Analiza sigurnosnih aspekata informacijskih sustava u tvrtki za internet usluge

Amadeo, Andrea

Master's thesis / Specijalistički diplomski stručni

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, Faculty of economics Split / Sveučilište u Splitu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:124:040807

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

REFST - Repository of Economics faculty in Split

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

Analiza sigurnosnih aspekata informacijskih sustava u tvrtki za Internet usluge

Mentor: **Studentica:**

dr.sc. Jadrić Mario **Amadeo Andrea**

Split, rujan, 2017.

SADRŽAJ

1. UVOD 1

1.1. Definicija problema 1

1.2. Cilj rada 1

1.3. Metode rada 2

1.4. Struktura rada 2

2. UVOD U INFORMACIJSKE SUSTAVE I INTERNET USLUGE 3

2.1. Pojam informacijskih sustava 3

2.2. Dijelovi i načela informacijskog sustava 5

2.3. Načela informacijskog sustava 8

2.4. Internet usluge 9

3. VAŽNOST INFORMACIJSKE SIGURNOSTI U SUVREMENOM POSLOVANJU 12

3.1. Važeći zakoni informacijske sigurnosti 15

3.1.1. Zakon o informacijskoj sigurnosti 15

3.1.2. Zakon o provedbi uredbe o elektroničkoj identifikaciji i uslugama povjerenja 16

3.1.3. Zakon o elektroničkoj ispravi 17

3.1.4. Zakon o zaštiti osobnih podataka 17

3.2. Institucije koje djeluju na području informacijske sigurnosti 18

3.2.1. Ured vijeća za nacionalnu sigurnost 18

3.2.2. Zavod za sigurnost informacijskih sustava 19

3.2.3. Hrvatska akademska i istraživačka mreža 19

3.2.4. Nacionalni CERT 20

3.2.5. Agencija za zaštitu osobnih podataka 21

3.3. Standardi informacijske sigurnosti 21

3.3.1. Standard ISO 27001:2013 22

3.4. Prijetnje informacijskih sustava 24

3.4.1. Prirodni izvori opasnosti informacijskih sustava 25

3.4.2. Ljudske prijetnje informacijskim sustavima 25

3.4.3. Ostale prijetnje infromacijskom sustavu 30

3.5. Mjere zaštite informacijskih sustava 31

4. ANALIZA SIGURNOSNIH ASPEKATA INFORMACIJSKIH SUSTAVA U TVRTKI ZA INTERNET USLUGE 35

4.1. Općenito o tvrtki i web hostingu 35
4.2. Aspekti sigurnosti 37
4.2.1. Fizička sigurnost poduzeća Totohost d.o.o. 37
4.2.2. Digitalna sigurnost poduzeća Totohost d.o.o. 38
4.3. Napadi na informacijske sustave 42
5. ZAKLJUČAK 44
LITERATURA 45
Knjige: 45
Internet izvori: 45
POPIS SLIKA I TABLICA 46
SAŽETAK 47
SUMMARY 47

1. UVOD

1.1. Definicija problema

Povećanje konkurentnosti jedan je od najvažnijih izazova i zadaća s kojima se poduzeća danas susreću. Za postizanje toga cilja važno je utemeljiti efikasno korištenje i optimizaciju suvremene informacijske tehnologije. 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. Također, uporabom suvremene tehnologije ljudi sve lakše proizvode i dijele znanje jer danas glavni resurs nije kapital već znanje.

Međutim sveprisutna informacijska tehnologija donosi i niz društvenih i etičkih pitanja. Oni se ogledaju u tome kako osigurati zaštitu privatnosti, intelektualnog vlasništva, dostupnost podataka te samim time i sigurnost informacijskih sustava što je tema ovog Završnog rada. Dakle, za uspješno poslovanje svake organizacije ključno je uspostavljanje informacijskog sustava koje će biti efikasno, pouzdano i nadasve sigurno.

Informacijski sustavi neke organizacije mogu biti ustrojeni svjesno s propisanim zakonima, propisima i uputama ili spontano dogovorom ili neformalno nastalom praksom. Naravno, za efikasno funkcioniranje informacijskog sustava trebale bi se poduzeti radnje za njegovu formalnu izgradnju umjesto da se prepusti spontanom razvoju.

1.2. Cilj rada

Cilj rada je objasniti informacijski sustav te analizirati sigurnost informacijskih sustava s teorijskog aspekta te naposljetku na praktičnom primjeru kroz studiju slučaja. Također, cilj je i 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 sustave.

1.3. Metode rada

U ovome radu će se koristiti različite znanstvene metode rada kroz teorijski dio te praktični. U teorijskom dijelu rada će se koristiti sljedeće znanstvene metode: metode analize i sinteze, indukcije i dedukcije, metoda deskripcije, klasifikacije, povijesna metoda te metoda kompilacije. Za potrebe praktičnog dijela rada koristiti će se metoda studije slučaja na primjeru tvrtke koja se bavi Internet uslugama.

1.4. Struktura rada

Rad se sastoji od pet dijelova uključujući uvodni i zaključni.

U uvodnom dijelu biti će biti definirana tema Završnog rada, njegovi ciljevi te metode koje su korištene u izradi ovog rada.

U drugom poglavlju rada će biti riječ o pojmu informacijskih sustava, njegovih dijelova, načela te o vrstama internetskih usluga.

Treći dio obuhvaćat će važnost informacijske sigurnosti, zakonsku regulativu i standarde kojom se uređuje informacijska sigurnost i sigurnost informacijskih sustava. Također će se navesti i objasniti prijetnje informacijskih sustava kao i njegove mjere zaštite.

Četvrti dio će biti studija slučaja. Tvrtka koja je predmet studije slučaja se bavi pružanjem internetskih usluga kao što je web-hosting, iznajmljivanje Internet prostora te izrada web stranica. U studiji slučaja će se na navedenoj tvrtci analizirati način na koji postiže sigurnost svojih informacijskih sustava.

Peti dio će sadržavati zaključak u kojemu će se dati kratki osvrt na temu rada.

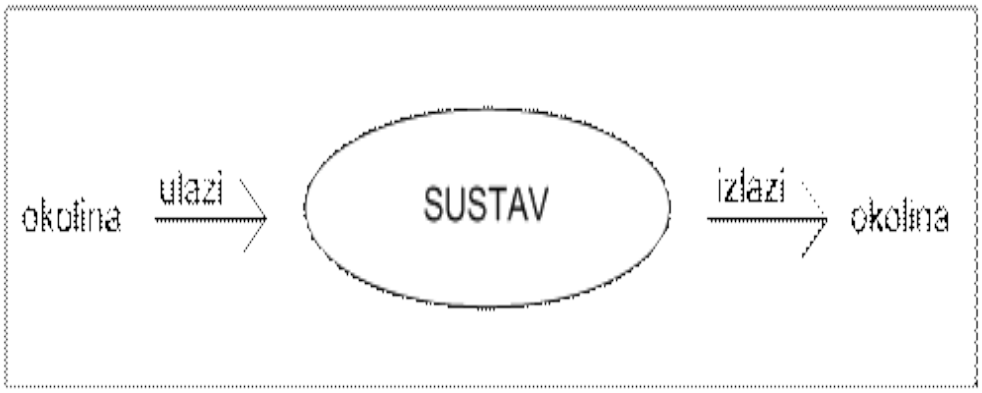
2. UVOD U INFORMACIJSKE SUSTAVE I INTERNET USLUGE

S obzirom na temu ovog Završnog rada u uvodnom dijelu će biti riječ o informacjskim sustavima i njegovim elementima te Internet uslugama.

