tjedna“ ili „Kliknite ovdje kako biste postali bogati preko noći“, nakon klika pojavi se novi tipa „Kliknite kako biste skinuli program za dionice“. Nakon čega dolazi do pitanja „Da li ste sigurni“ i korisnik pritisne „Da, i tako pokrene skidanje programa koji naravno treba platiti i to je to. Zajedno sa programom koji je skinut dolazi i Dialer koji nakon paljenja interneta korisnika pruža

Dialeru mogućnost korištenja vašeg interneta/računa (Iskon, T-com, A1) koji ćete vi saznati tek kada dobijete račun telefonske usluge na kraju mjeseca.

- Hoax – ili virusna lažna uzbuna je zapravo obavijest koju primamo od strane napadača koji je šalje u obliku elektroničke pošte npr. „Pažnja, računalo vam je zaraženo virusom koji nije moguće ukloniti sa niti jednim anti virusom, nakon aktivacije ovog virusa u roku od 5 dana izbrisati će vam sve sa računala u koliko posjedujete datoteku ABD.EXE na svome računalu, odmah je izbrišite kako se ne bi virus dalje širio na sljedeća računala“. Kada korisnik toga računala nije dovoljno informatički educiran i uklonit datoteku, nakon toga računalo gubi pola programa ili mu uopće više ne funkcionira kao prije.
- Spyware – spada pod kategorijom malwarea. Pojam „Spyware“ korišten je za opis skupa programa koji posjeduju razne sposobnosti kao npr. mijenjanje telefonskog broja koji se spaja direktno na vaš model, nadziranje i prikupljanje podataka preko tipkovnice koju korisnik otvara ili utipkava kako bi napadač zatražio naredbu od programa da kopira vaše podatke unesene na internet stranici (Contry-Murray i Weafer, 2005).

4.2.7.3 Vrsta virusa na njihov način funkcioniranja

Kod kategorije vrsta virusa na temelju njihovog načina funkcioniranja imamo: (Bukovac, T. 2016)

- Virus datoteka – izvršavaju akciju nakon što se pokrene (DIRECT ACTION) ili oni koji se nalaze u memorijama i čekaju na korisnika kojem se virus nalazi u memoriji računala.
- Boot Sektor i Master Boot Record Virus – su skupina virusa koji napadaju Master BOOT sektor ili BOOT sektor diska odnosno njihovo nalaženje unutar diska (Tom Erjavec, programski virusi) .
- Parazitski virusi – vrlo su česti virusi koji su u mogućnosti napasti korisnikovo računalo dodavanjem novog sadržaja npr. preko: .COM, .EXE, SYS, OVL. itd.
- Svestrani virusi – Virusi koji napadaju posebno BOOT sektore i izvršne programe od kojih imaju koristi većeg proširivanja na računalu.
- Link virusi – kao što sam naziv govorio oni predstavljaju viruse preko link web stranica koji mora biti poslane od strane napadača prema korisniku kojem može izazvati veliku katastrofu na hard disku.

- Kernel virusi – njihova specifičnost je po tome što ciljaju funkcije programa (kernel ili core) operativnog sistema na primjer 3APA3A je DOS-kernel virus koji spada pod kategoriju višestranačkih virusa.

4.2.8 Phising

Phising se smatra jednom vrste manipulacije koju najčešće koriste napadači kako bi imali pristup neovlaštenim i povjerljivim podatcima. Zadatak napadača jeste da iskoristi lažni identitet i poruke kako bi uspio izvući korisnikove lozinke, broj bankovne kartice i pina. Phising napadi mogu biti poslani bilo kojem korisniku računala putem elektroničke pošte ili web mjesta. Ova vrsta manipulativnog napada se smatra jako opasne i ozbiljne zbog toga što mogu dovesti korisnika do velikih i teških financijski posljedica nakon napada.

