# Rizici primjene informacijske tehnologije u poslovanju

**Jakovac, Nikola**

**Undergraduate thesis / Završni rad**

**2016**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Polytechnic Nikola Tesla in Gospić / Veleučilište Nikola Tesla u Gospiću**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:107:614236

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

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

*Repository / Repozitorij:*

Polytechnic Nikola Tesla in Gospić - Undergraduate thesis repository

zir.nsk.hr

Image not found or type unknown

**VELEUČILIŠTE „NIKOLA TESLA“ U GOSPIĆU**

**Nikola Jakovac**

# RIZICI PRIMJENE INFORMACIJSKE TEHNOLOGIJE U POSLOVANJU
# RISKS OF APPLICATION OF INFORMATION TECHNOLOGY IN BUSINESS

Završni rad

Gospić, 2016.

**VELEUČILIŠTE „NIKOLA TESLA“ U GOSPIĆU**

**Poslovni Odjel**

**Stručni studij Ekonomike poduzetništva**

# RIZICI PRIMJENE INFORMACIJSKE TEHNOLOGIJE U POSLOVANJU
# RISKS OF APPLICATION OF INFORMATION TECHNOLOGY IN BUSINESS

Završni rad

MENTOR:

Aleksandar Skendžić dr. sc.

STUDENT:

Nikola Jakovac

MBS: 2962000604/13

Gospić, rujan, 2016.

Veleučilište „Nikola Tesla“ u Gospiću

Poslovni odjel

Gospić, 19.07. 2016.

# ZADATAK

za završni rad

Pristupniku Nikoli Jakovcu, MBS: 2962999694/13

Studentu stručnog studija Ekonomike poduzetništva izdaje se tema završnog rada pod nazivom „Rizici primjene informacijske tehnologije u poslovanju“.

Sadržaj zadatka :

Primjena informacijskih tehnologija i sustava u poslovanju, njihove zlouporabe i informacijski rizici, sigurnost informacijskih sustava i zaštita, sigurnost u elektroničkom poslovanju.

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

Mentor: dr.sc. Aleksandar Skendžić (ime i prezime) zadano: 19.7.2016 (nadnevak), _____ (potpis)

Pročelnica odjela: Ivana Tonković Pražić, dipl.oec (ime i prezime) predati do: 30.09.2016. (nadnevak), _____ (potpis)

Student: Nikola Jakovac (ime i prezime) primio zadatak: 19.07.2016. (nadnevak), _____ (potpis)

Dostavlja se:

- mentoru
- pristupniku

# IZJAVA

Izjavljujem da sam završni rad pod naslovom „Rizici primjene informacijske tehnologije u poslovanju“ izradio samostalno pod nadzorom i uz stručnu pomoć mentora Aleksandra Skendžića.

Ime i prezime

Nikola Galovac

(potpis studenta)

# Sažetak

U suvremeno doba poslovanja nezamislivo je bez informacijskih tehnologija u svim segmentima poslovanja, jer današnje poslovne organizacije bile one male ili velike ne mogu poslovati bez informacijskog sustava koji je zasnovan na informacijsko – komunikacijskim tehnologijama.

Tako smo svjedoci informacijskih tehnologija svugdje gdje se nalazimo bilo poslovno ili privatno što ujedno i znači da je neodvojivi čimbenik modernog čovjeka u njegovom svakodnevnom životu. Neprestano smo u doticaju s informacijskim tehnologijama i njihovim informacijskim sustavima bilo kod podizanje ili polaganje gotovine putem bankomata, plaćanje putem pametnih kartica u fizičkim i online trgovinama, elektronička naplate cestarine odnosno ENC, te pri svakom telefonskom razgovoru i u mnogo drugim životnim okolnostima.

Razlog njihove primjene je automatizacija koja dakle omogućuje daleko bržu obradu informacija koja je manje podložna pogreškama te je ekonomski i ekološki prihvatljiva, odnosno radi se o hardveru i softveru koji predstavljaju informacijske tehnologije koje omogućuju prikupljanje, obradu, pohranu i isporuku informacija. Time osigurava poslovnoj organizaciji rast, povećanje prihoda i konkurentnost na tržištu.

Primjena informacijskih tehnologija u sebi sadrži nepoznanice, rizike, nesigurnosti i probleme koji mogu biti uočeni s vremenom. To može biti primjena neodgovarajućih odluka, metoda, provedba neodgovarajućeg znanja, gubitak podataka, nedovoljna izobrazba korisnika sustava, zlouporaba informacijskih tehnologija radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina. To rezultira nezadovoljavajućim poslovnim informacijskim sustavom koji ne udovoljava kritičnim faktorima uspjeha jedne poslovne organizacije. Rizik informacijskih tehnologija nije samo objektivne prirode već i subjektivne, odnosno rizik može nastati namjerama pojedinaca i skupinama unutar poslovnog informacijskog sustava.

Za otklanjanje rizika informacijskih tehnologija potrebno je poznavanje specifičnih metoda i alata kojima se uočava i prepoznaje rizik. Te specifične metode i alati podrazumijevaju pravilnike sigurnosne politike informacijskog sustava i međunarodne standarde sigurnosti čijom se implementacijom osigurava kvalitetno upravljanje informacijskim tehnologijama i sustavima.

Ključne riječi: informacijske tehnologije, informacijski sustav, automatizacija, ekonomska i ekološka prihvatljivost, rizici, nezadovoljavajući poslovni informacijski sustav, sigurnosna politika, međunarodni standard sigurnosti.

Summary

In contemporary times information technologies play a crucial role in all segments of business. Today's business organizations, both small or big ones, cannot operate without an information system which is based on information communication technologies.

Information technologies can be found in both, business and private environment, which means that they represent an essential factor in modern men's everyday life. There are many examples of this constant contact with information technologies and their information systems, such as: cash withdrawal or cash depositing by means of ATM, paying by smart cards in physical or online stores, Electronic Toll Payment or ENC, telephone conversations as well as many other examples.

The main reason of their use is automatization, which not only enables faster information processing, but is also economically and ecologically acceptable and less sensitive to errors. Information technologies, in fact, refer to a hardware and a software which enable information gathering, processing, storage and delivery and in that way ensure growth, income increase and market competitivness for a business organization.

However, the use of information technologies also implies some risks, insecurities and problems which can be noticed over time. Some of these are: the application of inappropriate decisions or methods, data loss, insufficient education of system users, misuse of information technologies in order to achieve unjustified or illegal benefits. This can result in an unsatisfactory business information system which doesn't accomplish critical success factors of a business organization. The risk of information technologies can also be subjective in nature, which means it can appear as a consequence of individuals' or groups' intentions within a business information system.

In order to be able to eliminate the risk of information technologies, it is necessary to be familiar with specific methods and tools for noticing and recognizing the risk. These specific methods and tools refer to information system safety policy handbooks, as well as international safety standards handbooks which are used in order to ensure quality information technologies and systems management.

Keywords: information technologies, information system, automatization, economically and ecologically acceptable, risks, unsatisfactory business information system, safety policy, international safety standards.

SADRŽAJ

Sažetak

Summery

1. UVOD ..... 1
2. Osnove informacijskih sustava i tehnologija ..... 2
   2.1. Informacijski sustavi ..... 2
   2.2. Informacijske tehnologije ..... 2
3. Rizici primjene informacijske tehnologije ..... 4
   3.1. Objektivni rizici ..... 4
   3.2. Subjektivni rizici ..... 5
4. Oblici narušavanja sigurnosti i rizici ..... 7
   4.1. Socijalni inženjering ..... 7
      4.1.1. Mrežna krađa identiteta (eng. phishing) ..... 9
      4.1.2. Telefonska krađa identiteta (eng. vishing) ..... 10
      4.1.3. Stvaranje scenarija (eng. pretexting) ..... 10
      4.1.4. Udičarenje (eng. baiting) ..... 11
   4.2. Prevencija socijalnog inženjeringa ..... 12
      4.2.1. Prevencija mrežne krađe identiteta ..... 12
      4.2.2. Prevencija stvaranje scenarija i telefonske krađe identiteta ..... 14
      4.2.3. Prevencija udičarenja ..... 15
   4.3. Zlođudni programi ..... 16
      4.3.1. Računalni virusi ..... 17
      4.3.2. Računalni crvi ..... 17
      4.3.3. Trojanski konj ..... 18
      4.3.4. Špijunski i oglašivački programi ..... 19
      4.3.5. Otkupni programi (eng. ransomware) ..... 20
   4.4. Prevencija zlođudnih programa ..... 21

4.4.1. Prevencija računalni virusa, crva i trojanskih konja ..... 21
4.4.2. Prevencija špijunskih i oglašivačkih programa ..... 22
4.4.3. Prevencija otkupnih programa ..... 23
4.5. Botnet mreža ..... 24
4.5.1. Distribuirani napadi uskraćivanjem usluga ..... 24
4.5.2. Neželjena elektronička pošta (eng. spam) ..... 25
4.6. Prevencija botnet mreža ..... 25
4.7. Rizici bežične mreže ..... 27
4.8. Prevencija rizika bežične mreže ..... 28
5. Sigurnosna politika informacijskih sustava i tehnologija ..... 30
5.1. Pravilnici sigurnosne politike ..... 33
5.1.1. Pravilnik o rukovanju zaporka ..... 33
5.1.2. Pravilnik o korištenju elektroničke pošte ..... 34
5.1.3. Pravilnik o antivirusnoj zaštiti ..... 35
5.1.4. Pravilnik o zaštiti neželjene pošte (eng. spam) ..... 35
5.2. Norme ..... 36
5.2.1. Norma ISO/IEC 17799 ..... 37
5.2.2. Norma ISO/IEC 17799:2005 ..... 39
6. HUB istraživanje o sigurnosti ..... 44
7. Zaključak ..... 47
Literatura
Popis tablica
Popis slika
Popis grafikona

# 1. UVOD

Informacija je važan resurs, pogotovo u suvremeno doba kada je svaka ustanova i pojedinac koriste, ne shvaćajući koliko ovise o njoj. Poznavanjem informacija, ustanove postaju uspješnije u svom radu i omogućuju kreativno stvaranje, sprječavanje loših odluka, grešaka i nepredvidivih situacija.

Tvrtke ili ustanove prate trendove informacijskih tehnologija kako bi mogle pratiti svoje konkurente i stanje na tržištu, kako bi oblikovali i prilagodili proizvode potrošačima, ne obaziruć se na sigurnost informacija koja je ključ njihovog uspjeha i produktivnosti.

Ozbiljna ustanova koja je svjesna važnosti informacija, gradi informacijski sustav sukladno sigurnosnoj politici i međunarodnim normama u cilju da njihovim implementacijama zaštiti informacijski sustav i ostvari certifikat koji ukazuje na kvalitetu i pouzdanost samog sustava ustanove.

Sigurnosna politika i usvajanje ISO standarda mogu pridonijeti uspješnom prepoznavanju i uklanjanju rizika, ali i nepredvidivih čimbenika sustava koji je i sam čovjek. Kroz rad ćemo govoriti o utjecaju socijalnih inženjera, zloćudnih programa, botnet mreža i ostalih rizika s kojim se zaposlenici suočavaju i gdje mogu dovesti u opasnost sebe i ugroziti informacijski sustav ustanove u cjelini.

# 2. Osnove informacijskih sustava i tehnologija

## 2.1. Informacijski sustavi

Sustav je ukupnost pravila, stvari i ostalih pojedinih dijelova koji se organiziraju i održavaju kroz svoju strukturu organizacije, te djeluje unutar svoje vlastite okoline s kojom održava određene veze. Sustav predstavlja karakteristiku složenih hijerarhijski organiziranih podsustava, odjela ili komponenata koji su kolektivno orijentirani u ostvarenju nekog zadanog cilja.

Slika 1: Osnovni model sustava




Izvor: Pavlić M., Informacijski sustavi, Sveučilište u Rijeci, Zagreb 2011.

Informacijski sustav treba informacijski udovoljavati zahtjevima korisnika pri donošenju važnih poslovnih odluka. Informacije koje sustav šalje i prima od okoline nastaju iz ulaza i osiguravaju smisao postajanja sustava. Izlazne informacije se prikazuju kao važni izvještaji koji daju rezultate općeg stanja sustava. Ulazne i izlazne informacije informacijskog sustava nužne su za funkcioniranje organizacije.

## 2.2. Informacijske tehnologije

Iako govorimo o informacijskim sustavima i tehnologijama kao da su to dva odvojena segmenta, moramo razumjeti da informacijski sustav se može, ali ne mora, koristiti informacijskom tehnologijom.

Informacijska tehnologija je skup računalnih alata koje se mogu primijeniti za izgradnju i upravljanje informacijskog sustava, ako je taj informacijski sustav izgrađen putem informacijskih tehnologija. Jer informacijski sustav može biti izgrađen bez informacijskih

tehnologija. Možemo uzeti za primjer knjigu ili čak kamen, koji mogu biti informacijski sustavi na kojemu je urezana informacija bez primjene informacijskih tehnologija.

Svakako ustanova koja primjenjuje informacijske tehnologije i sustave, shvaća da ta dva segmenta ne mogu jedan bez drugog, jer za izgradnju informacijskih sustava potrebne su informacijske tehnologije, a za korištenje tehnologija potrebni su sustavi.

Termin informacijske tehnologije objedinjuju ta dva elementa, tako kad govorimo o informacijskim tehnologijama, podrazumijevamo i njihove sustave.

Informacijska tehnologija predstavlja spregu mikroelektronike, računala, telekomunikacija i softvera, koja omogućuje unos, obradu i distribuciju informacija (Ćerić, Varga, 2014)

Informacijska tehnologija se sastoji od računalnog sklopovlja, hardvera (miš, zaslon, tipkovnica, računalne komponente itd.) i računalnog program, softvera (operacijski sustavi, aplikacijski programi, razvojne alate itd.). One predstavljaju fizičke elemente koji u sebi imaju integrirane neopipljive elemente, koji se međusobno upotpunjuju.

# 3. Rizici primjene informacijske tehnologije

Rizik se dijeli u dvije vrste, u subjektivne i objektivne rizike.

