ISSN 1864-6168

ZAŠTITA ELEKTRONIČKIH PODATAKA

Varga M.[1]
[1]Tehnička škola Čakovec, Čakovec, Hrvatska

Sažetak: *Cilj ovog rada je upoznavanje korisnika web servisa ili usluga s internetom, zaštitom podataka na internetu, zaštitom podataka od upada preko interneta i zaštitom podataka od upada u računalo fizičkim postupcima. Važno je istaknuti da će u radu osim teorijski objašnjenih opasnosti i načina zaštite podataka od zlonamjernih osoba biti prikazani i praktični primjeri, te alati za onemogućavanje upada u računalo (putem interneta ili fizički). Korisnici internetskih usluga naučit će kako zaštiti podatke pomoću pojedinih alata lozinkom i fizički. Kod zaštite podataka od upada s interneta bit će razrađene sigurnosne stijenke, kao što su stijenke koje filtriraju komunikacijske pakete, stijenke koje djeluju kao prividni poslužitelji, te stijenke koje djeluju kao stvarni poslužitelji. Najprikladnije istraživačke metode za ovu temu su: (1)istraživanje modeliranjem, (2)anketiranje korisnika internetskih usluga, (3)promatranje, (4)analiza.*

Ključne riječi: *internet, društvene mreže, antivirusni program, mobilna telefonija, fizička zaštita, kriptiranje, sigurnosni mehanizmi, zaštita transakcija, anketa.*

Abstract: *The aim of this paper is to inform Web services users or Internet users of data protection on the Internet, data protection from intrusion via the Internet and data protection from physical intrusion into the computer. It should be noted that besides the theoretically explained dangers and ways of protecting data from malicious persons the paper will present practical examples, as well as tools to prevent intrusions into your computer (via Internet or physically). Users of Internet services will be shown how to protect your data with a particular tool, password, and physical protection. For data protection from intrusion from the Internet, elaborate and detailed security wall (firewall) descriptions will be presented, such as walls that filter communication packages, the side walls that act as virtual servers, and walls that act as real servers. The most appropriate research methods for this subject matter are: (1) research modeling, (2) survey's online services, (3) observation, (4) analysis.*

Key words: *internet, social networks, antivirus software, mobile phones, physical protection, encryption, security mechanisms, protecting transactions, poll.*

1. UVOD

U današnje vrijeme kada je internet važan resurs u svim organizacijama potrebno je posvetiti određenu pozornost računalnoj sigurnosti i računalnim sigurnosnim mehanizmima. Pri tome vatrozid, brisanje povijesti pregledavanja, antivirusni programi, fizička zaštita, optimalne lozinke i kriptiranje imaju veliku ulogu jer štite računalni sustav od brojnih zlonamjernih korisnika interneta. Osim vatrozida, brisanja povijesti pregledavanja, antivirusnih programa, fizičke zaštite, optimalnih lozinka i kriptiranja u radu su prikazani i mnogi drugi sigurnosni mehanizmi, te preporuke za sigurno korištenje interneta. Zbog stalne prisutnosti na internetu, najviše su izloženi korisnici DSL veze, kabelskog interneta i stalnih veza, ali i ostali korisnici interneta nisu izvan opasnosti. Zaštita sigurnosnom stijenkom postoji u različitim oblicima, pa se zbog toga preporučuje odabir rješenje u skladu s potrebama. Korištene istraživačke metode za ovu temu su (1)istraživanje modeliranjem, (2)anketiranje korisnika internetskih usluga, (3)promatranje, (4)analiza. U većini slučajeva anketirani su korisnici interneta u dobi od 13 do 18 godina, od 19 do 29 godina, te stariji od 40 godina. Analiza rezultata ankete napravljena je u alatu za analitičku obradu podataka i prikazana je grafički 3D tortnim grafikonima. Za izračun rezultata ankete korištene su funkcije:
f_x=COUNTIF(B3:B200;"a,b,c,d"),f_x=COUNTIF(D3:D200;"a"),f_x=COUNTIF(R3:R200;"Microsoft SecurityEssentials"),f_x=COUNTIF(R3:R200;"NOD Eset"),f_x=COUNTIF(R3:R200;"AVGfree"), f_x=COUNTIF(D3:D200;"b") i mnoge druge.