Postoji danas nekoliko Phising metoda, a to su:

- Jednostavni zahtjevi – poslani su najčešće putem elektroničke pošte
- lažna web sjedišta – nalaze se najčešće u poveznicama na određenim Internet stranicama na koje ulazimo
- lažni prozor na legitimnim web sjedištima – Popup prozori pojavljuju se prilikom samog ulaska na stranicu
- lažni linkovi – najčešće su poslani ciljanim korisnicima od strane napadača u obliku linka putem elektroničke ili društvene mreže (Bukovac, T. 2016)

5. ZAŠTITA SIGURNOSTI INFOMRACIJSKOG SUSTAVA

Zaštita sigurnosti informacijskog sustava i sama zaštita podataka od raznih napada putem raznih virusa možemo zaštiti na razne načine. Zaštita sigurnosti informacijskog sustava u današnjem svijetu postaje sve poznatija korisnicima računala i informacijskog sustava. Kako bi se zaštitili od mogućih napada korisnici su se educirali više o mogućnostima korištenja zaštitnih podataka. Pri samim početcima pojave prvih računala i informatizacije njihova oprema je postala centralizirana i zbog toga prva zaštita je bila fizička zaštita. Fizička zaštita najčešće se koristila za računala koja su se nalazila u posebnim prostorijama i objektima koje je trebalo čuvati zbog tajnih podataka. Nakon pojave interneta upoznajemo se sa novim pojmom zaštite sigurnosti informacijskog sustava koji se naziva hardversko softverska zaštita. Hardversko softverska zaštita se pojavila nakon pojave interneta zbog toga jer podatci su bili uključivani na Internet, tako da je bila potrebna također nova zaštita informacija organizacijsko administrativna zaštita. Prilikom uvođenja novih kategorija zaštite informacijskog sustava ciljano prioritet je postala potreba za izradom i upotrebom uputa o zaštiti podataka koje se koriste u raznim tvrtkama (Juran, 2014).

Zaštitu sigurnosti informacija s obzirom na razvoj informatizacije i pojave interneta kod informacijske sigurnosti možemo nabrojati na tri osnovna područja:

1. Fizička sigurnost
2. Programska sigurnost (hardversko – softverska)
3. Organizacijske mjere zaštite

5.1 Fizička sigurnost

Fizička metoda sigurnosti pojavljuje se jos od početka informatizacije i prvih računala. Ona se smatrala jedna od bitnih komponentni u zaštiti informacijskog sustava. Fizička sigurnost informacijskog sustava može se ugroziti na više načina npr. sabotaža, krađa, elementarne nepogode (potres, požar). Prirodne nepogode mogu imati jak utjecaj na računala kao i kada računalna oprema dođe u doticaj s dimom, prašinom, vibracije, vlaga koja može uništiti sustav i njegove podatke koje sadrži (Kovačević, D., 2008). Prve mjere postavljene fizičke sigurnosti odnosile su se na osiguranje ulaza i izlaza odnosno uključivanje zaštite: postavljanje lokota, postavljanje zaštitara, kamera i alarmnih sustava.

5.1.1 Područja zaštite

Kod područja zaštite informacijskog sustava potrebno je zaštiti područje u kojem se nalaze povjerljive informacije kako bi se spriječio ulazak do određenih informacija, zbog toga postoji zaštita okoline, prostorija ili recepcija.

Kod većine poslovnih organizacija pri samom ulasku u objekt nalazi se vrsta recepcije odnosno mjesto određenih administrativnih poslova koji pružaju mogućnost pristupu raznim informacijama. Rad na takvim vrstama recepcija potrebno je uvesti kontrolu kako povjerljive informacije i dokumenti ne bi bili na vidljivim mjestima koje su dostupne svima u tom objektu. Također potrebno je dobro zaštiti rad zaposlenika kako pojedini klijenti ne bi vidjeli njihove povjerljive informacije i njihov rad na informacijskom sustavu. Pored fizičke zaštite recepcije potrebno je postavljanje kamera kako bi se vršio bolji nadzor i postavljanje alarma u slučaju opasnosti. Sve prostorije koje sadrže povjerljive informacije potrebno ih je zaštiti u skladu s korištenjem informacija u takvim prostorijama. Kada govorimo o fizičkoj zaštiti područja također moramo napomenuti kako kontrola pristupa predstavlja fizičku zaštitu informacija. Njen zadatak je zabraniti pristup ulaska osobama koji nemaju odobrenje za to. Kontrola pristupa predstavlja fizičku zaštitu na način da se zapošljavaju zaštitari ili osobe koje imaju odobren pristup za ulazak (Lutkevih, B., Access control). (Juran, 2014)