2.1. Pojam informacijskih sustava

Prije same definicije informacijskih sustava potrebno je objasniti nekoliko pojmova kao što su sustav, podatak i informacija koji će doprinijeti boljem razumijevanju informacijskih sustava.

Pod pojmom sustava podrazumijeva se svaki uređeni skup od najmanje dva elementa koji svojom interakcijom ostvaruju jednostavnu ili složenu funkciju cjeline odnosno ostvaruju neki zajednički cilj. Dio cjeline koji nije obuhvaćen sustavom nazivamo okolinom sustava. Svaki sustav ima četiri elementa: ulaz, izlaz, proces i povratnu spregu (vezu). Dakle, sustavi se sastoje od ulaznih i izlaznih podataka koji se transformiraju izvršnim i upravljačkim procesima te time ispunjavaju postavljeni cilj. Cilj sustava je transformiranje različitih vrsta ulaza u izlaze pri čemu se transformacija obavlja djelovanjem različitih procesa u sustavu.



Slika 1. Prikaz sustava

Izvor: http://www.pfri.uniri.hr

Podatak je skup znakova zapisanih na nekome mediju, primjerice papiru, filmu, magnetskome, optičkome ili poluvodičkome mediju, tehnikom zapisivanja koja je primjerena mediju.[1] Nakon što pročitamo i interpretiramo zabilježeni skup znakova, tj. podatak, dobivamo informaciju odnosno obavijest.

Informacija je novina, odnosno podatak koji primatelju posreduje neku relevantnu novost. Informacija je korisna ako sadrži određenu vrijednost koja će kod primatelja informacije otkloniti određenu neizvjesnost pri odlučivanju. Time navedeno, za kvalitetno odlučivanje potrebne su kvalitetne informacije koje odlikuje točnost, potpunost, primjerenost i pravovremenost.

Objašnjenjem gore navedenih pojmova zaključuje se da sustav u kojem se postupa s podacima i informacijama predstavlja informacijski sustav.

Dakle, informacijski sustav jest sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju i društvo, tao da budu dostupne i upotrebljive svakome kome su potrebne. Informacijski sustav aktivni je društveni sustav koji se može, ali ne mora, koristiti suvremenom tehnologijom.[2] Cilj informacijskog sustava je dostaviti pravu informaciju na pravo mjesto i u pravo vrijeme uz minimalne troškove. Definicija informacijskog sustava najbolje se postiže odgovorom na tri pitanja: što mu je cilj, koje mu su funkcije i od čega se sastoji.[3]

Poslovni informacijski sustav je skup uzajamno povezanih komponenata koje rade zajednički na unosu, obradi, isporuci, pohranjivanju i drugim upravljačkim aktivnostima kojima podatke pretvaraju u informacije namijenjene predviđanju, planiranju, upravljanju, koordinaciji, donošenju odluka i operativnim aktivnostima u organizaciji.[4]

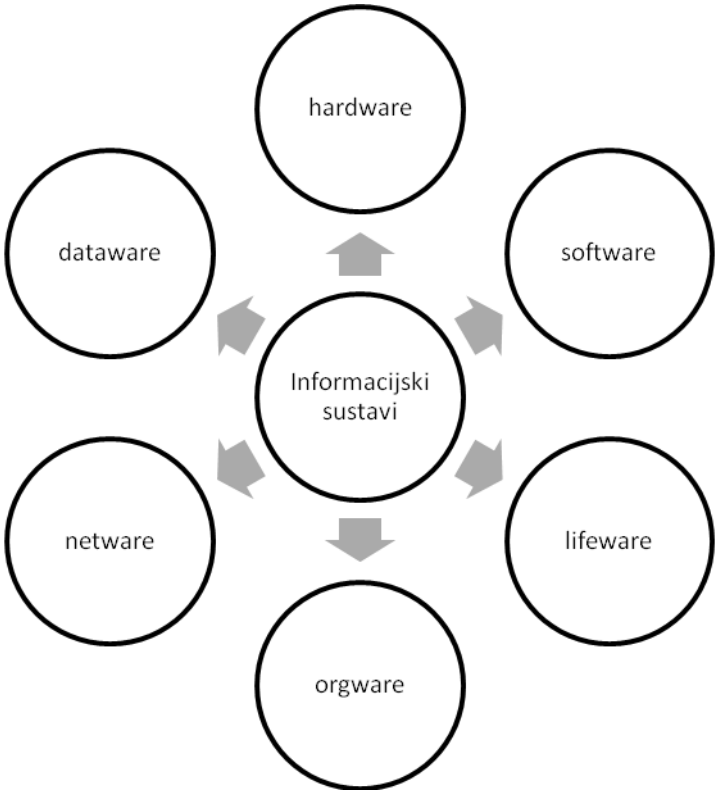
[1] Pejić Bach, M. i dr., (2016.), Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Zagreb str. 3.
[2] Varga, M., (1994.), Društvo za razvoj informacijske pismenosti, Zagreb
[3] Srića, V., (2003.), Uredsko poslovanje: Strategija i koncepti automatizacije ureda, Sinergija, Zagreb
[4] Bocij, P. I dr., (2006), Business Information Systems; Technology, Development & Management for the e-business

2.2. 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:[5]

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]

[5] Panian, Ž., (2005.), Poslovna informatika za ekonomiste, Masmedia, Zagreb, str. 35.
[6] Dragičević, D., (2004), Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb, str. 18.



Slika 2. Komponente informacijskog sustava

Izvor: Prikaz autora

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 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.



Slika 3. Dijelovi informacijskog sustava s obzirom na procese koje podupire

Izvor: Prikaz autora

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

2.3. Načela informacijskog sustava

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.

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.

[8] Dragičević, D., (2004.), Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb

2.4. Internet usluge

Danas je Internet globalna informacijska mreža rasprostranjena na svim kontinentima diljem svijeta sa preko 3,5 milijarde korisnika. Internetu se može pristupiti neovisno o državnim, regionalnim ili drugim teritorijalnim granicama iz skoro svakog dijela svijeta. Svojim uslugama i velikim brojem jednostavnih, jeftinih ili besplatnih programa i aplikacija, Internet je učinio razmjenu informacija i komunikaciju među ljudima daleko lakšom i pristupačnijom nego bilo koje sredstvo u povijesti čovječanstva.