Ovisno o uzorku (izvoru), rizici mogu biti (Bosilj, Pejić, Čerić, Panian, Požgaj, Srić, Varga, Ćurko, Spremić, Strugar, Jaković, Vlahović, 2009.):

- Objektivni, kada oni proizlaze iz prirode i zakonitosti funkcioniranja sustava u kojem se informacijska tehnologija primjenjuje;
- Subjektivni, kada oni nastaju namjerom pojedinaca ili skupina, ili pak kada se u sustavu ne poduzimaju raspoložive mjere zaštite (prevencije) od objektivnih rizika.

Objektivni rizici su rizici koji su nastali slučajno. Oni mogu biti prirodni kao što su požari, poplave, prašina, vlaga itd. No mogu nastati i posljedicom ljudske pogreške kao što su brisanje podataka, pogrešno rukovanje, nemar ili nedovoljna educiranost korištenja informacijskih tehnologija.

Veća pažnja posvećuje se subjektivnim rizicima, koji nastaju namjernom ljudskom aktivnošću radi ostvarivanja protupravne koristi. Objektivni rizici nastaju po već propisanim pravilima sigurnosne politike informacijskog sustava. Zbog svoje nepredvidljivosti, objektivne rizike nije moguće u potpunosti izbjeći. Dok subjektivni rizici mogu se u potpunosti izbjeći poduzimanjem odgovarajućih preventivnih mjera.

## 3.1. Objektivni rizici

Pošto objektivni rizici nastaju pukom slučajnosti nepredvidivih uzroka prirodnih elemenata i ljudskih pogrešaka, pažnja se usmjerava više na zaposlenike jer u nekoj mjeri možemo utjecat na njihova ponašanja. Zaposlenike koji nenamjerno oštete imovinu informacijskog sustava putem nepravilnog rukovanja, potrebno je ponovno pravilno educirati i upozoriti na posljedice nepravilnog korištenja. Nepažnja korisnika može imati za posljedicu otkrivanja osjetljivih podataka. Ne postoje nikakve druge alternative otklanjanja ljudske nepažnje.

Objektivni rizici prirodnih elemenata sastoje se od nekoliko skupina, a to su:

- Meteorološke nepogode. Ova prirodna prijetnja uključuje sve atmosferske nepogode, kao što su razne padaline, vjetar, oluje, ekstremno visoke i niske temperature. Te nepogode u velikoj mjeri utječu na ljudski rad, no predstavljaju i prijetnju od gubitka ili smanjenja kvalitete podataka, pa sve do uništenja uređaja a samim time i informacija, koje su pohranjene na tim uređajima.
- Geofizičke nepogode predstavljaju potrese i vulkanske erupcije te sve aktivnosti koje izazivaju požare, potrese. Ova prirodna nepogoda može stvarati rizike kao što je ispuštanje raznih štetnih plinova i kemikalija, a što ima za posljedicu dolaska do prekida napajanja, trovanja, opeklina ili čak do gušenja zaposlenih.
- Sezonski fenomeni mogu biti uzrokovani ekstremnim vremenom, kao što su uragani, tornado ili šumski požari. Što uzrokuje rizike gubitaka ili degradacija komunikacijskih mreža.
- Astrofizički fenomeni su rijetke pojave kao što su meteori koji mogu uzrokovati gubitak satelitskih veza.
- Biološke prijetnje su prijenosne prehlade, virusi i ostale razne prijenosne bolesti koje mogu smanjiti broj zaposlenika, te smanjiti produktivnost i dobit informacijskog sustava.

Objektivni rizici, pogotovo prirodni segmenti, mogu naveliko prouzročiti materijalne gubitke i štete. Nažalost ne postoji rješenje kod nastanka takvih problema, jednostavno se mogu poduzeti određene mjere da se omogući kontinuirano poslovanje i da se umanji, spriječi ili spasi gubitak informacije.

## 3.2. Subjektivni rizici

Subjektivni rizici podrazumijevaju ljudske namjerne prijetnje, koje mogu ugroziti sustav na bilo koji način, bilo materijalno ili nematerijalno. Prirodni elementi mogu ugroziti organizaciju fizičkim putem svojih prirodnih nepogoda. Dok se čovjek može služiti svojim znanjem i putem svojih namjera ugroziti informacijski sustav da nije ni pristupio u fizički prostor organizacije.

Prvo ćemo navesti fizičke prijetnje zaposlenih s kojima se možemo suočiti, a to su:

- Neposlušnost zaposlenika što dovodi do prosvjeda kojim mogu prouzročiti oštećenje opreme ili uređaja, ali i može doći do ozljede samih zaposlenika;
- Zlouporaba ovlasti. Neodgovornost zaposlenika i nepridržavanja pravilnika o poslovanju, može se dogoditi ako prekomjerno i prekovremeno koriste imovinu organizacije ili tu istu iznose van prostora za koju nije namijenjena.
- Krađa. Zaposlenici namjerno prisvajaju ili otuđuju imovinu koja nije u njihovom vlasništvu. Time stvaraju dodatne troškove organizaciji.

Pod nefizičkim prijetnjama spadaju sabotaže, koje mogu biti i fizičkog oblika, no njihova pojava je često ostvarena putem računalnog programa ili telekomunikacijskih linija.

Sabotaža podrazumijeva namjerno narušavanje rada sustava i ispravnost uređaja, te time organizacija mora uvest određene mjere i zaštite kako bi se ta pojava spriječila. Sabotaža su kriminalne aktivnosti usmjerene na uništavanje informatičke opreme i podataka.

Fizička sabotaža ostvaruje se manualno odnosno ručno. Stvaraju se nenormalni uvjeti rada, kao što su: povećanje temperature, vlage u radnom prostoru, strujni udari itd. No mogu se ostvariti putem telekomunikacijskih kanala. One osobe koje provode kriminal putem telekomunikacijskih kanala zovu se hakeri. Oni neovlašteno pristupaju podacima ili imovini putem telekomunikacija i traže nezaštićene ili nedovoljno osigurane elemente tuđih informacijskih sustava.

Hakeri mogu ostvariti svoje sabotažne radnje kroz:

- Manipulaciju sredstvima informacijske tehnologije;
- Neovlaštenu upotrebu softvera i povredu vlasništva;
- Računalne viruse;
- Zlouporabu korisničkih računa;
- Zlouporabu bankomata, inteligentnih kartica i slično;
- Zloupotrebu privatnosti.

# 4. Oblici narušavanja sigurnosti i rizici

## 4.1.Socijalni inženjering

Socijalni inženjering je umjetnost i znanost nagovaranja ljudi da ispune zahtjeve napadača.

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-172.pdf (6.8.2016./18:18)

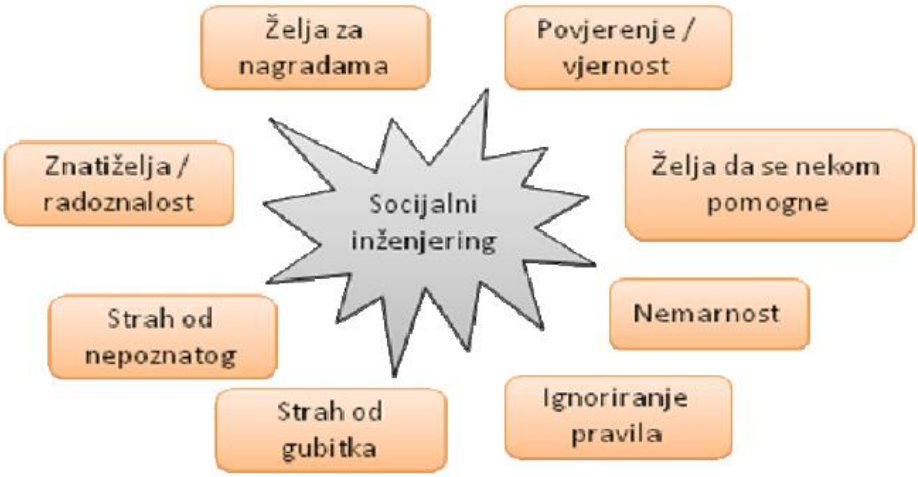
Socijalni inženjering je umjetnost koja na maštovit način upućuje ljude da ispune zahtjeve napadača. Napadači pokušavaju pridobiti povjerenje od zaposlenih te tako izvući od njih povjerljive informacije i podatke do kojih napadači ne bi mogli doći legitimnim putem.

Ovakva vrsta napada može se pojavljivati u običnoj komunikaciji s zaposlenicima, tako socijalni inženjeri u lažnoj ulozi nadređenog, autoritativno zapovijeda zaposleniku što treba učiniti za njega. To im često polazi za rukom, jer zaposlenici imaju želju za dokazivanjem i poštivanjem autoriteta u nadi da budu nagrađeni.

Socijalni inženjeri mogu biti u ulozi službenika, te na taj način mogu doći do informacija službenika na istoj razini s dobrom namjerom da drugi službenik želi pomoći napadaču. Zaposlenici su skloni pomoći novim zaposlenicima, time napadači dolaze do detaljnih informacija o radu organizacije koje žele napasti. Zaposlenici imaju čestu želju za nesebičnim pomaganjem, pogotovo ako se napadač lijepo ophodi prema zaposleniku. Tim lijepim riječima stvara moralnu dilemu zaposlenika, jer pobuđuje krivnju žrtve i potiče ju je na razmišljanje da će i njoj s vremenom trebati neka vrsta pomoći. Dakle, jedan od najopasnijih lažnih uloga napadača u koju zaposlenici ne sumnjaju je uloga osobe iz podrške, primjerice tehničke ili sigurnosne. Socijalni inženjeri tom ulogom stvaraju povjerenje zaposlenika, te dolaze do podataka kao što su korisničko ime i zaporka.

Socijalni inženjeri također često dolaze do povjerljivih informacija pretraživanjem otpada. To mogu biti pronalaženja pisama, dopisa, telefonskih brojeva, detalja različitih dnevnika, optičkih diskova i raznih memorija za pohranu.

Slika 2: Prikupljanje informacija u socijalnom inženjeringu




Izvor:http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-292.pdf (7.8.2016./11:20)

Socijalni inženjer može bit i sam zaposlenik informacijskog sustava, svatko može pridobiti ulogu socijalnog inženjera ako ugrozi informacijski sustav organizacije. Na primjer, zaposlenik može poslati elektroničku poštu svim primateljima s kojima je stupio u kontakt, ne vodeći računa da je uključio ili ima uključenu opciju „send all“ (pošalji svima). Tim aktom je podijelio svima povjerljive podatke organizacije. Drugi primjer je da zaposlenici mogu biti nezadovoljni i okrenuti se protiv organizacije i ignorirati njezina pravila. Česti razlozi su: preniske plaće, loši uvjeti rada, težina posla, nemogući zahtjevi nadređenih itd.

Dakako najčešći oblici napada socijalnog inženjeringa se ostvaruje putem informacijskih tehnologija.

Greška kod velikog broja tvrtki je usavršavanje sigurnosti informacijskog sustava putem hardvera i softvera, gdje se ulaže mnogo novaca da se ostvari njihova idealna zaštita protiv napadača. Tvrtke često zanemare ulaganje u obrazovanje zaposlenih koji su najveće meta napadača, ne pazeći na ljudski faktor. Dovoljno je da napadač prikupi određeno saznanje o zaposleniku i o informacijskom sustavu u kojem posluje (proučavanje opisa posla, odnos zaposlenika prema nadređenom) te se predstavi kao njegov nadređeni. Kad se dogodi šteta uzrokovana socijalnim inženjeringom, većina tvrtki ne želi da se ta informacija proširi javnosti, zbog straha da ne izgube na reputaciji i da ne izgube povjerenje od korisnika.

Socijalni inženjeri ne trebaju poznavati nikakve posebne vještine programiranja, već je dovoljno poznavanje slabosti ljudske psihologije i snalaženje u razgovoru, kako se ne bi stvorila sumnja napadača. Svakako je do dolaska povjerljivih informacije lakše doći putem ljudi nego izgradnji zloćudnog programa (eng. malware) koji bi zaobišao zaštitu informacijskog sustava i njegovih korisnika.

Ovakvi oblici napada putem informacijskih tehnologija često dolazi u obliku interneta ili telekomunikacijskih linija, i imaju razne prijetnje kao što su:

- Mrežna krađa identiteta;
- Telefonska krađa identiteta;
- Stvaranje scenarija;
- Udičarenje.

### 4.1.1. Mrežna krađa identiteta (eng. phishing)

„Phishing“ ili tako zvana mrežna krađa identiteta su najprometniji i najštetniji napadi današnjih prevaranata s interneta. Mnogi „phishing“ napadi počinju porukom elektroničke pošte s ciljem da se korisnik putem poveznica usmjeri na lažnu web stranicu koja izgleda identično kao i originalna, zakonita stranica. Kada se jednom korisnik nađe na lažnom odredištu on se prijavljuje sa svojim korisničkim imenom, lozinkom, brojevi kreditnih kartica, PIN kodovi i sl., koje tako dolaze u ruke napadača, te ih on zlouporabi za pristup stvarnoj Web lokaciji.

Nakon prikupljenih povjerljivih informacija putem lažne Web stranice, prikupljene informacije mogu se iskoristiti za izravno ostvarivanje financijske koristi ili te iste informacije mogu preprodavati zainteresiranim osobama. Često krajnji cilj napadača je financijska korist ali napadači mogu imati i druge motive, kao što je sabotiranje informacijskog sustava ustanove.

Korisnici sustava su najveća meta krađe mrežnog identiteta, jer socijalni inženjeri su svjesni da koriste jednu zaporku za prijavu na višestruke račune.

Ovakva vrsta napada pojavljuje se često kod korisnika sustava ali i žrtve mogu biti zaposlenici koji nisu dovoljno educirani ili upoznati s takvom vrstom napada.

### 4.1.2. Telefonska krađa identiteta (eng. vishing)

Telefonska krađa identiteta se odnosi na lažne telefonske pozive u kojem se napadači predstavljaju kao zaposlenici banke ili neke druge organizacije te od korisnika traže da sa svog korisničkog računa prebace novac na neki nepoznati račun. Napadač se može predstaviti kao djelatnik pružatelja financijskih, televizijskih, sigurnosnih, telefonskih ili internetskih usluga.

Socijalni inženjer može putem telefona provoditi lažnu anketu kako bi mogao pristupiti tuđem bankovnom računu. Pitanja na prvi pogled izgledaju bezopasna, kao što su djevojačko prezime, datum rođenja, osobni identifikacijski broj itd. To je pokazatelj da napadač putem tih podataka može pristupiti web bankarstvu te doći do korisničkog računa žrtve i nanijeti financijsku štetu.