Istaknuta područja zaštite kontroliraju se pomoću EPS (electronic physical security) koji ima zadatak primjene brojnih elektroničkih sustava kao što su (CARNET, 2010):

- sustavi za detekciju požara
- sustav za suzbijanje plinova
- sustavi za nadzor
- sustavi za kontrolu pristupa
- sustavi za detekciju upada
- oprema za zaštitare
- sustav za opremanje okoline i prostorija

5.1.2 Elementi fizičke sigurnosti

Elementi fizičke sigurnosti predstavljaju postizanje zaštite kroz alarmne sustave koji pružaju vizualnu ili zvučno upozorenje sustava koji je doveden u opasnost. Kod alarmnih sustava postoje vrste koji se razlikuju po namjeni (Juran, 2014):

1. Alarm za sigurnost – njegova uloga je obavijestiti prilikom prirodnih nepogoda ili izvanrednih situacija poput širenja radijacije
2. DCS sustav (disributed control manufactoring system) – obavještava zaposlenike prilikom događanja važnih situaciju u kemijskim i nuklearnim laboratorijima
3. Vremenski alarmi – aktiviraju se na postavljenom vremenu kad ga osoba postavi
4. Alarm Q&M sustav (operation and maintenance) – prilikom lošeg radnog stanja sustava koji se nadzire
5. Alarm protiv provala – kao što sam naziv govori, njegova uloga je obavijestiti policiju prilikom provala koji su poznati pod nazivom „tihi alarmi“ kako ne bi provalnici također bili obavješteni.

Alarm danas u informacijskom sustavu predstavlja veliku važnost zbog toga što oni zaštićuju neovlašteni pristup informacijama. Naravno alarm ima negativnu stranu zbog toga što se može aktivirati sam od sebe kada za to nema potrebe, najčešće su to greške pri samom njegovom radu ili slučajno aktivirano od strane zaposlenika. Također napomenuto je da alarm za prepoznavanje dima se može aktivirati u slučaju da zaposlenik koji se nalazi u zaštićenom objektu ga može slučajno aktivirati, jer alarm prepoznaje dim i aktivira se zbog toga kako bi zaštitio objekt od mogućnost požara, a zapravo radi se o dimu cigarete. Pravovremeno reagiranje alarma dovodi do pravovremene informacije koja postaje zaštićena i pruža mogućnost očuvanja informacijskog sustava. (Juran, 2014)

5.2 Programska sigurnost (hardversko softverska zaštita)

Programska sigurnost predstavlja zaštitu odnosno hardversko softverska zaštita operacijskog sustava na razini korisničkih podataka. Ona se smatra jednom od najranjivijih zaštita zbog toga što danas postoji jednostavna i brza distribucija softvera koja pruža mogućnost brže internetske veze koja postaje glavni mediji računalne mreže koji to omogućava. Softversko održavanje je relativno skupo i nije ga moguće u potpunosti zaštiti, jer danas postoje piratske verzije softvera koja predstavlja zamjenu za originalne verzije programa. Svaki takav program, odnosno softver predstavlja zaštitu podataka koji omogućava drugim poduzećima, ali naravno ako je verzija originalna tada postiže se prednost nad konkurencijom i mogućnost veće zarade od softvera (CARNET, 2004).

5.2.1 Zakonska zaštita računalnog programa

Prethodno spomenuti izraz „piratska verzija“ koja predstavlja danas zamjenu za originalu verziju softvera. Kako bi se obranili od piratski verzija postoje doneseni zakoni koji reguliraju prava autora softvera i njegova prava korisnika (CARNET, 2004). Softverska industrija pruža prava zaštite izvornog i izvršnog programa, strukture i organizacije koja zahtjeva kod programa te sadržava upute i ostale dokumentacije u pismenom obliku. Patentnom se zaštićuje osim autorski prava svaki proizvodni proces, mehanizam ili princip koji je potpuno nov, te se ne nalazi u prethodnom objavljenom patentu. Kod oblika autorskih prava, patenta postoji i pojam licenca. Licenca je pravni instrument koji pruža korisniku softvera određenog vremensko razdoblje upotrebljavanja tog softvera.