Širenjem Interneta razvijale su se i njegove mogućnosti te danas osim osnovne usluge pristupa Internetu profilirale su se i ostale, standardizirane usluge.

Najvažnije internetske usluge su:[9]

- WWW (World Wide Web)
- E-pošta (e-mail)
- Daljinsko preuzimanje datoteka (FTP)
- Dostavne liste (Mailing List)
- Korisničke diskusijske skupine (Usernet)
- Čavrljanje (Chat)
- VoIP (Voice over IP)
- Internet telefonija
- Videokonferencije
- WAP (Wireless Application Protocol)

World Wide Web (WWW) je rasprostranjen i vrlo popularna softverski sustav, odnosno internetska usluga. Često se pojam WWW-a poistovjećuje pojmom Interneta što naravno nije isto jer je WWW samo jedna od usluga koju omogućava Internet. WWW se zasniva na hipertekstualnim i hipermedijskim dokumentima. Hiperteksutalni dokumenti su skupovi informacija izraženih u tekstualnom obliku čiji su dijelovi logički povezani s dijelovima nekih drugih takvih dokumenta pohranjenih u memoriji istog ili nekog drugog umreženog računala.[10] Sukladno time, hipermedijski dokumenti su skupovi srodnih informacija,

[9] Garača, Ž., (2007), Informatičke tehnologije, Sveučilište u Splitu, Split, str. 218.
[10] Panian, Ž., (2005.), Poslovna informatika za ekonomiste, Masmedia, Zagreb, str. 258.

iskazanih u tekstualnom, grafičkom, video i/ili zvučnom obliku, a koje se također mogu po volji povezivati s dijelovima sličnih takvih dokumenata u memorijama različitih računala. Veze među tim dokumentima se nazivaju poveznicama (eng. link) te zapravo taj hipermedijski sustav čini World Wide Web. Danas je WWW integriran u gotovo svim područjima ljudske djelatnosti kao jedan od najvažnijih izvora različitih informacija. U samom početku WWW je služio kao sredstvo za razmjenu znanstvenih informacija, a danas je jedan od temelja e-poslovanja.

E-pošta je internetska usluga koja omogućava razmjenu elektroničnih poruka između sudionika prijavljenih kod nekog davatelja internetskih usluga koji im je dodijelio odgovarajuću adresu. Prije nastanka Interneta e-pošta postojala je kao telekomunikacijska usluga, ali bila je omogućena samo velikim poslovnim sustavima. Nastankom Interneta i njegovim razvojem uspostavljen je jedinstveni standard za elektroničku poštu, te je danas neizostavan alat u svakodnevnom poslovanju. Najprivlačnija obilježja e-pošte je jednostavnost pri uporabi i primjerenost svakodnevnim komunikacijskim potrebama poslovnih i privatnih korisnika

Daljinsko preuzimanje datoteka je usluga namijenjena prijenosu digitalnih sadržaja koji nisu hipermedijski dokumenti već datoteke različitih vrsta i sadržaja. Koristi se za različite svrhe, a najčešće su: prijenos binarnih datoteka između udaljenih računala, prijenos tekstualnih datoteka između udaljenih računala, preuzimanje programa s udaljenih računala, te prijenos multimedijskih datoteka.

Treba napomenuti da se prilikom korištenja servisa daljinskog prijenosa datoteka uz očekivani sadržaj može preuzeti i računalni virusi koji napadaju i inficiraju računala na koje se prenosi datoteka. Srećom, danas uz postojanje širokog spektra antivirusnih programa i zaštite lako se može zaštititi od virusnih prijetnji.

Dostavne liste je usluga kontinuiranog primanja novosti iz nekog područja od interesa za korisnika. Poslužitelj dostavnih lista zadužen je za prosljeđivanje sadržaja svim pretplatnicima na taj servis koji može biti besplatan i plaćeni. Nadzor nad radom dostavne liste mogu obavljati ljudi ili programi. Radi li se o dostavnim listama koju administriraju ljudi, komunikacija je slobodnija i ne zahtijeva striktno pridržavanje pravila. U robotiziranoj listi su pravila puno restriktivnija te se poruke zasnivaju na ključnim riječima. Navedeno time,

dostavne liste mogu biti realizirane kao potpuno slobodne liste, kao liste sažetaka i kao posredovane liste.

Korisničke diskusijske skupine oblik su korištenja Interneta koji omogućava formiranje diskusijskih skupina na temelju zajedničkih interesa. Na prvi pogled ova usluga je slična dostavnim listama, ali se razlikuje u tome što rasprava u diskusijskim skupinama nije ničim ograničena tj. ne postoji posrednik ili moderator koji bi vodio njen smjer ili priječio neke njezine oblike. Preciznije rečeno, moderatori su sami sudionici u diskusijskoj skupini.

Čavrljanje je popularna internetska usluga koja se razvila iz elektroničke pošte te organizirana na način da davatelj usluge, u ovom slučaju je to Internet Relay Chat (IRC), prihvaća pozive korisnika koji žele stupiti u izravni online kontakt s nekim drugim korisnikom. Sudionici komuniciraju na pisani način kao i kod elektroničke pošte, ali u realnom vremenu odnosno izravnim dijalogom.

Internet telefonija, zapravo jako slična čavrljanju, je usluga koja se razvila izravno iz klasične telefonije te omogućava izravno povezivanje dva korisnika i vođenje razgovora preko Interneta. Posredovanje IRC poslužitelja ovdje nije nužno, ako se točno zna s kime se želi razgovarati i koja mu je adresa. Razgovor između korisnika je zapravo isti kao kod običnog telefonskog razgovora. Naravno, računala komunikatora moraju biti opremljena uređajima za govorni ulaz i izlaz.

VoIP tj. glas preko Internet protokola, kodira standardne glasovne signale korištenjem Internet protokola, odnosno paketnog prijenosa podataka.

Videokonferencije su internetska usluga koja omogućava dvosmjerno audiovizualno komuniciranje dva ili više udaljenih korisnika.

WAP ili protokol bežičnih aplikacija je tehnologija dizajnirana da omogući korisnicima mobilnih terminala brz i efikasan pristup Internetu.

Neke od navedenih internetskih usluga su već pomalo zastarjele, te se ne koriste često jer se mogućnosti Interneta sve više šire tako se i njegove usluge prilagođavaju i mjenjaju u korak sa suvremenom informatičkom tehnologijom.

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.[11] 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.

[11] 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.[12]



Slika 4. Sigurnosni trokut

Izvor: http://panmore.com

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.[13] 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.