Prikupljenom dovoljnom količinom informacija o žrtvi, napadač se može lažno predstaviti pružateljima usluge glumeći da je sama žrtva, te tako zatražiti obnovu korisničkog računa i zaporke i ostvariti krajnji cilj, a to je pristup povjerljivim informacijama žrtve.

### 4.1.3. Stvaranje scenarija (eng. pretexting)

Pretexting ili stvaranje scenarija predstavlja dobro razrađene laži, koje omogućuju napadaču da otkrije povjerljive informacije korisnika ili da navode korisnike da izvode neke radnje. Uvijek je to više od običnih laži, jer napadači upotrebljavaju neka prijašnja istraživanja ili pripreme podatka za oponašanje (dan rođenja, broj socijalnog osiguranja itd) da bi ukazao žrtvi da su njegove aktivnosti legitimne. Sam napad se odnosi na istraživanje žrtve, informiranje o osobi i njezinim aktivnostima ili informiranje o strukturi tvrtke, upoznavanje internim žargonom, prikupljanje imena zaposlenih itd.

Stvaranje lažnog scenarija najviše daje rezultata na društvenim mrežama, jer na društvenim mrežama korisnici se često slobodnije i opuštenije ponašaju. Također napadačima društvene mreže predstavljaju izvor vrijednih informacija, gdje korisnici otkrivaju privatne informacije iz svog života. To im omogućuje da s lakoćom prate žrtvine navike, aktivnosti i profil ponašanja.

Jedan od čestih primjera napada su prikupljanje informacija i odgovori na sigurnosna pitanja koja nudi većina internetskih poslužitelja s namjerom da povrate korisniku zagubljenu zaporku.

Poslužitelji omogućuju korisniku tijekom izrade korisničko računa da odgovori na sigurnosna pitanja, kako bi na njihov odgovor moga povratiti zaporku u slučaju ako je izgubljena.

Na taj način sigurnosna pitanja omogućuju korisniku da zaobiđe unos zaboravljene zaporke i da je povrati odgovorima na pitanja. Mnogi poslužitelji daju opciju unosa druge adrese elektroničke pošte kako bi poslali zaboravljenu zaporku. Također mnogi poslužitelji nude i korisničku podršku te se napadači služe lažnim telefonskim predstavljanjem, što im polazi za rukom jer su prikupili dovoljno informacija o žrtvi. Glumeći da je žrtva ili netko s autoriziranim pristupom žrtvinog računa može steći mnogo povjerljivih podataka.

Većina korisnika interneta koristi jednu lozinku za pristup više korisničkih računa. Ako se to potvrdi točnim, napadač ostvaruje njihov pristup. Tako ima pristup žrtvinoj elektroničkoj pošti, financijskim poslužiteljima, informacijama radnog mjesta, broj računa kartica i ostalih povjerljivih informacija koje nisu javno dostupne.

### 4.1.4. Udičarenje (eng. baiting)

Udičarenje bi mogli opisat kao vrstu prevare, gdje napadač na vidljivom mjestu postavlja optički disk ili određenu vrstu memorije, koja je zaražena računalnim virusom i zamaskirana zaštitnim znakom od tvrtke. Žrtva odnosno zaposlenik ga uzima i upotrebljava na svom računalu. Na optičkom disku ili memoriji nalazi se lažni dokument u kojem se nalazi neki softver ili multimedijski sadržaj zloćudnog koda. Zloćudni kod prati računalne aktivnosti žrtve, te šalje rezultate napadaču u obliku lozinka, dopisa, internetskih aktivnosti i slično.

Udičarnje ne mora biti prisutno putem hardvera. Korisnici ili zaposlenici mogu pristupit nesigurnim stranicama ili otvaranjem poveznicama, koje se bez antivirusne zaštite prekriveno instaliraju bez znanja korisnika. Tako udičarenje ne treba biti namjerno ili isplanirano od strane napadača, čak je dovoljna žrtvina neopreznost i neznanje kojim napadač može nelegitimno pristupit povjerljivim podacima.

## 4.2. Prevencija socijalnog inženjeringa

Lažno predstavljanje je najčešća korištena metoda napada socijalnih inženjera. Vrlo je važna da svaka tvrtka koja posjeduje informacijski sustav educira zaposlenike kako bi znali prepoznati napad i sukladno tome reagirati. Unutar organizacije mora se stvoriti komunikacija koju poznaju samo zaposlenici sustava, a van organizacije pravila i procedura kojih se moraju držati svi zaposlenici i korisnici sustava. Sve što je suprotno tim mjerama predstavlja sumnjive aktivnosti.

Također napomenuli smo da socijalni inženjeri mogu pretraživati i prikupljati otpad u cilju da se dokopaju povjerljivih informacija bilo one u digitalnom ili papirnatom obliku. Radi prevencije krađe otpada koji mogu sadržavati povjerljive povijesne informacije, ustanove bi trebale omogućiti i njihovo uništavanje. Tako se postavljaju u uredima uređaji koji uništavaju papirnate dokumente, drobeći dokument u više dijelova kojeg je kasnije otežano ili nemoguće sastaviti.

Digitalna dokumentacija se pohranjuje na tvrdi disk računala u kojem se nalazi magnetizirani disk u kojem se podaci upisuju na način da se magnetiziraju čestice tog diska. Brisanjem i formatiranjem sadržaja ne mogu se u potpunosti ukloniti podaci. Da bi se podaci u potpunosti uništili i tako osigurala informacijska povjerljivost ustanove, tvrdi diskovi i ostali memorijski uređaji šalju se na reciklažu elektroničkog i elektronskom otpada.

### 4.2.1. Prevencija mrežne krađe identiteta

Socijalni inženjeri služeći se lažnim stranicama koje izgledaju identično legitimnim stranicama koriste tako zvane tehnike i alate maskiranja web adrese. Tehnike maskiranja URL adrese ostvaruje se korištenjem naprednih svojstva HTML jezika, jezika za izradu web stranica.

Ako se korisnik prijavljuje na službenu stranicu financijskog poslužitelja, uvijek treba provjeriti početak web adrese. Službene stranice prijave uvijek će glasiti „https://signin.financijskiposlužitelj.com/“ odnosno „https“. Sve službene stranice na koje se korisnik prijavljuje počinju sa „https“, što znači da je stranica sama po sebi na zaštićenom serveru. Ako počinje s „http“ stranica je lažna.

Tablica 1: Primjeri stvarne i lažne adrese

| Stvarne adrese | Lažne adrese |
|---|---|
| http://pages.ebay.com/help/index.html | http://signin.ebay.com@10.19.32.4/ |
| http://hub.ebay.com/community | http://page.@ebay.com |
| https://signin.ebay.com/ | http://signin-ebay.com/ |

Izvor: http://pages.ebay.com/help/account/recognizing-spoof.html#recognizing (9.9.2016 /14:40)

Dakle, nijedan financijski poslužitelj neće slati svojim korisnicima poveznice web lokacije prijave. Međutim, ako je nastao problem uputit će ga da se putem svog web preglednika prijavi na službenu stranicu poslužitelja. Kad se prijavi tamo ga čekaju detaljne upute za rješeavanje novonastalog problema.

Sprečavanje mrežne krađe identiteta (Murray, Weafer, 2005.):

- Legitimne organizacije ne šalju poruke e-pošte u kojima od vas traže podatke o vašem računalu;
- Korporacije budno paze da u korespondenciji (redovna pošta na koju se odgovara) s klijentima nema pravopisnih i gramatičkih pogrešaka. Pazite se poruka s pravopisnim i gramatičkim pogreškama i s čudnim frazama;
- Nemojte kliknuti ni na koju poveznicu u poruci. Pogledajte pažljivo te poveznice, one bi mogle imati čudne nastavke;
- Ako mislite da bi stvarno mogao postojati problem s vašim računom, najbolja opcija je da podignete telefonsku slušalicu i nazovete službu za korisnike. Ako to nije moguće, zatvorite poruku e-pošte i u svoj Web pretraživač sami upišite URL. Nikako nemojte izrezivati i uljepljivati URL iz poruke;
- Dobijete li poruku, e-pošte iz banke ili s lokacije za e-trgovinu s kojima ne poslujete, izbrišite tu poruku bez otvaranja. Mnoge phishing poruke e-pošte sadrže viruse i druge malware koji mogu zaraziti vaše računalo ako otvorite poruku;

- Koristite antivirusni softver, stalno ga ažurirajte i provjerite je li kofiguriran za automatsko skeniranje vaše e-pošte.

### 4.2.2. Prevencija stvaranje scenarija i telefonske krađe identiteta

Vremenom je zabilježeno mnogo napada stvaranja lažnog scenarija, pogotovo kod web poslužitelja koji imaju mnogo korisnika i koji su najčešća meta napadača. Srećom, mnogi internetski poslužitelji visoke reputacije odbacuju ponovnu obnovu računa pomoću sigurnosnih pitanja i umjesto toga oporavak računa se može obnoviti putem pametnog telefona. Sve veća primjena mobilnih pametnih telefona korisnika, rezultiralo je vrlo domišljatim povećanjem sigurnosti, jer se primijetilo da većina korisnika provodi vrijeme na pametnim telefonima. Korisnici tako mogu dobiti obavijesti ako je netko drugi pristupio na njihovim korisničkim računima i imaju uvid u sve aktivnosti koje su izmijenjene, te im se omogućuje opcija manipuliranja izmijenjenim sadržajem i promjena lozinke.

Najveće žrtve socijalnog inženjeringa su korisnici financijskih internetskih usluga, kojim su čestim napadima stvorili uređaj pod nazivom token koji omogućuje visoku razinu sigurnosti provođenja internet bankarskih usluga. Token djeluje tako da nakon unošenja inicijalne zaporke kombinira PIN korisnika s brojem koji token sam generira složenom matematičkom pravilnošću i dobivenu vrijednost prikazuje na ekranu. Tom se kombinacijom brojeva korisnik predstavlja izdavaču tokena banke. Svaki token je pojedinačan od drugih, pa dva tokena nikad ne mogu generirati isti broj. Korisnik ima tako dva faktora. Prvi je faktor PIN nešto što korisnik zna, a drugi faktor je sam token nešto što korisnik ima. Čak ako napadač sazna korisnikov pin (korisničko ime i lozinku) ne može pristupit korisničkom računu bez drugog faktora.

Bez obzira što je socijalnim inženjerima u suvremeno doba otežana krađa identiteta putem „pretexting-a“ i telefonske krađe identiteta, ipak ćemo navest nekoliko preporuka zaštite:

- Nemojte odavati svoje osobne informacije preko telefona, elektroničke pošte osim ako vi niste nazvali korisničku podršku i uvjereni ste da je takva služba sigurna. Svi pozivi upućeni vama koji zahtijevaju takve povjerljive informacije su sumnjive. Napadači su posebno zainteresirani za vaš broj socijalnog osiguranja, djevojačko prezime, ime kućnog ljubimca, banaka, brojeva računa kreditnih kartica, OIB i slično;

- Nikad ne koristite jednostavne zaporke kao što su ime vašeg djeteta, kućnog ljubimca ili datume rođenja;
- Upitajte vaše financijske poslužitelje da vam pošalju njihovu sigurnosnu politiku za korisnike njihovih usluga;
- Budite jako oprezni kod ispunjavanja anketa, nemojte davati osobne podatke svakom tko vas zove na telefon ili traži putem elektroničke pošte;
- Ako se od vas ipak traži da odgovorite na sigurnosna pitanja u slučaju izgubljene lozinke, mnogi poslužitelji usluga imaju opciju da kreirate svoje vlastito sigurnosno pitanja. To može biti odgovor za kojeg jedino vi znate. Ako se ipak ne nudi takva opcija, probajte odgovorit na pitanje u raznim simbolima, pazeći da se sjetite ako zagubite zaporku.
- Proširite informaciju prijateljima i članovima obitelji o opasnostima i tehnikama socijalnih inženjera. Jer njihove kriminalne aktivnosti su jedino efektivne ako korisnik nije upućen u njihove radnje.

### 4.2.3. Prevencija udičarenja

Udičarenje je mamljenje korisnika ili zaposlenika da kopiraju na svoja računala zloćudne datoteke ili da pristupaju na sumnjive internetske stranice. Zaposlenici bi trebali izbjegavati korištenje optičkih ili prijenosnih memorija koje nude korisnici njihovog sustava i oslanjati se na resurse koje nudi informacijski sustav. Najčešće su to trojanski i špijunski programi koji prate svaku aktivnost korisnika sustava.

Informatički stručnjaci trebali bi educirati zaposlenike o socijalnim inženjerskim taktikama i napadima redovito. Općenito sadržaj ovog tipa educiranja kod zaposlenika je ubrzo zaboravljena, tako da je zaposlenike potrebno educirati najmanje svakih šest mjeseci i educirati ih oko sigurnosne politike ustanove i posljedice koje mogu nastati ako se krše njezina pravila.

Svakako, svaka bi se organizacija trebala adekvatno zaštiti od socijalnog inženjeringa, kroz:

- Redovitu provedbu sigurnosnih testiranja;
- Edukaciju zaposlenika o socijalnom inženjeringu, sigurnosnim rizicima i pravilnim postupcima u rukovanju dokumentima i tehnologijom;

- Izrada internih propisa i procedura;
- Izrada i primjena sigurnosne politike organizacije i vanjska kontrola primjene sigurnosnih procedura.

## 4.3. Zloćudni programi

Zloćudni programi ili „malicious software“ je termin koji se odnosi za one programe koji nanose štetu, bilo da se odnosi na sigurnost podatak na računalu ili na štetu nanijetu korisnikovoj privatnosti.

Napadači koji stvaraju zloćudne program, motivirani su profitom odnosno novcem. Međutim postoje i napadači koji su iznimka. Oni stvaraju zloćudne programe kako bi stekli reputaciju istomišljenika, ali zloćudni kod koji dobiva na publicitetu u medijima brzo se lovi i uklanja. Tako je napadačima koji su motivirani profitom, glavni cilj da njihov zloćudni program ostane što duže prekriven.

Zlonamjerni programi na računalnoj mreži mogu dospjeti putem računala i ostvarit svoje širenje na nekoliko načina:

- Internet konekcija;
- Elektronička pošta;
- Zaražene prijenosnici memorije;
- Prijenos podataka;
- Razmjena podataka s zaraženim lokalnim mrežama na udaljenim lokacijama;
- Preuzimanje i instalacija piratskih programa.