Zakonski oblik softvera se dijeli na nekoliko kategorija:

- Public domain – pruža mogućnost korisniku da radi sve što poželi pa čak i prodavanje bez dozovole autora.
- Open source – softver besplatnog korištenja, umnožavanja i distribucije.
- Freeware – softver besplatnog korištenja, ali nemogućnost mijenjanja zbog autorskih prava.
- Shareware – vrlo sličan Freeware koji zahtjeva po licenčnom sporazumu određenu svotu novca koja treba biti poslana autoru softvera.

- Komercijalni softver – softver kojeg je potrebno kupiti i koji zabranjuje kopiranje, mijenjanje ili distribuiranje.
- Komercijalni licencirani softver – omogućava korištenje softvera u skladu s licenčnim sporazumom zakona o autorskim pravima.

5.2.2 Metoda zaštite softvera

Prilikom korištenja hardversko softverske programe postoji metoda zaštite koja omogućava korištenje računalnih programa pomoću autentifikacije korisnika kako bi se zaštitile informacije. Korisnik treba imati poseban hardver koji se koristi na način spajanja komunikacijskog porta ili upisivanje registracijske šifre prilikom instaliranja programa. Takav uređaj se naziva „Dongle“ on je jednostavna naprava koja sadrži implementirani ključ za pristup određenoj aplikacija. Unutar same aplikacije postoje razna mjesta funkcija koja ima uspostavljenu komunikaciju s dongle ključem i na temelju toga šalje razne upite i provjerava pristigle odgovore. U koliko dongle nije prisutan program prestaje s radom. Teško ga je kopirati zbog toga što treba probiti funkciju za komunikaciju s dogle ključem unutar same aplikacije. Osim Dongle metode postoje i druge metode zaštite:

1. Debugging – alat koji ispravlja pogreške u kodu koje omogućuju pokretanje programa. Njegovo djelovanje može se prekinuti prilikom izvršavanja programa između dvije instrukcije. Jedan od poznatijih alata debugginda je SoftIce tvrtka Compuware koji pomaže drugima alatima da riješe pogreške u koliko im promaknu.
2. Disassembling – program koji pretvara izvršni kod natrag u izvorni kod kako bi imao mogućnost analiziranja. Najčešće korišten program disassemblinga je IDA Pro tvrtke NuMega.
3. Decompiling – pretvaranje binarnog koda u program kao izvorni kod od strane programskog jezika razine C++ ili Java. Prednost ovog alata je onemogućavanje piratima da poznaju jezik više od razine asemblera zbog čega je takav kod lakše analizirati. (CCERT, 2004)

5.3 Organizacijske mjere zaštite

Organizacijske mjere zaštite predstavljaju mjere zaštite koje se upotrebljavaju s ciljem da poslovni sustav osigura željenu razinu funkcioniranja i integritet podataka koji su izloženi

mogućim prijetnjama. Pod organizacijskim mjerama možemo uvrstiti sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebno za primjenu i donošenje organizacijskih uputa kako bi se provodile na radnom mjestu (Šehanović i Hutinski, 2002).

Kod organizacijskih mjera zaštite postoje tri razine sigurnosti:

1. Infrastruktura informacijske sigurnosti
2. Sigurnost pristupa treće osobe
3. Outsourcing

5.3.1 Infrastruktura informacijske sigurnosti

Upravljanje informacijskog sigurnosti unutar organizacije, odnosno kako bi organizacija funkcionirala trebaju se zaštiti potrebne informacije kojima se potiču multi disciplinirani pristup sigurnosti informacija koja je zajedno u suradnji sa najvišim predstavnicima hijerarhije organizacije. Infrastruktura informacijske sigurnosti dijeli se na (Garač, 2005):

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

5.3.2 Sigurnost pristupa treće zainteresirane strane

Kod ovakvog sigurnosnog pristupa potrebno je znati razliku i identificirati rizik koji dolazi zajedno sa ovim pristupom. Postoje dva pristupa: Fizički i logički pristup. Fizički pristup treće strane podrazumijeva omogućavanje korisnicima pristup uredima, prostorijama i ormarima koji sadrže opremu za pohranu. Logički pristup podrazumijeva pristup bazama podataka koji su zaštićeni od strane organizacije i informacijskog sustava. Primjer trećih strana mogu biti: dobavljači, zaštitari, usluge omogućene outsourcingom, zaposleni studenti, osoblje koje vodi računa od hardveru i softveru.