[12] http://panmore.com/the-cia-triad-confidentiality-integrity-availability
[13] 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:[14]

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.

[14] 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.[15] Zakon se

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

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 su 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 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.[16] 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:[17]

- 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.

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.[18] Njegova svrha je zaštita privatnog života i ostalih ljudskih prava i temeljnih

[16] https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
[17] https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
[18] https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka

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.[19] Mjere i standardi informacijske sigurnosti se odnose na sigurnosne provjere osoblja, 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.

[19] http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html

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.[20] 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.

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.[21]

[20] https://www.zsis.hr/default.aspx?id=13
[21] http://www.carnet.hr/o_carnetu/o_nama

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 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 općeprihvaćeni 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:[22]

- 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 sljedi.

3.3.1. 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).

Standard se sastoji od 14 dijelova:[23]

1. Politike informacijske sigurnosti (obuhvaća smjernice i podršku uprave za informacijskom sigurnosti)

[22] M., Spremić, (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 108.
[23] M., Spremić, (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 112.

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)
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. Izvori prijetnji mogu biti:

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 1. Izvori opasnosti i rizika u informacijskome sustavu[24]

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

Svaka od navedenih prijetnji može prouzročiti velike gubitke za poslovanje ukoliko se na adekvatan način ne pristupi mjerama zaštite informacijskih sustava i njegove okoline. 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.

[24] Prema: Srića, V. i suradnici, Menedžerska informatika, MEP Consult, Zagreb, 1999.

3.4.1. Prirodni izvori opasnosti informacijskih sustava

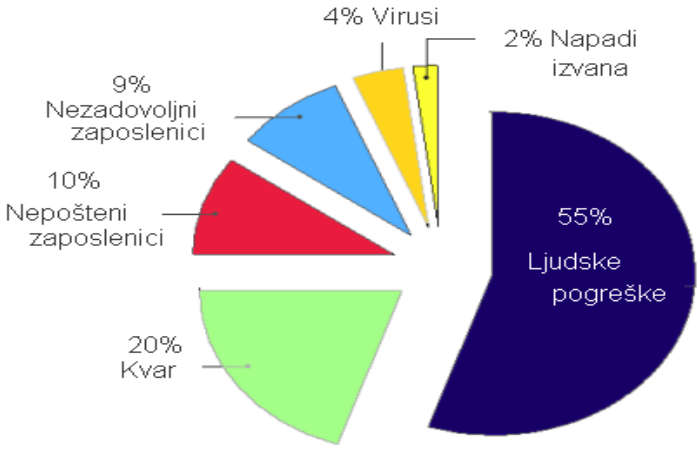
U skupinu prirodnih prijetnji spadaju meteorološke, geofizičke nepogode, sezonski fenomeni, astrofizički fenomeni te biološke prijetnje.[25]

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

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.[26]

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



Slika 5. Prijetnje sigurnosti informacijskih sustava

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

Gore prikazana slika 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.[27] Prema procjenama američkog Federalnog istražnog ureda (FBI) tek se oko 5 % informatičkog 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:[28]

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

[27] Panian, Ž., (2005.), Poslovna informatika za ekonomiste, Masmedia, Zagreb, str. 314.
[28] Panian, Ž., (2005.), Poslovna informatika za ekonomiste, Masmedia, Zagreb, str. 315.

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 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:

- 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.

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 prirodnim djelovanjem. Te prijetnje su: eksplozija, prašina, poplava, gubitak električnog napajanja te elektromagnetska radijacija.[29] 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.

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

3.5. Mjere zaštite informacijskih sustava

Najčešće mjere zaštite kojima se štite tri ključna parametra informacijske sigurnosti su:

- Povjerljivost se ostvaruje primjenom zaštitnih kontrolnih mjera pristupa informacijskome sustavu korištenjem kontrolnih mjera identifikacije i autorizacija korisnika (metode logičke, fizičke i biometrijske mjere zaštite, geolokacijske mjere zaštite, dodjele ovlasti)
- Integritet se ostvaruje zaštitom podataka pri prijenosu (dinamički podaci) i zaštitom podataka u mirovanju (statički podaci) uz primjenu metoda kao što su šifriranje podataka, sigurnosni protokoli prijenosa podataka, kao što su https, ssl, end-to-end enkripcija i slični, e-potpis, zaštita pristupa računalnoj mreži itd.
- Dostupnost ili raspoloživost se ostvaruje primjenom kontrola vezanih za upravljanje kontinuitetom poslovanja, dostupnosti sustava i njegovih resursa i metodama oporavka poslovanja nakon neželjenoga događaja.

U daljnjem tekstu će biti opisane mjere zaštite informacijskih sustava kao što su fizička zaštita, provjera pristupa, biometrijska i antivirusna zaštita, kriptografija, vatrozid (firewall), sigurnosne kopije (backup) te digitalni potpis.

Fizička zaštita informacijskih sustava obuhvaća skup metoda i sredstava koji se koriste radi zaštite materijalne osnovice informacijskog sustava počevši od neovlaštenoga fizičkog pristupa sustavu i korištenje njegovih resursa do njegove zaštite od djelovanja vanjskih događaja čije se nastupanje ne može predvidjeti (zaštita od naponskih, strujnih udara, od prekida rada zbog nestanka električne energije i sl.). Fizička sigurnost je najvažniji element zaštite, a obuhvaća kontrolu zaštite prostorija, postrojenja, zgrada i druge imovine. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara[30] (postrojenja, uredi, objekti, zgrade). Fizička zaštita se, osim na materijalne dijelove informacijskog sustava, odnosi i na zaštitu ljudi i informacija, iako se na njih odnose i druge mjere zaštite.

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

Ciljevi fizičke sigurnosti su sprječavanje neautoriziranih pristupa računalnom sustavu, sprječavanje krađe podataka s računalnih sustava, zaštita integriteta podataka pohranjenih na računalu i sprječavanje gubitaka ili oštećenje podataka prilikom nepogoda ili nesreća.

Provjera pristupa je jedan od najčešćih načina zaštite informacijskih sustava od neovlaštenog pristupa i korištenje njihovih resursa. Pritom se ne misli na fizički pristup sustavu, koji je predmet fizičke zaštite, već na mrežni ili neposredni daljinski pristup putem komunikacijskih kanala. Sastoji se od identifikacije korisnika (ima li pravo pristupa) i autorizacija (koja su njegova ovlaštenja).