Osnovne vrste zloćudnog programa su:

- Računalni virusi;
- Računalni crvi;
- Trojanski konj;
- Špijunski i oglašivački programi;
- Ransomware.

Svaki zloćudni program je različit od drugog. Vrlo važno je znati njihove uloge i jedinstvenosti od drugih zloćudnih programa, kako bi korisnik poduzeo određene mjere i bezbrižno upravljao računalnim sustavom.

### 4.3.1. Računalni virusi

Računalni virusi su programi, odnosno zlonamjerni kodovi koji se repliciraju u datotekama ili programima s kojima se dolazi u kontakt. Pokretanjem programa ili otvaranjem datoteka, virusi se aktiviraju te nanose štetu: računalnim softverima, sektoru za podizanje sustava i datotekama.

Računalni virusi se jedino mogu aktivirati i širiti uz pomoć korisnika ako ga on pokrene ili otvori. Odnosno računalni virusi se ne mogu širiti bez ljudskog djelovanja. Šteta može biti u više oblika. Jedan od najčešćih je da se pokretanjem virusa pokreće postupak replikacije što može uzrokovati preopterećenje računalnih resursa odnosno memorije, a to smanjuje produktivnost korisnika ili zaposlenika. Može biti u obliku neželjene pošte (eng. spam), gdje se klikom na poveznicu otvaraju veliki brojevi web adresa i pokreće postupak slanja neželjene pošte svim ostalim korisnicima s kojim je korisnik stupio u kontakt.

Računalni virusi također brišu podatke i datoteke. Svakako glavni cilj virusa je umanjiti efikasnost i produktivnost informacijskih sustava, te tako sabotirati rad i stvoriti ogromne troškove tvrtkama koje su u velikoj mjeri oslanjaju na povlastice informacijskog sustava.

### 4.3.2. Računalni crvi

Za razliku od računalnih virusa, računalni crvi su samorepli cirajući programi koji se prenose s računala na računalo, bez ikakve ljudske interakcije. Najčešće putuju računalnom mrežom koristeći prometne značajke mrežnog sustava, a to je ono što omogućuje da putuju bez pomoći. Oni su samodostatni programi koji rade nezavisno od drugih programa.
Korištenje mrežnog prometa kao što je elektronička pošta ili sustav za dopisivanje u stvarnom vremenu, crvi putem mehanizma repliciranja enormno se brzo šire.

Osim umnožavanja i stvaranja opterećenja računalnog prostora i memorije, crvi mogu biti dizajnirani da rade druge radnje. Računalni crvi tako koriste funkciju „payload“ koja

predstavlja aktivnosti kao što su brisanje ili promjena podataka, instaliranje softvera na računalu ili kreiranje stražnjih vrata (eng. backdoor software) kojim se napadač služi da bi potajno pristupio neovlašteno na korisnikovo računalo. Korištenjem funkcije „backdoor“ računalni crv koristi računalni sustav korisnika kao točku kojom se šalju neželjen email poruke (eng. spam) komercijalnog oblika.

### 4.3.3. Trojanski konj

Trojanski konj je računalni virus, odnosno zloćudni program koji se predstavlja kao bezazleni program. On može biti u obliku animiranog isječka, čuvara ekrana ili besplatnog softvera koji stvara interes korisnika, s namjerom da ga instalira na svoje računalo. Cilj trojanskog konja je da instalira stražnja vrata na korisnikovom računalu, te tako da napadač stekne udaljenu kontrolu na korisnikovom računalu s namjerom da pridobije korisničko ime i lozinku. Trojanski konj poprimio je osobine virusa, crva i socijalnog inženjeringa da bi potakao korisnike koji ništa ne sumnjaju da ih preuzmu s interneta.

Glavna razlika trojanskog konja u odnosu na računalne viruse i crve je da se trojanski konj ne replicira. Ako je trojanski konj instaliran napadač će imati neograničeni pristup korisnikovom računalu što mu omogućuje pristup osobnim podacima.

Posljedice koje trojanski konj može prouzročit:

- Pad sustava ili uređaja;
- Izmjena ili brisanje podataka;
- Korupcija podataka;
- Oblikovanje ili formatiranje računalnog prostora odnosno diskova;
- Širenje preko mreže;
- Špijuniranje aktivnosti korisnika i pristup osjetljivim informacijama.

### 4.3.4. Špijunski i oglašivački programi

Špijunski programi (eng. spyware) su softveri koji nadziru aktivnost korisnika putem računala i prenose informacije na druga računala odnosno lokacija na internetu. On prikuplja podatke i distribuira ih, tako da promatra informacije koje se odnose na računalo korisnika, aplikacije koje se na njemu izvode, korištenje internet pretraživača itd.

Najčešće se špijunski programi za prikupljanje podataka služe „Keystroke loggerima". „Keystroke logger" je program koji nedopušteno bilježi sve korisnikove pritiske na tipke tipkovnice. Te se informacije mogu pohraniti za kasnije učitavanje, mogu se prenositi na udaljeni procesor ili se mogu prenijeti osobi koja koristi „keylogger" preko elektroničke pošte.

„Chat loggeri" su špijunski programi koji zapisuju svaku vrstu razgovora vođenu programima za razmjenu poruka u stvarnom vremenu. Ova vrsta programa pokazala se korisnim alatom za nadzor djece na internetu, ali može biti izrazito opasno ako su se uz program instalirala stražnja vrata, te se podaci šalju na računalo napadača.

Infekcija špijunskog programa može se ostvariti prilikom posjeta web stranica s ilegalnim sadržajem koje sadrže zlonamjerni kod i pronalaze sigurnosne propuste web pretraživača te se na taj način instalira bez znanja korisnika. Također se može predstaviti u obliku trojanskog konja tj. u obliku besplatnog bezazlenog programa.

Oglašivački programi (eng. adware) su programi koje ne kreiraju kriminalci već komercijalne softverske tvrtke u obliku besplatnog programa. Primjer ako korisnik kupuje preko online trgovine pohranjuju se informacije o povijesti trgovine, omiljeni artikli. Praćenje korisnikovih navika radi poboljšanja reklamnog segmenta tvrtki općenito su bezopasna.

Oglašivački programi koriste tako zvane kolačiće (eng. cookies).

Kolačići su male tekstualne datoteke koje Web pretraživači postavljaju na korisnikovo računalo kada posjete neku web lokaciju. Kolačići sadrže informacije o korisniku koje se prenose na računalo i pohranjuju. To omogućuje korisniku brži pristup na često posjećenim web lokacijama i pomaže u prilagođavanju njegovog posjeta.

Postoji druga kategorija kolačića koja se naziva kolačići za praćenje (eng. tracking cookies) koja bilježi posjete korisnika na web lokacijama i njihovo dijeljene sadržaja.

Oglašivačke mreže skupljaju takve kolačiće radi provođenja istraživanja tržišta i koriste ih kao pomoć ciljanih oglasa na korisnikovo računalo.

Primjer ako korisnik kupuje preko online trgovine pohranjuju se informacije o povijesti trgovine, omiljeni artikli. Praćenje korisnikovih navika radi poboljšanja reklamnog segmenta tvrtki općenito su bezopasna.

Oglašivački programi mogu se služiti tzv. tehnikom otmice pretraživača (eng. browser hijacker). Kad otimač pretraživača zarazi korisnikovo računalo, on preusmjerava web pretraživač na neželjene i nepoznate tražilice. Funkcija ovakvih programa je da se preusmjeri promet na određene web stranice zbog povećanje zarade na reklamnim materijalima. Često takvi program ne dopuštaju korisniku da promjeni početnu web stranicu i da se ukloni takav web pretraživač.

### 4.3.5. Otkupni programi (eng. ransomware)

„Ransomware“ ili otkupni program je vrsta zlođudnog programa koja korisniku onemogućuje ili uskraćuje pristup računalnom sustava i programima, te traži plaćanje otkupnine za njihovo ponovno korištenje.

Tehnike njegove zaraze su da koriste slične metode trojanskog konja i socijalnog inženjeringa. Korisnik pristupa zlođudnoj ili zaraženoj web stranici, koja sadrži obavijest koja ga upozorava da je zaražen zlođudnim programom i upućuje ga da preuzme i instalira odgovarajući program kako bi ga uklonio. Instaliranjem takvog programa korisnikovo računalo biva zaraženo.

Otkupni programi stvaraju smetnju i smanjuju performanse računalnog sustava korisnika, u obliku odskočnih poruka koji zahtijevaju da se otkupi određena svota njihove prevencije. Svakako, on može i šifrirati korisničke podatke nakon čega napadač ucjenjuje žrtvu da otkupi ključ kojim se podaci mogu povratiti.

## 4.4. Prevencija zloćudnih programa

### 4.4.1. Prevencija računalni virusa, crva i trojanskih konja

Zaštita od zloćudnih programa su antivirusni programi. Antivirusni programi mogu spriječiti, otkriti, izolirati i ukloniti viruse, crve, trojanske konje, špijunske i oglašivačke programe s korisnikovog računala. Oni provjeravaju odnosno skeniraju datoteke, čiste zaražene programe i neprekidno nadgledavaju ulazno-izlazne operacije u potrazi za zloćudnim kodom.

Antivirusni programi se isporučuju sa skenerom u stvarnom vremenu koji provjerava datoteke svaki put kada im korisnik pristupi. Nužno je da korisnik skenira cijeli operativni sustav, jer funkcija skeniranja u stvarnom vremenu pregledava one podatke kojim korisnik pristupa, dok se zloćudni programi mogu nalaziti u drugim mapama.

Antivirusni programi stvaraju tako zvane potpise svakog zloćudnog programa. Ti potpisi identificiraju sekcije koda koji se pojavljuju u zloćudnim programima. Tvrtke antivirusnih programa evidentiraju identitet zloćudnog programa u bazu podataka i tako traže potpise od svakog podatka na mreži ili računalu. Tako, ako se podaci poklapaju s potpisima koji su evidentirani, ti podaci se smatraju zaraženim. Takva metoda se zove „Detekcija bazirana na uzorcima“. Njezin nedostatak je, da antivirusna tvrtka mora imati evidentiran zloćudni program u svojoj bazi kako bi ga mogla identificirat. Novi zloćudni programi tako imaju slobodan prolaz unutar sustava, dok ih antivirusne tvrtke ne uspiju analizirati, kreirati potpis, testirati ga i distribuirati svojim korisnicima.

Osim detekcije bazirane na uzorcima, neki antivirusni programi imaju i metodu detekcije zvanu „Heuristička metoda“. Ova metoda se koristi kod novih i nepoznatih zloćudnih programa koji ispituje ponašanja koja upućuju na to da će takvi programi učiniti nešto nepoželjno računalnom sustavu, te kao takvi bivaju uklonjeni ili izolirani. Metoda prepoznaje aktivnosti kao što su brisanje, mijenjanje podatka ili instaliranje stražnjih vrata. Pregledava se svaka promjena rada u sustavu, pogotovo one radnje koje nisu uzrokovane od strane korisnika.

### 4.4.2. Prevencija špijunskih i oglašivačkih programa

Kako bi korisnik prepoznao da je pod utjecajem špijunski i oglašivački programi, mora obratiti na:

- Stabilnost sustava;
- Preopterećenje performansa sustava iako je korisnik neaktivan;
- Moraju objavljivat osjetljive informacije;
- Skrivanje njihove instalacije;
- Zatajivanje rada aplikacije;
- Nemogućnost ostvarivanje veze na internetu ili lokalnoj mreži;
- Isključivanje sigurnosnih postavka na web pregledniku i antivirusnim programima;

Oglašivački programi koji imaju funkciju praćenja web aktivnosti korisnika i generiranje oglasa i koji utječu na performanse sustava, korisnik može ukloniti primjenom antišpijunskog programa koji nudi opciju brisanja kolačića, putem postavka i instalacijom dodataka koje nudi web preglednik ili odlazak i brisanje podatka u mapi privremene datoteke.

Također postoje web preglednici koji prekrivaju IP adresu korisnika i omogućuju mu sigurno i anonimno korištenje interneta. Jedan od takvih web preglednika je web preglednik „Tor“.

Kako bi korisnik izbjegao instalaciju otmice pretraživača odnosno oglašivačke tražilice, korisnik tijekom odabira instalacije pojedinih programa mora izbjegavati automatsku instalaciju i pažljivo pročitati upute i dodatne opcije instalacije koje pojedini program nudi. Ako je pak instaliran otimač pretraživača, korisnik u postavkama svog pretraživača može ukloniti takvu vrstu tražilice.

Kada se pojavi novi oblik zloćudnih programa potrebno je mnogo testiranja i identificiranja da bi zloćudni program bio zapisan u repertoar antivirusnog programa. Antišpijunski programi i antivirusni programi se međusobno upotpunjuju, te tako antišpijunski program može uloviti špijunske, oglašivačke i ostale zloćudne programe, što je antivirusni program propustio i daje mu bezbrižno vrijeme da ga provede u svoju bazu podataka.

Svakako, korisnik bi trebao izbjegavati instalaciju dva antivirusna programa. Svaka antivirusna tvrtka ima svoj vlastiti skup definicija, što znači da svaka kompanija identificira i

rješava zloćudne programe na drugačiji način. Tako, dva se antivirusna programa mogu sukobljavati, jer prvi antivirusni program smatra drugog kao prijetnju ili obrnuto. To uzrokuje preopterećenje računalnih performansi i smanjuje produktivnost antivirusnog programa za pronalaženje pravih prijetnji.

Antišpijunski programi ne uzrokuju takve smetnje, jer ne dolaze s opcijom skeniranja u stvarnom vremenu već se pokreću na zahtjev korisnika. U slučaju da antišpijunski program dolazi s opcijom skeniranja u stvarnom vremenu poželjno ju je isključiti i pokrenuti manualno u slučaju ako korisnik zamijeti sumnjive aktivnosti na svom sustavu.

Špijunski programi često koriste funkciju „Keystroke logger" koja prati svaku pritisnutu tipku korisnika. Antišpijunski programi omogućuju maskiranje ili šifriranje svake pritisnute tipku na tipkovnici i omogućuje prevenciju bilo kakvog oblika nadgledavanje rada korisnika.

Antišpijunski ili antimalwer programi prate trendove novonastalih zloćudnih programa te ih mogu uloviti i ukloniti prije antivirusnih programa.