5.3.3 Outsourcing

Definiramo kao upotreba pojedinaca i vanjskih poduzeća za obavljanje posebno odabranog posla. Kod ugovaranja poslova uloga outsourcinga je da pruža ostalim trećim strana vrstu ugovora kojim će se kontrolirati mehanizam, procjena rizika i sigurnost postupka provođenja neovlaštenog korištenja informacija unutar organizacije. Ugovor outsourcinga ima određene zahtjeve kojih se treba pridržavati prilikom obavljanja poslova za organizaciju, takav ugovor se sastoji od sljedećih stavki (Moj Posao, 2006.)

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

Outsourcing ima prednost fokusiranja na osnovnu aktivnost koja pomaže organizaciji da usredotoči kao i kod razvoja poslovnih procesa jer uloga sporednih poslova jeste da ih obavlja za njih.

6. ZAKLJUČAK

Za uspješnost poslovne organizacije važno je znati koliko su danas informacije jako korisne i potrebne koje trebaju biti točne i dostupne u svakome trenutku. Informacija poslovne organizacije se smatra najbitnijim resursom poslovanja i zbog toga je važno imati jako razvijen sustav zaštite informacija od mogućih prijetnji.

Svaki informacijski sustav predstavlja dio poslovnog sustava koji ima ulogu prikupiti, obraditi, analizirati, čuvati i rasporediti dodatne informacije koje su vezane za donošenje odluka i upravljanje poslovanja organizacije. Informacijski sustav ne predstavlja rad samo sa računalima već obrada podataka koji su korišteni u ručnom dobu obrade podataka, a danas takva metoda se i dalje koristi.

Potrebno je odrediti važnost informacije poslovanju kako bi sačuvali integritet koji omogućava rast, korisnost i povjerljivost informacije. Informacijska sigurnost temeljena je na tri glavna aspekta povjerljivost, integritet i dostupnost koje treba zadovoljiti.

Postoje razni zakoni vezani za sigurnost informacijskih sustava koji su potrebni kako bi osigurali zaštitu informacija. Oni se nazivaju: Ured vijeća za nacionalnu sigurnost koji koordiniraju i donose primjenu mjera i standarda vezanih za informacijsku sigurnost, Zavod za sigurnost informacijskog sustava sklapa međunarodne ugovore za zaštitu podataka koji su klasificirani i Nacionalni CERT obuhvaća obradu događaja incidenata na internetu koje je usmjereno samo na informacijsku sigurnost u Republici Hrvatskoj.

Informacijska sigurnost dovodi se u pitanja kada su se pojavili različiti oblici i izvori prijetnji. Kako bi se zaštitili od različitih vrsta prijetnji poput virusa kao što su: trojanski konj, malware, keylogger, backdoor i crv postoji nekoliko važnih područja zaštite informacijskog sustava. Prvo područje zaštite odnosi se na fizičku sigurnost informacija koja se pojavila još početkom informatizacije i prvih računala, kojoj je zadatak bio zaštiti objekte na način postavljanja lokota, zaštitara, kamera i alarmnih sustava. Drugo područje odnosi se na programsku sigurnost informacija koja uključuje razne programske alate poput anti virus i antispyware programa. Treće područje obuhvaća organizacijske mjere zaštite koja se sastoji od tri razine sigurnosti: infrastruktura informacijske sigurnosti, sigurnost treće osobe i outsourcing. Njen zadatak je održavanje poslovnog sustava sa svrhom lakšeg održavanja sigurnosti informacija.

Cilj završnog rada je predstaviti moguće oblike i izvore prijetnji informacijskom sustavu te kako se zaštiti od njih u pravo vrijeme i tako sačuvati uspjeh poslovanja u organizacijama.

IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Ivan Krešimir Uskok

Matični broj studenta:

Naslov rada: IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum Potpis studenta

_____ _____

7. POPIS LITERATURE

1) Knjige

1. Klasić, K i Klarin, K. (2009) Informacijski sustavi: načela i praksa. Zagreb: Intus informatika
2. Pavlić, M., 2011., Informacijski sustavi, Zagreb: Školska knjiga.
3. Panian, Ž. et al. (2010) Poslovni informacijski sustavi. Zagreb: TISKARA ZELINA d.d.
4. Antoliš, K., Ždrnja, B., Pakšić, I., Vugrek, A., … Jušić, S., (2010) Sigurnost informacijskih sustava: priručnik. Zagreb : Algebra d.o.o.
5. Contry-Murray A. i Weafer V. (2005) Sigurni na internetu. Zagreb: MIŠ d.o.o.
6. Šehanović, J., Hutinski, Ž., i Žugaj, M. (2002) Informatika za ekonomiste. Pula: Fakultete ekonomije i turizma (Dr. Mijo Mirković)
7. Garača, Ž. (2005) Informatičke tehnologije. Split: Ekonomski fakultet

2) Članci

1. Klasić, K. i Klarin, K. 2003 Informacijski sustavi. (Seminarski rad). Split: Veleučilište u Splitu, Odjel računarstva
2. Mijatović, M. (2019) Zaštita i sigurnost informacijskih sustava. Stručni rad. Banja Luka: Fakultet za informatiku. 285-292 str.
3. Gospočić, Z. (2018) Analiza aplikacijskih rješenja informacijskog sustava mrežnog operatora. Završni rad. Zagreb: Sveučilište u Zagrebu, Fakultet prometnih znanosti.
4. Bukovac, T. (2016) Sigurnost informacijskih sustava. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Filozofski fakultet.
5. Tukić, I. (2018) Nacionalna sigurnost i razvoj sigurnosno-obavještajnih službi u Republici Hrvatskoj. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Odsjek za informacijske i komunikacijske znanosti
6. Bogati, J. (2011) Norme informacijske sigurnosti ISO/IEC 27K. 113-114 str.
7. Horvat, T. (2017) Analiza sigurnosti i zaštite informacijsko-komunikacijskog sustava u korporativnom okruženju. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Prometne znanosti.

8. Bukovac, T. (2016) Sigurnost informacijskih sustava. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Filozofski fakultet
9. Juran, A. (2014) Sigurnost informacijskog sustava. Diplomski rad. Rijeka: Sveučilište u Rijeci, Pomorski fakultet
10. Kovačević, D. (2008) Sigurnosna politika. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.

3) Ostali izvori

1. Razvoj obrade podataka kroz povijest (2013), dostupno na: https://matura14.wordpress.com/2013/05/01/obrade-podataka-kroz-povijest/, pregledano, 20.6.2021.
2. Računala kroz povijest, dostupno na http://web.studenti.math.pmf.unizg.hr/~bozana/povijest.html , pregledano 19.6.2021
3. Računalo ENIAC službeno pušteno u pogon (1946.), dostupno na https://povijest.hr/nadanasnjidan/racunalo-eniac-sluzbeno-pusteno-u-pogon-1946/, pregledano 19.6.2021
4. UVNS, Što je to informacijska sigurnost? Dostupno na: https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost, pregledano 19.6.2021
5. Zakon o informacijskog sigurnosti NN 79/07, dostupno na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, pregledano 20.6.2021
6. Središnji portal za potrošače. Računalno-sigurnosni incidenti: Nacionalni CERT, dostupno na: https://www.szp.hr/sve-potrosacke-teme-na-jednom-mjestu/racunalno-sigurnosni-incidenti/418, pregledano 20.6.2021
7. CERT, (2010) O virusima, dostupno na: https://www.cert.hr/virusi/, pregledano: 20.6.2021
8. CARNET; Fizička zaštita informacijskog sustava (2010) Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf, pregledano 22.6.2021
9. CARNET , (2004) Zaštita softvera dostupno, na https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf pregledano 22.6.2021

10. CCERT-PUBDOC, (2004) Zaštita softvera, dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf , pregledano 25.6.2021
11. Moj Posao, 2006. Outsourcing – što je i zašto se koristi, dostupno na: https://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/ , pregledano 25.6.2021

8. POPIS TABLICA I SLIKA