Korisnik najčešće mora upisati svoju šifru (password) i korisničko ime (user name). Postoje sustavi koji omogućuju korištenje sigurnijih metoda radi zaštite pristupa sustavima kojima se identifikacija provodi uz pomoć uređaja kojima se identitet korisnika provjerava magnetskim karticama, analizom otiska prsta ili dlana, provjerom zjenice oka, analizom glasa, potpisa i sl. Zloupotrebe kod provjere pristupa uglavnom se izvode unutar samog sustava te uglavnom počinitelja nije teško otkriti. Česta greška korisnika informacijskog sustava leži u lošem odabiru lozinke ili nemarnom odnosu prema njezinom sadržaju. Da bi provjera pristupa bila djelotvorna jedan od uvjeta je da korisnici imaju odgovarajuće lozinke. Pravilno postavljanje lozinke obuhvaća pravilan odabir lozinke, redovito mijenjanje lozinke, enkripciju lozinke pri komunikaciji kao i zaštitu datoteka lozinkama. Za bolju sigurnost mogu se koristiti jednokratne lozinke ili lozinke koje su vremenski ograničene. Moguće su također i kombinacije lozinke i kartice kao što je slučaj kod korištenja bankomata.

Biometrijska zaštita se temelji na primjeni biometrijskih uređaja koji provode identifikaciju korisnika temeljem njihovih jedinstvenih fizičkih obilježja. To su fizički uređaji koji skeniraju prst, dlan, rožnicu oka pa čak DNK strukturu, otkucaje srca i sl. da bi se predstavili informacijskom sustavu. Nakon što uređaj očita podatke odobrava ili uskraćuje pristup.

Kriptografske metode su sredstvo zaštite podataka pri čemu podaci mogu biti pohranjeni unutar memorije računala, na nekom drugom mediju ili se prenositi putem mreža ili udaljenih računalnih sustava. Cilj ove metode je osiguravanje tajnosti podataka kako njihov sadržaj ne bi došao u ruke neovlaštenim osobama. Danas, u uvjetima moderne i visoke tehnologije gdje se kao glavni način komuniciranja koriste internetske i računalne mreže, ovakve metode su iznimno važne kako bi se zaštitila privatnost građana i povjerljivost podataka, osigurala

nesmetana razmjena podataka unutar informacijskog sustava, kao i njihova komunikacija s okolinom.

Antivirusna zaštita ili antivirusni program koristi se za sprječavanje, prepoznavanje i uklanjanje zlonamjernih programa kao što su računalni virusi, računalni crvi, trojanski konji, špijunski programi ili oglašivački programi. Antivirusne mjere zaštite se razmatraju, planiraju, utvrđuju i provode kao zaseban segment cjelokupnog sustava osiguranja i zaštite informacijskog sustava od navedenih zlouporaba. Antivirusne mjere je potrebno provoditi što češće kao dio rutinskih operativnih procedura u svakodnevnome radu informacijskog sustava. Ponekad, antivirusni programi mogu imati i negativne posljedice na informacijske sustave jer mogu umanjiti performanse računala neznanjem korisnika koji ne razumiju zahtjeve i upite koje antivirusna zaštita donosi što može dovesti do proboja sigurnosti.

Vatrozid ili obrambeni zid, a popularno znan kao firewall, je softverski ili hardverski bazirana zaštita računalne mreže s primarnom ulogom kontrole dolaznoga i odlaznoga prometa mreže. Analizira podatkovne pakete koji pristižu prema mreži i prema unaprijed utvrđenim sigurnosnim pravilima provjerava smije li ili ne smije podatkovni paket ući u štićeni dio mreže, predstavljajući svojevrsnu branu koji u unutarnji tj. branjeni dio mreže propušta samo sigurnosno ispravan sadržaj. Dakle, vatrozid stvara most između lokalne mreže za koju se smatra da je pouzdana i sigurna i druge vanjske mreže, kao što je Internet, koja je najčešće nepouzdana i nesigurna.

Sigurnosne kopije (backup) podrazumijevaju redovnu pohranu podataka i programa i njihovo čuvanje na zaštićenom mjestu. Preduvjet su sigurnosti informacijskih sustava i jedna su od najjednostavnijih metoda za otklanjanje štetnih posljedica uslijed namjernog ili slučajnog brisanja ili mijenjanja podataka. Ova vrsta zaštite ne pruža izravnu obranu od napada, ali redovitim arhiviranjem podataka omogućuje se lako i efikasno vraćanje stanja prije nekog zlonamjernog napada.

Digitalni potpis je zaštitna mjera koja osigurava autentičnost i integritet podataka. To je elektronički generirani potpis čija je svrha jamčenje autentičnosti sadržaja poruke, čime dokazuje da poruka nije mijenjana na putu od pošiljatelja do primatelja te jamči identitet pošiljatelja.

Zakonska regulativa digitalnog potpisa neovisna je o tehnologiji i utvrđuje formalne zahtjeve koje korištena tehnologija mora zadovoljiti:[31]

- digitalni potpis mora biti jedinstven za osobu koja ga koristi,
- mora postojati mogućnost provjere kome digitalni potpis stvarno pripada te
- digitalni potpis mora osigurati i sebe i podatke koje potpisuje te postupkom verifikacije osigurati mogućnost provjere autentičnosti poruke.

Kako je već prije navedeno, prijetnje informacijskim sustavima najviše su generirane od strane zaposlenika i to zbog lakoće pristupa istima ipak predstavljaju napade koje je uglavnom lako za otkriti. Za razliku od takvih prijetnji, prijetnje putem računalnih mreža zbog inovativnost i domišljatost napadača u pronalaženju propusta sustava i kreiranje sve razornijih malicioznih programa otežavaju da se počinitelji otkriju i primjerno kazne. Nažalost, danas ne postoji ni jedan informacijski sustav ili sustav općenito za kojeg se može reći da je siguran. Zato se svaka organizacija mora usmjeriti na poboljšanje postojećih i uvođenje novih mjera zaštite da bi se ostvarila što veća sigurnost.

[31] M., Spremić, (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb, str. 161.

4. ANALIZA SIGURNOSNIH ASPEKATA INFORMACIJSKIH SUSTAVA U TVRTKI ZA INTERNET USLUGE

Za potrebe pisanja ovog dijela rada bilo je potrebno istražiti aspekte sigurnosti informacijskih sustava na primjeru tvrtke Totohost d.o.o. koja se bavi pružanjem Internet usluga. Prikupljanje podataka za studiju slučaja obavilo se razgovorom s vlasnikom tvrtke kao i njezinim zaposlenicima od čije velike pomoći je bila osoba zadužena za tehničku podršku. Osim intervjua sa djelatnicima tvrtke do određenih podataka sam došla opažanjem, prvenstveno o aspektima fizičke sigurnosti. Korištenje Interneta je također bilo potrebno za izradu ovog dijela rada.

4.1. Općenito o tvrtki i web hostingu

Totohost d.o.o. za Internet usluge sa sjedištem u Korčuli osnovano je 10. veljače 2014. godine te temeljna djelatnost navedene tvrtke je pružanje usluga Internet poslužitelja (web hosting) i registracija domena. U razdoblju između 2005. i 2014. godine poduzeće je poslovalo kao obrt obavljajući istu djelatnost, ali da bi imao mogućnost postati ovlašteni registar „.hr“ domena osnovan je Totohost d.o.o. jer sukladno pravilima CARNeta obrt ne može biti ovlašteni registar .hr domene. Danas je jedini ovlašteni registar .hr domene na nekom hrvatskom otoku i jedini u Dubrovačko-neretvanskoj županiji.