### 4.4.3. Prevencija otkupnih programa

Ako se radi o odskočnim prozorima otkupnog programa, mogu se ukloniti novim ili nadolazećim ažuriranjem antimalware i antišpijunskim programa. Ako je korisnik zaražen s otkupnim programom koji je šifrirao korisničke podatke, nažalost ne može povratiti ni na koji način svoje podatke ukoliko on ne uplati napadaču. Ovakva vrsta zloćudnog programa koristi vrlo visoku razinu enkripcije. Gotovo je nemoguće vremenski probiti takvu vrstu zaštite i pokazalo se da napadači neće ukloniti zaštitu ukoliko im žrtve uplate.

Korisnici trebaju:

- Izbjegavati pristup nepouzdanim stranicama;
- Izbjegavanje instalacije programa koje takve stranice nude;
- Izrada sigurnosne kopije, kopiranje podataka na druga računala ili kopiranje podataka „online" čiji poslužitelji usluga nude mrežnu pohranu podataka s dodatnom enkripcijom podataka (primjer takvog programa je backblaze);

## 4.5. Botnet mreža

Simptomi da je korisnik dio bootnet mreže mogu biti većina navedenih zloćudnih programa u prijašnjem poglavlju. Računala korisnika mogu biti resursi za napade na druga računala te inficirana računala botnet mrežom mogu postati oružje kojim se napadači mogu poslužit protiv tvrtke ili vlade. Općenito govoreći ako su računalni resursi (procesor, memorija itd.) umreženi njihova snaga se povećava. Takva računala nalaze se pod kontrolom jednog ili nekoliko hakera koji mogu izvoditi razne napade (slanje neželjene pošte, špijunski programi, širenje zloćudnih programa…).

Haker je onaj koji potajno i neovlašteno upada u tuđa računala ili u mreže, provjeravajući ili mijenjajući programe i podatke pohranjene u njima (Anić, 2004.).

Hakeri se mogu služiti automatiziranim programskim alatima koji skeniraju široko područje interneta u potrazi za ranjivim ili nezaštićenim računalima. Nakon što pronađu popis ranjivih računala, ulaze neovlašteno u njihov informacijski sustav instalirajući zlonamjerne programe pomoću kojih napadači mogu nad njima ostvariti kontrolu.

Zaražena računala nazivaju se botovi u prijevodu roboti koji predstavljaju sinonim za zaražena računala u kontroli napadača.

Botovi su unaprijeđena inačica crva i virusa koji koriste programe za razmjenu podataka putem RPC (eng. Remote Producer Call) protokola te se na taj način šire. To su protokoli http ili IRC (eng. Internet Relay Chat) koji omogućavaju direktnu komunikaciju s više računala.

### 4.5.1. Distribuirani napadi uskraćivanjem usluga

Hakeri se mogu koristiti vrstom distribuiranih napada uskraćivanja usluga (eng. Distibuted Denail-of-Service). To je napad u kojem mnoštvo kompromitiranih sustava napada jedan cilj te time uzrokuje uskraćivanje usluga za korisnike ciljanog sustava. Tako napadač koji upravlja botnet mrežom može narediti svim računalima da pristupe određenoj internetskoj stranici, usluzi, odnosno poslužitelju u isto vrijeme.

Distribuirani napadi uskraćivanja usluga sastoje se od odašiljanja velike količine mrežnog prometa na cilj poput web lokacija ustanove i time rezultira preopterećenje informacijsko sustava. Ovisno o broju umreženih računala napadač tako može ugroziti rad informacijskog sustava poslužitelja što može i rezultirati izbačaj iz web lokacije mreže.

Napadači odnosno hakeri takav napad mogu iskoristit, služeći se ucjenama da od vlasnika informacijskog sustava ili web lokacije pridobiju novac, u suprotnom ciljana lokacija će biti ugašena. To im najčešće uspijeva jer ustanove nisu sklone tražiti pomoć od zakonskih tijela zbog gubitka ugleda.

### 4.5.2. Neželjena elektronička pošta (eng. spam)

Botnet može pretvoriti zaražena računala u stroj za širenje neželjene elektroničke pošte. Ma da je stopa uspješnosti oko dva posto, jer su davatelji internetski usluga i ant-spam organizacije brzi u otkrivanju i blokiranju svakog računala koji šalje takvu poštu. Napadače to ne zaustavlja. Napadači putem „botnet“ mreže mogu poslati naredbu zaraženim računalima da šalje tisući čak i milijune nepoželjnih elektroničkih pošta i tako anti-spam i ostalie organizacije blokiraju računala korisnika kao izvor „spama“. Zaražena računala tako ne mogu slati više elektroničku poštu jer su računala korisnika blokirana.

Ostali botnet mrežni napadi koriste se tehnikama socijalnog inženjeringa. To su često mrežne krađe identiteta (eng. phishing) kojim putem poveznica i lažnih web lokacija uvjeravaju korisnike da unesu osobne informacije.

## 4.6. Prevencija botnet mreža

Zaštita od botnet-a je poprilično otežana jer računala koja su uključena u botnet mrežu su lokacijski raštrkana i imaju promjenjivu IP adresu. Administratori mogu zaštiti informacijski sustav konfiguracijom vatrozidova u mreži. Vatrozid (eng. firewall) nadzire programe i aplikacije koji pokušavaju započeti komunikaciju s korisnikovim računalom putem interneta.

Često botnet mreže koriste DNS (eng. Domain Name System) servise kako bi kreirale poddomenu IRC (razgovor putem interneta) poslužitelja odnosno usmjeravaju žrtve računala

prema nepouzdanim IP adresama napadača. Takvi servisi su uočljivi i njihovo uklanjanje može prouzročiti pad botnet mreže te ustanove ulažu u svoje domene kako bi ih očistili od takvih poddomena.

Otkrivanjem jednog poslužitelja botnet mreže često rezultira i do otkrivanja ostalih poslužitelja botnet mreže pa  i otkrivenje glavnog bot računala.

Popularni operativni sustavi stvorili su tehnike naprednih algoritma u vatrozidovima koji uočavaju i uklanjaju bot ponašanje.

Da bi izbjegli infekciju bot mreže:

- moramo izbjegavati skidanje i instaliranje sadržaja iz nepouzdanih stranica, kao što su piratske stranice;
- Redovno ažuriranje novijih verzija i sigurnosnih zakrpa aplikacija, antivirusa i operativnih sustava;
- Moramo biti oprezni s sumnjivim porukama (phishing, pharming), te takve poruke izbrisati, prijaviti i proširiti informaciju svim korisnicima informacijskog sustava;

Simptomi botneta:

- Sustav je sporiji nego inače;
- Tvrdi disk radi stalno iako ne koristimo računalo;
- Dolazi do nestajanja ili promjene strukture datoteka;
- Kolege i prijatelji vam javljaju da su dobili mail koji niste poslali;
- Vatrozid vas obavještava da se neki program pokušava spojiti na Internet;
- Antivirusni ili drugi sigurnosni alat vas upozorava na sumnjive pojave;

Izvor: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2014-01-340.pdf
(23.8.2016. / 21:51)

## 4.7. Rizici bežične mreže

U suvremenim informacijskim tehnologijama sve se više odbacuje ideja o žičnom povezivanju a sve se više pažnje poklanja bežičnom ili WLAN umrežavanju. Bežična povezivanja omogućuju mobilno dijeljenje podataka i eliminira kabelsko povezivanje koje stvara nered u prostoru. Za umrežavanje koristi se usmjerivač (eng. router) koji usmjerava podatkovne pakete. Svakako žično umrežavanje nije imalo sigurnosne propuste kao bežično, osim ako se netko nije povezao žično putem usmjerivač.

Bežične mreže (eng. WLAN, wireless local area network) koriste tako zvane pristupne točke (eng. Access Point) koji osiguravaju pristup mreži za bežične korisnike. One komuniciraju s drugim pristupnim točkama bežično ali mogu se i podesit žično s korisnicima.

Mnoge javne bežične mreže ne koristi zaporke, odnosno bilo koji način šifriranja ili enkripcije. Što omogućuje napadaču da vidi sav promet korisnika koji su povezani s tom mrežom. Napadačima kod takvih mreža ne trebaju nikakve vještine ili napredne tehnike upada. Na internet mogu preuzeti i instalirati programe koji omogućuju špijuniranje nezaštićenih mreža.

Većina modernih usmjerivača koristi enkripciju WPA2 koja omogućuje šifriranje protoka podataka. Ona predstavlja veliku sigurnost za ograničeni broj korisnika kao što su članovi obitelji, poslovni suradnici ili ustanove. Bežična mreža sigurna je samo ukoliko je dostupna užem krugu korisnika.

Napadač može ukrasti informaciju služeći se aplikacijama za njuškanje koje presreću i prikupljaju sav vidljiv promet na mrežnom kanalu. Iako WPA2 kodira svaku vezu između Wi-fi mreže i korisnika, dizajnirana je da s mreže drži podalje samo one korisnike koji ne znaju zajednički ključ. Pristupajući na javnu mrežu napadač se služi aplikacijama za njuškanje i zaobilazi četverostruko rukovanje te dohvaća zajednički ključ i tako može dešifrirat sav promet koji je konstruiran i namijenjen za korisnikov uređaj, sve dok se zajednički ključ ne promjeni.

Mrežno njuškanje je najčešće pasivna aktivnost koja nadgledava aktivnosti svih korisnika koji su umreženi na javnu pristupnu točku. To su svi podaci, paketi i promet koji su uhvaćeni.

Najčešće se koristi za statističku analizu s namjerom razumijevanja koliko prometa putuje kroz mrežu, kojeg oblika ili koji je broj postotka posjeta određenih internetskih stranica.

Mogu se, također nadgledavati koji sustavi uspostavljaju komunikaciju s drugim sustavima što je vrlo korisno za mrežne menadžere, administratore sustava, kako bi mogli imati uvid u prijenosne količine podataka i sumnjive aktivnosti u sustavima.

Napadač može pratiti i saznati aktivnosti od korisnika i tako pristupiti njegovim korisničkim podatcima, zaporkama i ostalim povjerljivim informacijama koje se nalaze na mreži. Može se i služiti aktivnim njuškanjem koje se oslanja na slanje velikih količina prometa, što ima za posljedicu preopterećenje mreže.

Svaki korisnik u svom vlastitom domu može pristupiti u uvidu svog vlastitog prometa što je dovoljno da ima pristup svojoj bežičnoj mreži s odgovarajućom aplikacijom.

Povezivanjem na javnu pristupnu točku putem računala, napadač koristi aplikaciju, koja omogućuje da stekne povjerenje od usmjerivača da je računalo napadača legitimni usmjerivač. Tako se korisnici mogu povezati na lažnu pristupnu točku koja omogućuje napadaču da ostala računala i usmjerivači šalju sve svoje pakete na napadačevo računalo.

## 4.8. Prevencija rizika bežične mreže

Korisnici koji ostvaruju vezu s javnim pristupnim točkama mogu se zaštiti na nekoliko načina:

- Pristupanjem povjerljivim web stranicama koji na svojim web adresama imaju ikonu lokota u desnom kutu ili „https“ web pretraživača. Ako stranica počinje s „https“ tada je informacija na web stranicama šifrirana prije nego što je poslana. Takve web stranice su šifrirane i omogućuju zaštitu od napada koji posreduju u komunikaciji;
- Korištenje virtualne privatne mreže (eng. Virtual Private Network). Virtualne privatne mreže su tehnologija koja osigurava konekciju i povezivanje računala koji su geografski odvojeni od ostalih korisnika, kupaca ili poslovnih partnera. Najčešće se mogu preuzeti besplatno ili se mogu kupiti ovisno o opcijama koje nude. Virtualne privatne mreže omogućuju šifriranje internet konekcije i eliminiraju rizike privatnosti. VPN omogućuje: sigurnost kod povezivanja pristupnih točaka, potpunu mrežnu privatnost i anonimnost, sprječavanje cyber kriminala i potpunu zaštita internet bankarstva;

- Korisnik bi svakako trebao pitati pružatelja ili ustanovu koji je naziv njihove pristupne točke, jer lažne bežične točke mogu sadržavati slične nazive ali ne i nazive legitimne pristupne točke;
- Povezivanje na WPA i WPA2 mreže koje imaju pouzdanu enkripciju od WEP-a. Ako korisnik nije siguran na kojoj mrežnoj enkripciji je povezan, informaciju može pronaći pod mrežnim postavkama.
- Ažuriranjem i postavljanje vatrozida, korisniku se omogućuje povezivanje na javnu pristupnu točku uz dodatnu zaštitu enkripcije.

# 5. Sigurnosna politika informacijskih sustava i tehnologija

Informacijski sustavi u sebi sadrže povjerljive podatke kojima se služe korisnici koji imaju ovlasti nad tim podacima i korisnici kojima je omogućeno da koriste podatke informacijskog sustava. To su na primjer: ime identifikacije, lozinka, podaci i obavijesti sustava koji ne smiju biti javno dostupni bez odobrenja ovlaštenih korisnika. Time se provodi sigurnosna politika koja zadovoljava navedene uvjete.

Sigurnosna politika predstavlja zaštitu slobode individualnih osoba, ostvaruje i implementira sankcijske mjere sigurnosne kontrole te omogućuje sigurnu razmjenu materijalnih i ljudskih resursa. To znači da sigurnosna politika informacijskih sustava obuhvaća tvrtke, državne institucije, svu računalnu opremu (hardver i softver), sve zaposlenike i korisnike sustava. Svi oni dijele zajednički interes da im se osiguraju uvjeti zaštite i sigurnosti informacija, koji su važni za ostvarenje individualnih, tehničkih, organizacijskih, zakonskih i operacijskih ciljeva.

Svrha sigurnosne politike je da omogući upravljanje s rizicima i sigurnošću informacijskih sustava te da definira elemente prihvatljivog i neprihvatljivog načina ponašanja. U suprotnom određuju se sankcije, u koliko se korisnik ne pridržava pravila koje je sigurnosna politika postavila. Da bi se provela mora biti usklađena s zakonima i propisima od države u kojoj se provodi, te biti odobrena i prihvaćena od strane uprave.