Slika 6. Totohost logo

Izvor: http://www.lunatron.eu

Poduzeće u 2015. godini je imalo jednog zaposlenika, te u skladu s definicijom malih i srednjih poduzeća Komisije EU spada u skupinu mikro poduzeća. Danas Totohost d.o.o. ima četiri zaposlenika uključujući i vlasnika poduzeća.

Rast obujma poslovanja praćen je i rastom broja klijenata koji se kroz godine kontinuirano povećavao. Poduzeće je započelo rad kada je imalo ugovorena četiri klijenta, a sada ih ima preko 3300. Poduzeće u budućnosti planira proširiti svoje poslovanje na područje Europske unije, posebice Njemačko, Austrijsko i Slovensko tržište na kojima već ima uspostavljene kontakte s potencijalnim klijentima.

Poduzeće planira implementirati sustav upravljanja sigurnošću i informacijama ISO 27001 te sustav upravljanja kvalitetom ISO 9001. Navedeno bi izravno omogućilo povećanje pouzdanosti i sigurnosti usluga što je izuzetno bitno s obzirom na djelatnost poduzeća. Time bi se omogućilo povećanje povjerenja klijenata što dovodi do jačanja lojalnosti postojećih, ali i većeg broja novih.

Web hosting je usluga zakupa prostora na Internet poslužitelju, odnosno serveru. Poduzeće Totohost iznajmljuje korisnicima hosting pakete, odnosno unaprijed definirane pakete (prostor na serveru). Paketi se razlikuju po svojim specifikacijama, koje mogu biti količina dostupnog prostora u MB/GB, količina dozvoljenog mjesečnog prometa, broj e-mail adresa koje korisnik može otvoriti, broj baza podataka koje može koristiti i sl. Usluge koje nudi su potpuno u skladu sa tehnološkim standardima. Kao pružatelj web hosting usluge poduzeće se brine za sigurnost Internet stranica klijenata, pruža tehničku podršku web dizajnerima u svakodnevnom radu te održava servere kako ne bi došlo do nedostupnosti web stranica klijenata.

4.2. Aspekti sigurnosti

Kada govorimo o sigurnosti kao najvećem i najvažnijem aspektu poslovanja istu možemo podijeliti na dvije jasne cjeline:

- fizička sigurnost, te
- digitalna (softverska) sigurnost.

4.2.1. Fizička sigurnost poduzeća Totohost d.o.o.

Fizička sigurnost se odnosi na zaštitu poslovanja putem raznih fizičkih mjera kao što su sigurnosno-protuprovalni sustav, sigurnosna vrata, kamere, itd.

Tvrtka Totohost je locirana u središtu grada na katu zgrade, ulaz je skriven u ulici te je pozicijski primamljiv za protuprovalne radnje. Stoga je tvrtka opremljena sa protuprovalnim sustavom koji sačinjavaju dobro pozicionirani senzori za pokret te tri kamere koje pokrivaju cijeli poslovni prostor. Također je strateški postavljeno osvjetljenje koje se aktivira prilikom provale da obeshrabri provalnika i privuče vanjsku pozornost. Prilikom provale sistem također odašilje zvuk velike jačine i frekvencije. Kako je sistem ovisan o električnoj energiji i ista mu je najveća slabost (prilikom nestanka struje ništa ne bi radilo) sve je pogonjeno s više USP baterija koje omogućavaju nesmetan rad i to do osam sati prilikom nestanka električne energije.

Prostor je također opremljen sa tri vatrogasna aparata punjenim ugljičnim dioksidom i količinom sredstva za gašenje u iznosu od šest kilograma koji služi za učinkovito gašenje plamena posebno na elektroničkoj opremi i instalacijama. Postavljen je i dimni alarm za bržu detekciju i reagiranje u slučaju požara.

Pojačana vrata i dvostruka brava su dodatne zaštite koje ovaj prostor čine fizički sigurnim.

4.2.2. Digitalna sigurnost poduzeća Totohost d.o.o.

Kada govorimo o digitalnoj sigurnosti ovo je tema koja je opsežnija od prve i kojoj je tvrtka Totohost predana u najvećoj mjeri zbog povećane zloupotrebe navedenih sustava putem Internet mreže tj. digitalnim oblikom.

Totohost kao tvrtka koja je u posjedu servera koji lokacijski nisu na istom mjestu kao i fizičko mjesto poslovanja već dugi niz godina ide u korak s vremenom i novim sigurnosnim standardima u pogledu softvera koji pogoni servere i sve fizičke komponente.

Također, tvrtka u svom uredu ima privatni server koji se sastoji od 10 SSD diskova kapaciteta 1TB gdje se drže sigurnosne kopije (backup) od hosting servera i koji ujedno i služe kao backup server za sva računala unutar tvrtke u slučaju kvara. Za nesmetan i siguran rad servera i njegovih komponenti, temperatura se regulira pomoću ventilatora koji osiguravaju adekvatno hlađenje.



Slika 7. Prikaz servera

Izvor: india.resellerclub.com

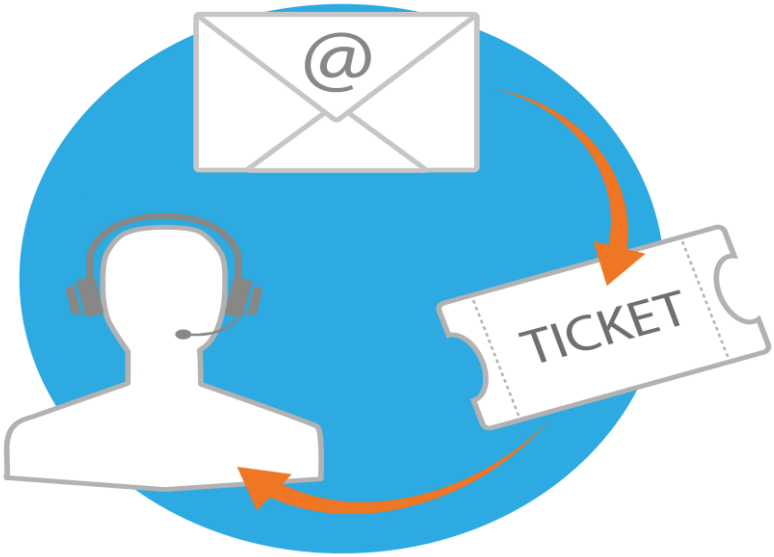
Kao najvažnije aspekte digitalne sigurnosti čak ne bih navela nadogradnje kao najvažnije već dvije stvari: backup i testiranje. To su zapravo i najvažnije mjere sigurnosti koje poduzeće navodi.

Prilikom nadogradnje mnogo toga može poći po zlu, a napravivši backup (sigurnosnu kopiju) osigurali ste mogućnost vraćanja u „prošlost“ na funkcionalne i ispravne postavke koje su testirane i valjane. Navedeno je neprocjenjivo u današnjem poslovanju zbog rastućih opasnosti koje su ubačene povećanjem dostupnih aplikacija i softvera.

Testiranje je također od iznimne važnosti jer nadogradnje donose mnoge prednosti i sigurnosne zakrpe, ali donose i mogućnost grešaka (bugova) i nekompatibilnost sa nekim postavkama na serveru bilo da govorimo o operacijskom sustavu ili drugim podsustavima.

U Totohost okruženju je postavljeno da svaka MAC adresa (fizička adresa) ima dodijeljenu točno određenu IP adresu i samo ta IP adresa ima dopuštenje za spajanje u upravljačko sučelje i konzole na serverima. Tako da se samo unutar ureda ostvaruje mogućnost spajanja na sučelja tj. konzole. Također, tu se nalazi i fizička komponenta koja služi kao interni vatrozid koji regulira i kontrolira spajanje na mrežu iz vanjskih izvora, te predstavlja još jedan sloj sigurnosti u poslovanju poduzeća.

Totothost ima ticket sustav koji je organiziran da pri primitku email-ova koje korisnik šalje u svrhu rješavanja problema dodjeljuje broj tiketa/upita koji se na taj način organizira i prati do finaliziranja slučaja.



Slika 8. Prikaz ticket sustava

Izvor: promlmsoftware.com

Totohost kao vatrozid, na svim serverima, koristi CSF tj. ConfigServer Security & Firewall. CFS je vatrozidna konfiguracijska skripta stvorena kako bi osigurala bolju sigurnost poslužitelju. CFS konfigurira vatrozid poslužitelja za zaključavanje javnog pristupa uslugama i dopušta samo određene veze, kao što su provjera pošte, učitavanje web stranica i sl. ConfigServer Firewall koji poduzeće koristi također dolazi s uslugom koja se zove Login Failure Daemon ili skraćeno LFD. LFD gleda korisničku aktivnost zbog prekomjernog kršenja prijave koji se obično događaju prilikom brute force napada. Ako se pojavi velika količina prijava zbog neuspjeha s iste IP adrese, taj će se IP privremeno blokirati iz svih servisa na poslužitelju. IP blokade će automatski isteći, no takve IP adrese mogu se ukloniti i ručno. Osim uklanjanja, CFS omogućuje i ručno dopuštanje IP adresa.

Kao antivirusnu platformu koriste Apache SpamAssassin koja administratorima sustava omogućuje filtriranje e-pošte i blokiranje neželjene poruke.

Tehnička podrška poduzeća rješava specifične probleme s proizvodom ili uslugom, a ne pružanjem obuke ili prilagodbe klijentima. Tehnička podrška se može dostaviti putem elektroničke pošte, softvera za podršku uživo na web stranici ili alatom kojim se prijavljuje incident tzv. ticket.

Inače, Totohost na serverima koristi CENTOS linux distribuciju sa instaliranim podsustavom CloudLinux OS-om koji se temelji na OpenVZ kernelu i potpuno je kompatibilan s CentOS/RHEL paketima. CloudLinuxOS je dizajniran za poboljšanje stabilnosti i sigurnosti na poslužitelju i optimiziranje rada sa izoliranjem korisnika na poslužitelju, postavljanje granica korištenja resursa za njih, optimiziranja rada s bazama podataka itd.

Kada govorimo o podsustavima ima ih mnogo, a neki od njih su: CageFS, cPanel te WHM.

CageFS – je virtualizirani datotečni sustav i skup alata koji sadržavaju svakog korisnika u vlastitom „kavezu“. Svaki kupac ima svoje potpuno funkcionalne CagFS kaveze sa svim datotekama sustava, alatima i sl.



Slika 9. CageFS – korisnici u „kavezu“

Izvor: cloudlinux.com

Prednosti CageFS-a su:

- korisnicima su dostupni samo sigurni programi,
- korisnik neće vidjeti druge korisnike i neće moći otkriti prisutnost drugih korisnika i njihovih korisničkih imena na poslužitelju,
- korisnik neće moći vidjeti datoteke konfiguracije poslužitelja te,
- korisnici će imati ograničen prikaz sustava i neće moći vidjeti druge procese korisnika.

Istodobno će korisnikova okolina biti potpuno funkcionalna, a korisnik ne bi smio ni na koji način biti ograničen.

cPanel je online Linux-based web hosting upravljačka ploča koja pruža grafičko sučelje i alate za automatizaciju. Osmišljen je kako bi pojednostavnio proces hostinga web stranice. cPanel koristi strukturu od tri razine koja pruža administratorima, prodavačima i vlasnicima internetskih stranica za kontrolu različitih aspekata administriranja web stranica i poslužitelja putem standardnog web preglednika.

WHM ili upravitelj web hostova je snažan program koji omogućuje administrativni pristup stražnjem dijelu cPanela. WHM daje puno više kontrole i fleksibilnosti prilikom upravljanja nekim vrlo popularnim i resursima bogatim web mjestima ili velikim brojem stranica.

Također je bino napomenuti da Totohost na svim svojim serverima primjenjuje i upotrebljava važeće SSL (Secure Socket Layer) certifikate u suradnji sa poznatom tvrtkom koja izdaje iste Comodo inc.



Slika 10. SSL certifikat

Izvor: https://southeastpublications.com

SSL certifikati omogućuju sigurnosnu vezu između poslužitelja i korisnika pri čemu nije moguće presretanje od treće strane što je krajnje potrebno kada se razmjenjuje sigurnosno osjetljivi sadržaj poput osobnih podataka,podaci o karticama pri kreditnim plaćanju, itd.

4.3. Napadi na informacijske sustave

Najčešći napadi na poduzeće su DdoS, phising, napad grubom silom tzv. brute force attack te exploit/injection napadi. Budući da potonji napad nije opisan u prethodnom dijelu rada, radi se o napadu koji koristi sigurnosne propuste u starijim nadogradnjama određenih operacijskih sustava i aplikacija. Općenito je uzrokovan ubacivanjem malicioznog koda u izvršavajuće skripte ili datoteke.

Zadnji DDoS napad dogodio se 03.10.2016., te je primijećen pad sustava, a uspješno je mitigiran tj. otklonjen već isti dan. Uzročnik istog je proistekao sa raznih IP adresa uglavnom kineskog podrijetla. Administrator je logiranjem u konzolu kod data (podatkovnih) centara (Hetzner), lociranog u Njemačkoj, utvrdio da se sa više IP adresa šalje velika količina podataka što uzrokuje prestanak rada sustava. Kontaktiran je navedeni podatkovni centar za rješavanje navedenog problema.