Korisnici i administratori pojedinog informacijskog sustava moraju biti upoznati s sigurnosnom politikom i njezinim uvođenjem u sustav. To znači da je potrebna izobrazba svih korisnika i administratora pogotovo kod novih korisnika sustava. Zaposlene je potrebno također upoznati sa osnovnim pravilima za korištenje elektroničke pošte, zaporki i pravilima o čuvanju povjerljivih informacija.

Vrlo je važno konstantno obrazovanje i usklađivanje pravila korisnika sustava, te je ustanova obavezna na svojim javnim web stranicama postavljati i ažurirati politiku prihvatljivog korištenja. Ustanova može postavljati i prilagođavati svoja pravila kako bi njihova sigurnosna politika bila usklađena s njihovim uvjetima i poslovanjem. Međutim, ne smije zanemarivati osnovne principe i pravila „Politike prihvatljivog korištenja“.

Sigurnosna politika mora omogućit slobodu korisnika u onoj mjeri koliko je potrebno za obavljanje poslova i ostvarenje cilja informacijskog sustava.

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu koja se nalazi u prostorima Ustanove;
- Administratore informacijskih sustava;
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti;
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

Izvor: http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf (2.8.2016./11:30)

Provođenjem sigurnosne politike informacijskog sustava moraju se znati uloge i zadaci svih sudionika, kako bi se raspodijelili zadaci, obaveze, obrazovanje i formirala tijela za upravljanje sigurnošću.

Slika 3: Primjer javne objave Sigurnosne politike i pravila sigurnosnog i efikasnog korištenja Facebook stranice




Izvor: https://www.facebook.com/security/ (2.8.2016./12:40)

Slika 3 predstavlja primjer sigurnosne politike „Facebook stranice“. Njihova sigurnosna politika svojim korisnicima navodi da čuvaju svoje zaporke i da ih ne koriste nigdje osim svog facebook korisničkog računa. Zaporke ne smiju sadržavat imena i obične riječi.

Da bi se razina sigurnosti korisničkog računa uvećala, zaporka korisnika mora biti vrlo složena. Facebook nikad neće poslat poruku ili elektroničku poštu u kojoj se zahtijeva od korisnika detaljni podaci prijave ili broj računa kreditne kartice. Ako netko drugi kontaktira korisnika i zahtijeva od njega povjerljive informacije, od korisnika se očekuje da ne pristupa nikakvim poveznicama koje se nalaze u poruci, već da prijavi sumnjivu aktivnost facebook stručnjacima, te blokira korisnika i izbriše njegovu poruku.

Informacijski sustav facebook-a je dobar primjer zato što sadrži puno privatnih i povjerljivih informacija. Time je facebook na visokoj meti napadača te se zahtijeva od facebook-a visoka profesionalnost od strane administratora.

## 5.1. Pravilnici sigurnosne politike

Pravilnici sigurnosne politike su nužni da korisnike informacijskog sustava nauče o pametnom i povjerljivom korištenju informacijskih sustava, da bi sustav kvalitetno i efikasno imao profesionalne administratore i korisnike koji su upoznati s najnovijim trendovima sigurnosti. Osnovni cilj svakog informacijskog sustava je da posjeduje kvalitetnu tehničku podršku i dobro informiran korisnike.

### 5.1.1. Pravilnik o rukovanju zaporka

Mnogo korisnika zanemaruje sigurnost svog računalnog sustava jer smatraju da ne sadrže vrijedne informacije. Upad napadača u računalo pojedinog korisnika može uzrokovati stvaranjem polazne točke na važnija računala i tim aktom ugrozit informacijski sustav u cjelini.

Ukoliko se korisnici ne pridržavaju pravilnika o rukovanju zaporki ugrožavaju informacijski sustav i moraju biti ponovno educirani. Tako su se svi zaposlenici i korisnici informacijskog sustava dužni pridržavati pravila o korištenju zaporki, a administratori su ih dužni ugraditi u informacijski sustav organizacije.

Pravila za korištenje zaporki:

- Minimalna dužina zaporke trebala bi se sastojat od šest znakova;
- Hakeri ili socijalni inženjeri posjeduju programe koji im omogućuju da dešifriraju jednostavne lozinke. Tako se od korisnika očekuje da ne koristi jednostavne riječi iz rječnika;
- Miješanjem malih i velikih slova, postavljanje brojeva, simbola i unošenje razmaka, dodatno otežava dešifriranje;
- Zaporke ne smiju sadržavati osobna imena, imena bliskih osoba, kućnih ljubimaca;
- Postavljanje više zaporki i njihovo učestalo mijenjanje.

Izvor: http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf (19.8.2016 / 17:15)

5.1.2. Pravilnik o korištenju elektroničke pošte

Sve ustanove moraju obratiti veliku pozornost na korištenje elektroničke pošte koja je dio svakodnevne komunikacije.

Pravila za korištenju elektroničke pošte:

- Zaposlenicima se otvara korisnički račun radi obavljanje posla;
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad;
- Zaposlenik mora biti svjestan da slanje elektroničkih poruka ili pošte ne predstavlja samo sebe već i ustanovu u kojoj radi;
- Zaposlenik se mora pridržavat pravila pristojnog ponašanja;
- Zaposleniku nije dozvoljeno slanje lančanih poruka gdje opterećuje mrežni sustav i ljudima oduzima radno vrijeme;
- Poruke se ne mogu prosljeđivati bez potvrde autora. Svaka napisana i poslana poruka smatra se dokumentom koji je pod propisima autorskog prava i intelektualnog vlasništva;
- Sve poruke automatski se pregledavaju putem aplikacije koja uočava viruse. Ako poruka sadrži zlonamjeran kod poruka neće biti isporučena, a pošiljatelj i primatelj bit će obavješteni;
- Ustanova zadržava pravo filtriranja poruka s namjerama da se zaustave neželjene poruke (eng. spam);

- U slučaju rizika uzrokovan sigurnosnim incidentom, sigurnosni tim može pregledavat kompletan sadržaj disk i e-mail poruke;
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati.

Izvor: http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf (19.8.2016 / 17:15)

### 5.1.3. Pravilnik o antivirusnoj zaštiti

Svaka ustanova koja posjeduje informacijski sustav mora instalirati i primijeniti antivirusni program. Antivirusni program je obaveza ustanova, administratora računala i svakog korisnika i provodi se na nekoliko razina:

- Na poslužiteljima elektroničke pošte;
- Na internim poslužiteljima, gdje se stavlja centralna instalacija;
- Na svakom osobnom računalu korisnika;

Administratori su dužni instalirati antivirusne programe na sva korisnička računala. Korisnici ne smiju samovoljno isključiti antivirusnu zaštitu na svom računalo. Ukoliko iz nekog razloga moraju privremeno zaustaviti antivirusni program, korisnici moraju obavijestiti administratore.

Izvor: http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf (19.8.2016 / 17:15)

### 5.1.4. Pravilnik o zaštiti neželjene pošte (eng. spam)

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala da se spriječi što više neželjenih poruka.

Prva razina zaštite jest da se definira ulazni filter koji će prilikom primanja poruke konzultirati baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje, te

baza s adresama poznatih „spamera.“ Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao „spam“ spremati na određeno vrijeme u karantenu.

Treću razinu zaštite određuju sami korisnici. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o „spamu“. Kako nije uvijek moguće pouzdano definirati što je „spam“, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Informatičar zadužen za sigurnost će obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike:

- Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj.
- Upozorenja na viruse su često lažna i šire zablude.
- Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

Izvor: http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf (19.8.2016 / 17:15)

## 5.2. Norme

Sigurnost i zaštita informacijskog sustava je tema kojoj se posvećuje dosta pažnje jer je ona postala moralna obveza svakog vlasnika informacijskog sustava. Da bi se olakšalo samo uvođenje sigurnosti informacijskog sustava na tržištu, postoje standardi koji omogućuju uspostavljanje kvalitetne sigurnosne kontrole. Tako zvana „Međunarodna organizacija za standardizaciju“ (eng. International Organization for Standardization) je usko povezana, te surađuje s „Međunarodnom komisijom za elektrotehniku“ (eng. International Electrotechnical Commission) koja je odgovorna za standardizaciju električne opreme.

Tako na tržištu imamo dva standarada ISO/IEC 17799 i 27001 koja nisu odvojena jedan od drugog, već su oba nužna za uspostavu kvalitetnog upravljanja sigurnošću informacijskog sustava.

### 5.2.1. Norma ISO/IEC 17799

Među svim normama, na međunarodnom planu ipak se najviše prihvaća ISO 17799, a ponajviše se odnosi na Europu i Japan. Razlog prihvaćenosti ove norme jest što osigurava fleksibilnost pri upravljanju jer ne zadire u konkretnu tehničku implementaciju, što je čini primjenjivim u organizacijama različitih tehničkih sustava. ISO 17799 daje osnovne i nužne preporuke i elemente koje bi trebalo poštovati pri izradi i primjeni vlastitog modela upravljanja sigurnošću. ISO 17799 2000. godine postaje prva međunarodna norma vezana uz upravljanje informacijskom sigurnošću.

Sadržaj norme ISO/IEC 17799:2000:

- Politika sigurnosti koja se izrađuje u obliku posebnog dokumenta;
- Organizacijska sigurnost koja uključuje način organizacije provedbe politike sigurnosti u poduzeću;
- Klasifikacija i nadzor imovine koja se primarno odnosi na imovinu informacijskog sustava;
- Sigurnost osoblja koja uključuje upravljanje ljudskim resursima i zaštitu tajnosti podataka;
- Fizička sigurnost i sigurnost okoline kojom se štiti fizički pristup imovini informacijskog sustava;
- Upravljanje komunikacijama i operativom koje uključuje upravljanje ljudskim resursima i zaštiti tajnosti podataka;
- Fizička sigurnost i sigurnost okoline kojom se štiti fizički pristup imovini informacijskog sustava;
- Upravljanje komunikacijama i operativom koje uključuje zaštitu logičke imovine od svih vrsta zloporaba;
- Kontrola pristupa kojom se štiti pristup resursima informacijskog sustava od neovlaštenih korisnika iz poduzeća, ali i putem mreže;
- Razvoj i održavanje sustava kojim se propisuje način ugradnje zaštite resursa sustava u tijeku razvoja i primjene informacijskog sustava;
- Upravljanje kontinuitetom poslovnih aktivnosti kojim se sprečavaju prekidi poslovnih aktivnosti i štite kritični poslovni procesi;

- Usklađenost sa zakonskom regulativom, te ocjena politike sigurnosti i suglasnosti s tehničkim uvjetima.

Izvor: http://hrcak.srce.hr/11861 (24.7.2016. /15:37)

Slika 4: Osnovni elementi informacijske sigurnosti ISO 17799:2000




Izvor:http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-133.pdf (3.8.2016./ 15:50)

Povjerljivost je zaštita podatka od neovlaštenog pristupa. Ključni oblik povjerljivosti je identifikacija korisnika i provjera autentičnosti. To je proces prijave korisnika u sustav, pri čemu sustav zna da takav korisnik postoji u bazi podataka. Primjer korisnik „xy“ želi se prijaviti u sustav, sustav vrši provjeru da li je korisnik „xy“ prijavljen u sustav i ako je, tada slijedi proces provjere autentičnosti. Provjera autentičnosti je proces kojim sustav želi biti siguran da je korisnik koji se prijavljuje pod imenom „xy“ upravo osoba „xy“. Imamo nekoliko oblika provjere autentičnosti, a najrašireniji je unos lozinke, no sve se više razvija tehnička oprema poput otiska prsta ili mrežnice oka, gdje se vrši proces skeniranja oblika i pretvara u digitalne signale.

Najčešće prijetnje povjerljivosti su:

- Hakeri;
- Lažno predstavljanje;
- Nezaštićeno preuzimanje podataka;

- Neovlaštena aktivnost;
- Računalni virusi.

Integritet jest zaštita procesa ili programa kako bi se onemogućilo namjerno ili slučajno neovlašteno mijenjanje podataka. Neovlaštene aktivnosti tada ne mogu mijenjati podatke na način da izbrišu, promijene ili učine podatke od presudne važnosti nesigurnom. Samo ovlaštene osobe mogu mijenjati podatke.

Polazne točke za kontrolu integriteta su:

- Dodjeljivanje pristupa na temelju potreba. Funkcija ove točke je da se omoguće korisnicima samo oni podaci koji su im potrebni za obavljanje zadanih poslova. Bilježi se podatak o mijenjanju podataka, kako bi se utvrdilo jesu li podaci ispravno mijenjani od ovlaštene osobe, čime se omogućuje zaštita integriteta podataka.
- Razdvajanje obveza osigurava da niti jedan pojedinac nema potpunu kontrolu transakcija, već za njezino izvršenje mora biti odgovorno dvoje ili više ljudi. Svaki od pojedinaca ima ulogu kreiranja transakcija i ulogu izvršenja transakcija, time se sprječava da se transakcije obavljaju radi vlastitih interesa.
- Rotiranje obveza. Zaposlenici se s vremenom mijenjaju kako bi kontroliranje transakcija za osobne potrebe bilo složenije, ali i sigurnije. Time se smanjuju neovlaštene aktivnosti među zaposlenicima, koji svaki od njih ima uvid u stanje podataka prijašnjih zaposlenika.

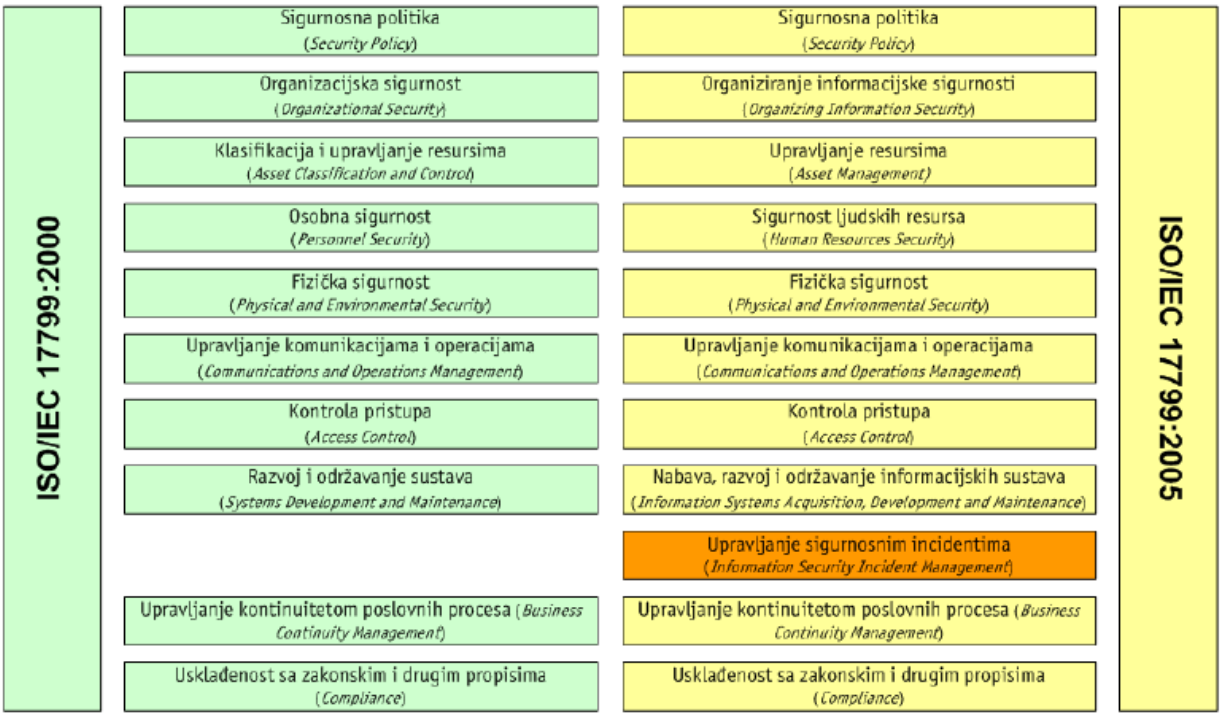
Raspoloživost je garancija dostupnosti relevantnih podataka u prihvatljivom vremenskom terminu zahtijeva korisnika, odnosno onda kada je to potrebno.

### 5.2.2. Norma ISO/IEC 17799:2005

Norma „ISO/IEC 17799:2005“ je drugi izdani standard 2005. godine, i omogućuje nova poboljšanja sigurnosti organizacije. Ostvaruju se nova i bolja poboljšanja sigurnosti s drugim poslovnim subjektima i omogućuje se rješavanje problema koji mogu nastati korištenjem mobilnih tehnologija i bežičnih računalnih mreža.

Za razliku od prošlog standarda, „ISO 17799:2005“ je dopunjeni standard koja detaljnije opisuje specifikacije procesa upravljanja informacijskom sigurnosti, kako bi se procesi upravljanja mogli što bolje opisati. Neki nazivi su izmijenjeni, no dodana je i nova inačica pod nazivom „Upravljanje sigurnosnim incidentima“ .

Slika 5: Usporedba ISO 17799:2005 i ISO 17799: 2000 standarda




Izvor: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-133.pdf (4.8.2016./16:33)

- Sigurnosna politika nema značajne promjene u odnosu na prošli standard, osim da sigurnosna politika može biti dio opće politike organizacije, no ne mora prijeko potrebno biti dokument.
- Organiziranje informacijske sigurnosti u novoj inačici uključeni su vanjski partneri. Detaljno se određuju kontakti odgovornih osoba i sigurnosnih grupa. Rješavanje problema u nekim situacijama potrebna je pomoć ovlaštenih institucija i potrebna je komunikacija s drugim stručnjacima sigurnosti pri sprječavanju nezgoda unutar sustava.
- Sigurnost ljudskih resursa. U prethodnoj inačici osobna sigurnost odnosila se na ciljeve poslovne sigurnosti, obuci korisnika i ponašanja zaposlenih u slučaju sigurnosnih nezgoda. Nova inačica sigurnosti ljudskih resursa odnosi se na redoslijed vremena i utvrđivanja zaposlenih: prije zapošljavanja, tijekom radnog odnosa i prestanak radnog

odnosa. Cilj je da se postave kontrole koje se odnose na odgovornost uprave prema prestanku radnog odnosa zaposlenih, vraćanje resursa i prestanak prava dolaska na posao.

- Upravljanje komunikacijama i operacijama. Zadatak je osigurati pravilan i siguran rad svih elemenata za obradu informacija. Upravljanje komunikacija i operacija određuje odgovornost izvršavanja svih pravila i procedura koje se koriste prilikom incidenata.

  Novi standard „ISO 17799:2005“ definira ciljeve koje stari standard nije poznavao u tom obliku:

  - Upravljanje vanjskim sustavima;
  - Sigurnosna pohrana podataka;
  - Razmjena informacija;
  - Elektroničko poslovanje;
  - Nadgledanje sustava.

Izvor: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-133.pdf (4.8.2016./20:06)

- Upravljanje sigurnosnim incidentima (eng. Information security incident managment) je nova kategorija koja se pojavljuje u „ISO 17799:2005“ standardu. Kategorija definira dva cilja:
  - Prijavljivanje sigurnosnih incidenata i ranjivosti (eng. Reporting information security events and weaknesses)
  - Upravljanje sigurnosnim incidentima i unapređenjem informacijske sigurnosti (eng. Management of information security incidents and improvements).

  Ova kategorija predstavlja skup ciljeva i sigurnosnih kontrola, od kojih je većina postojala i u prethodnoj inačici standarda no, međutim, te su kontrole bile definirane u različitim kategorijama i ciljevima, (Osobna sigurnost – Prijavljivanje sigurnosnih incidenata i nepravilnosti u radu, Upravljanje komunikacijama i operacijama – Operativne procedure i odgovornosti, te Usklađenost sa zakonskim i drugim propisima – Sukladnost sa zakonskom regulativom). Standard je uočio da je upravljanje sigurnosnim incidentima jedinstven proces, te ga na taj način i definirao, što predstavlja znatno unaprjeđenje u odnosu na staru inačicu standarda.

Izvor: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-133.pdf (4.8.2016./20:26)

Ostale inačice koje nisu nabrojane nisu značajno izmijenjene u odnosu na staru inačicu standarda.

5.2.3. ISO 27001

„ISO 27001“ je najraširenij sigurnosni standard koji se može implementirat u bilo kojoj organizaciji i kako se kao u takvoj organizaciji može organizirati informacijska sigurnost. Omogućuje implementaciju i uspostavu sustava upravljanja sigurnošću informacija, a sadrži skup zahtijeva koje organizacija mora ispuniti kako bi se priznao certifikat za informacijsku sigurnost. Prvi standard „ISO 27001:2005“ objavljen je 2005. godine. Njegova implementacija sastoji se od dvije faze:

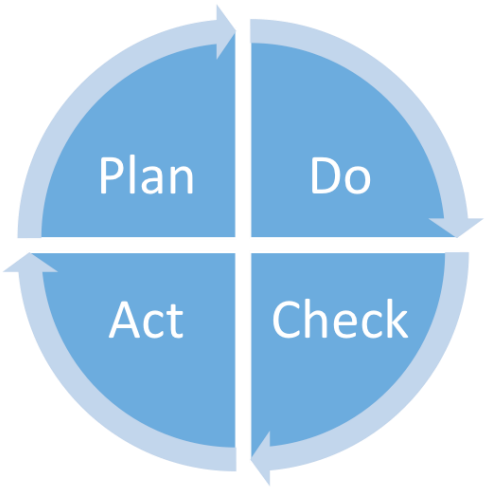
- Prva faza je administrativna u kojoj menadžment donosi važne odluke putem ISO projekata, i provodi njezina pravila i procedure.

- Druga faza podrazumijeva nekoliko koraka, a to su: određivanje opsega i granice ISMS (Informacijski sustav upravljanja sigurnošću – zbirka politika koje se odnose na sigurnost informacijskih sustava), definiranje politike ISMS, evidencija imovine (za čuvanje, prijenos i obradu informacija), procjena rizika, donošenje dokumenata „izjava prihvatljivosti“, prihvaćanje i odobrenje uprave, priprema dokumentacije, implementacija ISMS, izrada procedura za upravljanje incidentima, provođenje monitoringa, identifikacija i implementacija poboljšanja itd.

Izvor: http://sigurnost.zemris.fer.hr/ISMS/2008_kovacevic/norme.html (5.8.2016./ 19:41)

ISO 27001 propisuje kako se upravljanjem informacijskom sigurnošću može ostvariti kroz metodom upravljanja informacijskom sigurnošću. To možemo zaključiti putem metodologije kontinuiranog poboljšavanja koja se temelji na „Demingovom krugu“ ili tako zvani PDCA (Plan/Do/Check/Act) pristupu. Taj čin omogućuje, da se faza upravljanja sigurnošću neprekidno provodi kako bi se umanjili rizici za povjerljivost, cjelovitost i dostupnost informacija.

Slika 6: PDCA model primijenjen na ISMS




Izvor: http://www.infrahouse.com/da/blog/author/pia-pedersen/pdca-plan-do-check-act-cycle-simple-and-useful-continuous-improvement (5.8.2016./ 20:53)

- Plan (faza planiranja) – u ovoj fazi uspostavlja se sigurnosna politika, ciljevi, procesi, procedure, postupci relevantni za upravljanje rizicima i u konačnici poboljšanje informacijske sigurnosti.
- Do (faza implementacije) – sve što je isplanirano u prethodnoj fazi provodi se u djelo. To se ostvaruje izradom projektnog plana kojim se procjenjuje rizik, odnosno implementacija i upravljanje sigurnosnom politikom, kontrola procesa i procedura.
- Check (faza provjere) – provjera izvršene implementacije i dostava izvješća rezultata menadžerima na preispitivanje.
- Act (faza djelovanja) – u zadnjoj fazi poduzimaju se korektivne i preventivne radnje na temelju rezultata zasnovanih iz izvješća, a sve to u svrhu stalnog poboljšanja upravljanja informacijskom sigurnošću. Korektivne mjere provode se nakon ostvarenog sigurnosnog rizika kako bi se spriječila ponovna pojava rizika u budućnosti. Preventivne mjere se koriste za unajmljivanje vjerojatnosti pojave rizika i unajmljivanje potencijalnih šteta.

Cilj svih normi je maksimalna zaštita informacijskih sustava i poslovnih resursa, a certifikacija je završni čin koji dokazuje primjenjivost. Standardi jednostavno predstavljaju poslovni indikator te je pokazatelj kako i na koji način smanjiti broj incidenta u sustavu.

## 6. HUB istraživanje o sigurnosti

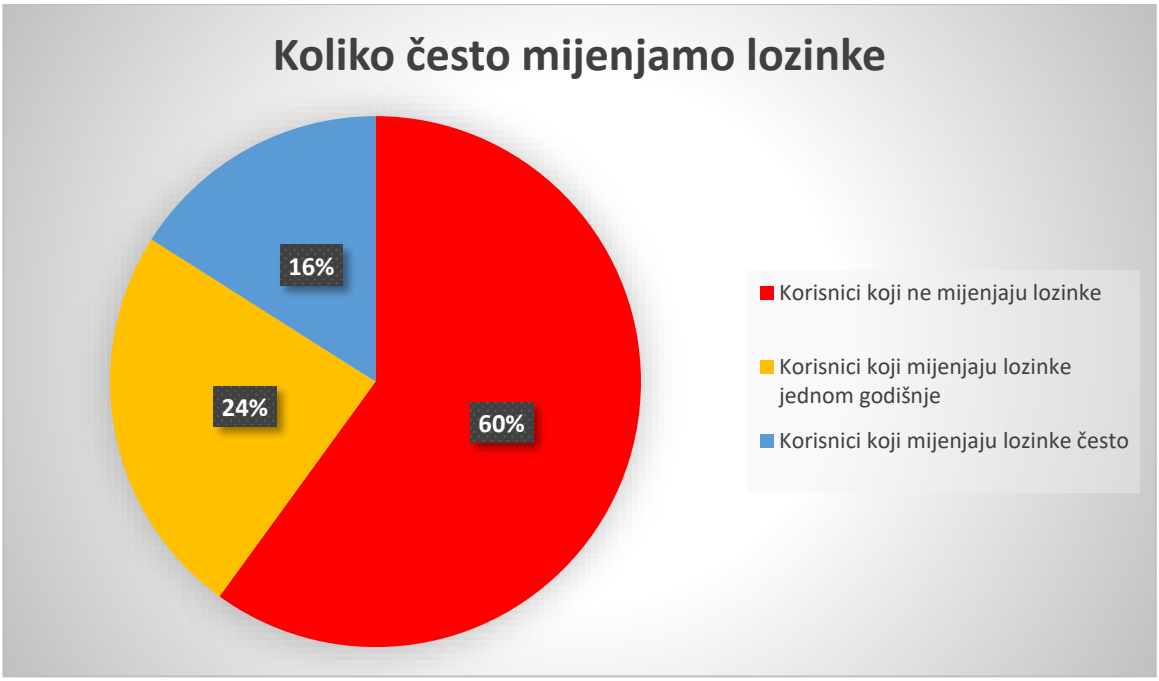
Hrvatska udruga banaka osnovana je u Zagrebu, 15. listopada 1999. godine. Hrvatska udruga banaka je stvorila kodeks bankovne prakse postavljajući standard poslovanja kojim promiče odgovornost i profesionalnost bankovne struke s ciljem uspješnijeg i sigurnosnog rada.

Udruga se sastoji od 19 vodećih banaka koje čine 97% ukupne aktive svih hrvatskih banaka.

Od uvođenja online usluga hrvatska udruga banaka je svojom predanošću i razvojem sigurnosnih trendova dosegnula vrlo visoku razinu zaštite sustava. HUB garantira vrlo visoku sigurnost svojih korisnika, no njihova najslabija karika upravo su sami korisnici koji su skloni prijevarama socijalnih inženjera.

Do takvog zaključka došli su provedbom anonimnih anketa koje su objavljene u lipnju 2016. godine.