DoS napadi na servere ne događaju se često, a jedini zabilježeni slučaj je bio prije deset godina.

Phishing i exploit/injection napadi su najčešći s obzirom na nemar klijenata koji na svoje hosting pakete instaliraju neprovjerene sadržaje i aplikacije te ne nadograđuju svoje CMS-ove i „plug in-ove“ koje dotične osobe iskorištavaju.

Totohost svakodnevno ima probleme gdje dotične osobe ili botovi (automatizirane aplikacije ili programi) inficiraju hosting pakete od naših klijenta raznim malware, phishing, malicioznim PHP skriptama, itd. zato i nevezano od strane korisnika se rade sigurnosne kopije.

Brute force napadi su manje česti iako prevladavaju u većoj mjeri upravo zbog ne pridržavanja klijenata određenom nivou sigurnosnih standarda. Navedeni problem rješavaju informirajući klijente o očekivanoj sigurnosnoj razini lozinki koju žele da primjenjuju jer pošto se navedene primjenjuju na CMS-ovima, aplikacijama koje korisnik osobno instalira, na njima nemaju direktnu kontrolu u vezi ovog pitanja.

5. ZAKLJUČAK

Danas, kada su suvremena otkrića i nova tehnologija postala naša svakodnevnica, kako u životu tako i u poslovnom smislu, biti na vrhu znači uspješno i pametno koristiti tehnologiju koja nam je pružena.

U poslovnom smislu utječe na ono najvažnije, odanost kupaca, napredak, konkurentnost na tržištu, ali i samu komunikaciju između poslovnih subjekata, zaposlenih i suradnika. Uz navedeno, još neki od važnijih ciljeva informacijskih tehnologija predstavljaju pružanje sigurnosti korisnika, te brže i uspješnije izvršavanje zadataka uz minimalne troškove.

Vjerujem, kako će se već u bliskoj budućnosti prirodne, a i one ljudske prijetnje svesti na minimum, te kako će mnoga poduzeća koja nisu dosada uvidjela važnost primjene odgovarajućih informacijskih tehnologija na području informacijske sigurnosti to u doglednoj budućnosti uspjeti kako ih sama konkurencija ne bi uništila.

Ova tema je zasigurno važna u sadašnjosti, ali i budućnosti na domaćem i svjetskom tržištu. Velikim dijelom postaje bitna kako najpoznatijim tvrtkama na svijetu tako i onim manjima jer ulažući u što bolju sigurnost informacijskih sustava idu ka cilju koji ih zapravo i vodi, biti prvi i vodeći.

LITERATURA

Knjige:

1. Bocij, P. I dr., (2006), Business Information Systems; Technology, Development & Management for the e-business
2. Conry-Morray, A. i Weafer, V., (2005.), Sigurni na Internetu, Miš, Zagreb
3. Dragičević, D., (2004.), Kompjutorski kriminalitet i informacijski sustavi, IBS, Zagreb
4. Garača, Ž., (2007.), Informatičke tehnologije, Sveučilište u Splitu, Split
5. Panian, Ž., (2005.), Poslovna informatika za ekonomiste, MASMEDIA, Zagreb
6. Panian, Ž. i Spremić, M., (2007.), Korporativno upravljanje i revizija informacijskih sustava, Sveučilište u Zagrebu, Zagreb
7. Pejić Bach, M. i dr., (2016.), Informacijski sustavi u poslovanju, Sveučilište u Zagrebu, Zagreb
8. Spremić, M., (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Zagreb
9. Srića, V. i dr., (2003.), Uredsko poslovanje: Strategija i koncepti automatizacije ureda, Sinergija, Zagreb
10. Varga, M., (1994.), Društvo za razvoj informacijske pismenosti, Zagreb

Internet izvori:

1. http://azop.hr/prava-ispitanika/detaljnije/zastita-osobnih-podataka
2. http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html
3. http://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html
4. http://panmore.com/the-cia-triad-confidentiality-integrity-availability
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.pfri.uniri.hr/~tudor/materijali/Informacijski%20sustavi,%20baze%20podataka.htm
8. https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka
9. https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
10. https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
11. https://www.zsis.hr/default.aspx?id=13

POPIS SLIKA I TABLICA

Slika 1. Prikaz sustava (str. 3.)

Slika 2. Komponente informacijskog sustava (str. 6.)

Slika 3. Dijelovi informacijskog sustava s obzirom na procese koje podupire (str. 7.)

Slika 4. Sigurnosni trokut (str. 13.)

Slika 5. Prijetnje sigurnosti informacijskih sustava (str. 26.)

Slika 6. Totohost logo (str. 35.)

Slika 7. Prikaz servera (str. 38.)

Slika 8. Prikaz ticket sustava (str. 39.)

Slika 9. CageFS – korisnici u „kavezu“ (str. 41.)

Slika 10. SSL certifikat (str. 42.)

Tablica 1. Izvori opasnosti i rizika u informacijskome sustavu (str. 24.)

SAŽETAK

U današnje vrijeme uporaba informatičke tehnologije je implementirana u sve spore društva, kako privatnog tako i poslovnog. U poslovnom svijetu uporaba suvremene informatičke tehnologije predstavlja jedan od temelja konkurentnosti te samog uspjeha na tržištu. Stoga bi imperativ svake organizacije trebao biti informacijskih sustav koji će biti efikasan, ekonomičan i siguran, a čija će primjena biti od strateške važnosti za poduzeće. Zbog činjenice da informacijski sustavi sadržavaju mnoštvo podataka važnih za poslovanje javlja se problem zaštite istih. Naime, bržim rastom informatičkih tehnologija nastaju i veće prijetnje informacijskih sustava te dolazi do ugroze sigurnosti informacija u vidu njihove povjerljivosti, cjelovitosti i raspoloživosti. Svaka prijetnja može bitno ugroziti kontinuitet poslovanja te izazov svake organizacije bi trebao biti kako na njega odgovoriti primjenom različitih metoda i mjera zaštite.

Ključne riječi: informatičke tehnologije, informacijski sustavi, sigurnost

SUMMARY

At present, the use of IT technology has been implemented in all the spores of society, both private and business. In the business world, the use of modern IT technology represents the pillar stone in terms of competition and success on the market. Therefore, the imperative of every organization should be information system that is efficient, cost-effective and secure, whose application will be of strategic importance to the enterprise. Due to the fact that information systems contain a variety of information of great importance for business, the problem of security is relevant. The faster the growth of information technology is, greater are the threats for information system which endagers the information security in terms of confidentiality, integrity and availability. Any threat can significantly jeopardize business continuity and challenge of each organization should be how to respond to it by applying different methods and measures of protection.

Key words: information technology, information systems, security