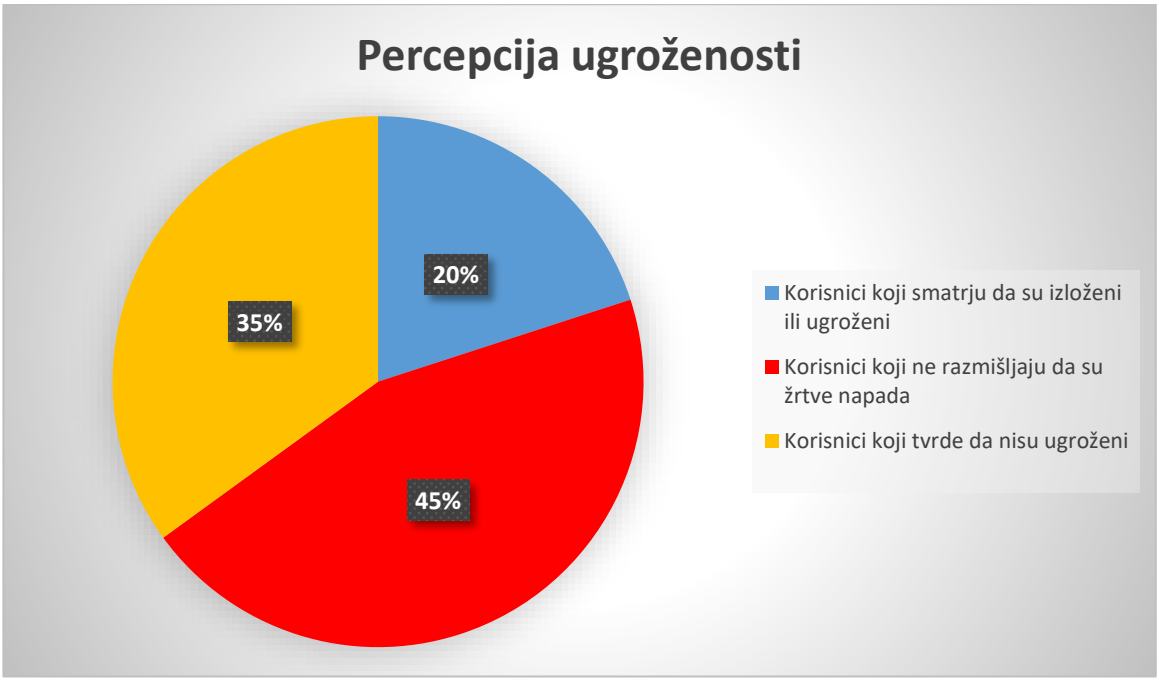
Grafikon 1: Koliko često mijenjamo lozinke




Izvor: http://www.sigurnostnainternetu.hr/images/preuzimanja/Infografika_-_Sigurnost_na_internetu_2016.pdf (25.8.2016./22:29)

Na tisuće ispitanika, istraživanje je pokazalo da 60% ispitanika ne ažurira svoju lozinku, dok 24 % mijenja jednom godišnje. Samo 16% ispitanika brine o svojoj sigurnosti korištenjem online bankovnih usluga.

Grafikon 2: Percepcija ugroženosti




Izvor: http://www.sigurnostnainternetu.hr/images/preuzimanja/Infografika_-_Sigurnost_na_internetu_2016.pdf (25.8.2016./22:44)

Ispitivanja su pokazala da je 20% korisnika stvorilo predodžbu da su izloženi ili ugroženi internetskim napadima. Njih 45% ne razmišlja da bi mogli biti žrtve prijevara dok preostalih 35% građana tvrdi da su sigurni.

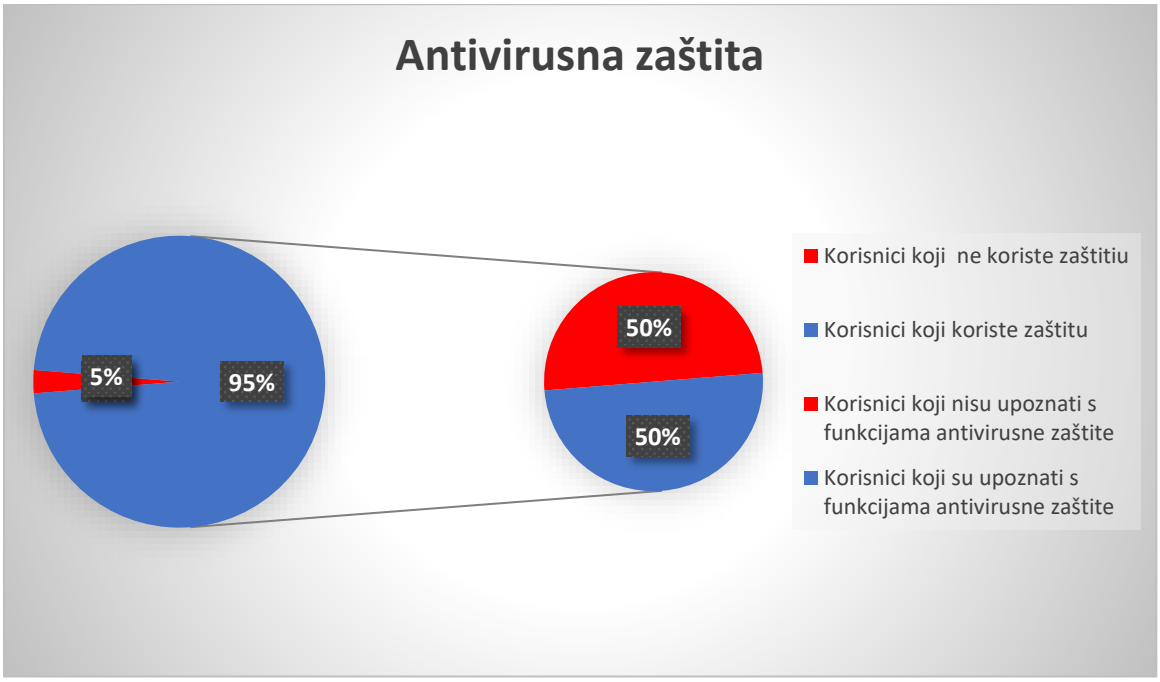
Također 43% ispitanika tvrdi da se nikada nisu susreli s pokušajima prijevara, 28% njih ništa ne poduzima povodom prijevare, 22% upozori svoje bližnje i 7% prijavi nadležnim institucijama.

U slučaju internetske prijevare 35% građana traži savjet prijatelja ili suradnika, 16% traži rješenje pretragom interneta dok preostali 16% konzultira se s IT stručnjacima ili na portalima.

Ovakve statistike su zabrinjavajuće i potrebno je educirati korisnike kako bi stvorila svijest o postojećim prijetnjama. 41% građana odnosno korisnika smatra da bismo se trebali više educirati o sigurnosti na internetu, 32% građana ne zna što bi mogli poduzeti da se

educiraju, 13% ih smatra da bi se edukacija trebala provoditi na radnom mjestu, 11% samostalno educiranje i samo 18% građana smatra da bi se edukacija trebala provoditi u školama.

Grafikon 3: Antivirusna zaštita




Izvor: http://www.sigurnostnainternetu.hr/images/preuzimanja/Infografika_-_Sigurnost_na_internetu_2016.pdf (25.8.2016./23:30)

Iako 95% građana ima antivirusnu zaštitu samo je polovica upućena čemu ona služi.

# 7. Zaključak

Informacijski sustavi ustanova suočeni su elementarnim rizicima koji mogu prouzročiti velike gubitke i štete, koje zbog svoje nepredvidljive prirode nije moguće u potpunosti izbjeći. Kad se ustanove suoče s takvim oblicima rizika važno je spriječiti i umanjiti štetu koje oni uzrokuju da se spasi gubitak informacije i omogući u što bržem roku kontinuitet poslovanja.

Dakako, ljudski faktor može djelovati izvana ili iznutra, a šteta može biti izazvana slučajna ili namjerno. Organizacija primjenom sigurnosne politike i educiranjem zaposlenika o pravilnicima rukovođenja informacijskih tehnologija može spriječiti ulazne incidente. Preporučljivo je da ustanove rotiraju obaveze zaposlenika te tako ostvaruju smanjenje i kontrolu neovlaštenih aktivnosti prijašnjih zaposlenika. Kod izlaznih incidenata preporučljivo je također educiranje ali i praćenje sigurnosnih trendova u prevenciji i prepoznavanju takvih napada.

Socijalni inženjeri raznim tehnikama zadobivaju povjerenja zaposlenih, koji ispunjavaju njihove zahtjeve s namjerom da izvuku povjerljive informacije i podatke koji nisu dostupni javnosti. Prevencijom takvih prevara, ustanove moraju tražiti od svojih zaposlenika potpuno ispunjenje i točnu izvedbu sigurnosne politike i pravilnika ophođenja s korisnicima, zaposlenicima, nadređenima i raznim oblicima podrške, kako bi se stvorio kodeks ponašanja i komunikacije, i tako uočile i spriječile sumnjive aktivnosti socijalnih inženjera.

Korisnici i zaposlenici moraju pristupati s oprezom ako se od njih traže osobne informacije preko telefona ili elektroničke pošte. Primjenom sigurnosne politike, kod korisnika i zaposlenika omogućuje da se drže protokola i da izbjegnu i prijave takve vrste napada. Korisnici moraju biti svjesni da su njihovi osobni podaci evidentirani kod poslužitelja usluga, te je svakako nepotrebno odavati detaljne osobne podatke putem raznih anketa.

Važno je imati višestruke zaporke, u slučaju ako napadač sazna zaporku da ne može pristupit svim računima korisnika, te ih je potrebno s vremenom ažurirati.

Poželjno je da korisnik proširi informacije ostalim korisnicima o opasnostima i tehnikama socijalnih inženjera. Njihove su aktivnosti jedino efektivne ako korisnici nisu upućeni u njih.

Svaki korisnik, zaposlenik i ustanova koja posjeduje računalni informacijski sustav mora imati instaliranu antivirusnu i vatrozidnu zaštitu i svakodnevno ih ažurirati radi prevencije zloćudnih programa.

Korisnici se mogu svakako pouzdati u antivirusnu zaštitu, ali ih antiviusna zaštita ne može u potpunosti zaštiti pri pristupanju nepouzdanih stranica i skidanja sadržaja koje takve stranice nude. Potrebno je mnogo vremena da antivirusni programi izrade sigurnosnu zakrpu za novonastale zloćudne programe tako da se od korisnika sustava očekuje da ne pristupa takvim stranicama. Od korisnika se također očekuje da izradi sigurnosnu kopiju podataka putem postavka operativnih sustava, poslužitelja koji nude takve usluge ili pohranu podataka na memorijske i optičke medije.

Iako spajanje na besplatnu javnu mrežu može biti primamljivo korisnicima moraju biti svjesni da dijele mrežu s ostalim osobama. Napadači putem aplikacija mogu presresti zaštitu usmjerivača ili pak glumiti da je njihovo računalo usmjerivač, te tako prikupljati sav vidljivi promet na mrežnom kanalu.

Vatrozid omogućuje zaštitu i regulaciju ulaznih i izlaznih veza i prepoznaje nove pristupne točke s kojim korisnik prvi put ostvaruje povezivanje. Tako mu nudi opciju da odabere prikladne postavke koje će mu omogućiti razinu sigurnosti takve mreže.

Mnogo stranice, pogotovo web stranice financijskih poslužitelja, imaju šifrirane stranice koje omogućuju zaštitu od napada koji posreduju u komunikaciji. Korištenje takvih stranica korisnici su sigurni jer napadači nemaju odgovarajući ključ kako bi mogli pristupiti web stranici korisnika i ukrasti informacije.

Internet bilježi sve više korisnika čiji broj eksplicitno raste. Problemi korisnika su njihova pasivnost i olako shvaćanje korištenja informacijske tehnologije. Ankete hrvatskih udruga banaka dokazuju upravo to. Informiranost građana o rizicima primjene informacijskih tehnologija je zabrinjavajuća. Kako se razvijaju tehnike zaštite i sigurnosti takao sukladno njima razvijaju se tehnike i alati koji ih zaobilaze. Educiranjem korisnika stvara se svjesnost i potreba za zaštitom, što može pridonijeti velikom značaju u informacijskoj sigurnosti i smanjenju svih oblika rizika informacijskih tehnologija kao u poslovanju tako i u privatnom životu.

Nikola Jakovac

Nikola Jakovac

Literatura:

Knjige:


1. Panian, Ž., Ćurko, K.: Poslovni informacijski sustavi, Element, Zagreb, 2010.
2. Pavlić M., Informacijski sustavi, Sveučilište u Rijeci, Zagreb 2011
3. Čerić V, Varga M., Informacijske tehnologije u poslovanju, Sveučilište u Zagrebu, Zagreb, 2014.
4. Panian Ž.: Poslovna informatika za ekonomiste, MASMEDIA Zagreb, 2005
5. Bosilj V., Pejić, M., Čerić V., Panian Ž., Požgaj Ž., Srića V., Varga M, Ćurko K., Spremić M., Strugar I., Jaković B.,Vlahović N., Poslovna informatika, Veleučilište u Zagrebu, Zagreb, 2009.
6. Medić G., Internet i rad na mreži, Učilište Algebra, Zagreb, 2008.
7. A. Conry-Murray, W. Weafer, Sigurnost na internetu, 2005.
8. Anić V., Veliki rječnik hrvatskog jezika, Zagreb, 2004.


Internet stranice:


1. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-06-124.pdf
2. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-09-133.pdf
3. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-02-107.pdf
4. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-172.pdf
5. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2007-12-213.pdf
6. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf
7. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf
8. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-10-280.pdf
9. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-292.pdf
10. http://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-026.pdf
11. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2014-01-340.pdf
12. http://www.cert.hr/malver/adware
13. http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf
14. http://www.infrahouse.com/da/blog/author/pia-pedersen/pdca-plan-do-check-act-cycle-simple-and-useful-continuous-improvement
15. https://perishablepress.com/paypal-phishing-spam/

16. https://www.paypal.com/signin?country.x=HR&locale.x=en_HR
17. http://hrcak.srce.hr/11861
18. https://www.facebook.com/security/
19. http://www.howtogeek.com/185354/security-questions-are-insecure-how-to-protect-your-accounts/

Popis tablica:

Tablica 1: Primjeri stvarne i lažne adrese…….13

Popis slika:

Slika 1: Osnovni model sustava……..2

Slika 2: Prikupljanje informacija u socijalnom inženjeringu……..8

Slika 3: Primjer javne objave Sigurnosne politike i pravila sigurnosnog i efikasnog korištenja Facebook stranice……...30

Slika 4: Osnovni elementi informacijske sigurnosti ISO 17799:2000……..36

Slika 5: Usporedba ISO 17799:2005 i ISO 17799: 2000 standarda…….38

Slika 6: PDCA model primijenjen na ISMS…….41

Popis grafikona:

Grafikon 1: Koliko često mijenjamo lozinke……42

Grafikon 2: Percepcija ugroženosti……...43

Grafikon 3: Antivirusna zaštita……44