2. ŠTO JE TO INTERNET?

Internet je globalni informacijsko-komunikacijski sustav koji povezuje računalne mreže pojedinih zemalja i organizacija, te omogućava posjednicima računala diljem svijeta da putem svojih lokalnih i

telefonskih mreža međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge.[3] Internet je danas jako široki pojam. Razvio se iz projekta američkog Ministarstva obrane pod nazivom Arpanet, kojeg su potkraj šezdesetih godina pokrenuli u SAD-u. U početku je bilo zamišljeno da mreža Arpanet nudi svojim korisnicima samo jedan jedini poslužitelj, a to je onaj za pokretanje programa na udaljenim računalima. Nedugo nakon puštanja mreže u rad dodana su još dva poslužitelja, te je bilo moguće prebacivati datoteke s jednog računala na drugo i mogle su se slati poruke s jednog računala na drugo putem elektroničke pošte. Razvojem Arpaneta u internet tijekom godina popularizacije interneta, poslužitelji i računala su se prilično nagomilali.

Internet je računalna mreža svih manjih računalnih mreža. Za internet možemo reći da je širokopojasna rasprostranjena mreža koja povezuje računala svih veličina. Internetom mogu biti povezani serveri ili poslužitelji, lokalna računala, stolna i prijenosna računala, mobilni uređaji, te dijelovi mreže kao što su DSL modem, kabelski modem, usmjernik, preklopnik itd. Internetom se povezuje sve više netradicionalnih krajnjih sustava kao što su televizijski uređaji, uređaji u automobilima, okviri za slike, kućni elektronski i sigurnosni sustavi, web kamere itd.[6]

Stariji uređaji kojima se pristupa internetu su analogni modem brzine 56 kbps, koji se danas gotovo ne koristi, i ISDN adapter koji ima brzinu prijenosa podataka 128 kbps, tj. 64 kbps po kanalu, a sadrži dva kanala.

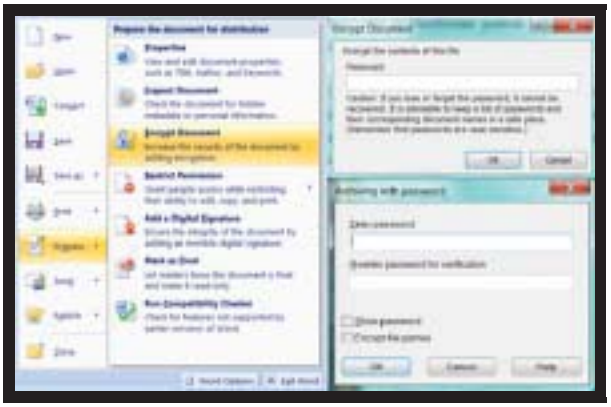
3. ZAŠTITA PODATAKA

Zaštita podataka se provodi kako bi se spriječila krađa podataka ili nedopušteno manipuliranje podacima. Postoje dva razloga zbog kojih se štite elektronički podaci: (1)zbog mogućnosti gubitka i (2)od neovlaštenog korištenja nepouzdane osobe koja ima zlonamjerne ciljeve. U različitim organizacijama za sprječavanje gubitka podataka podaci se pohranjuju na različite medije koji također imaju određenu zaštitu od brisanja. Na uređajima za pohranu podaci se mogu uništiti samo fizički ukoliko su zaštićeni od brisanja.

Način i provedba zaštite klasificiranih i neklasificiranih podataka propisani su zakonom koji regulira područje informacijske sigurnosti. Kada govorimo o zaštiti podataka, potrebno je naglasiti da se dužnosnici i zaposlenici određenih ustanova moraju držati zakona o tajnosti podataka koji glasi:

Dužnosnici i zaposlenici državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravnih osoba s javnim ovlastima, kao i pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima, dužni su čuvati tajnost klasificiranog podatka za vrijeme i nakon prestanka obavljanja dužnosti ili službe, sve dok je podatak utvrđen jednim od stupnjeva tajnosti ili dok se odlukom vlasnika podatka ne oslobode obveze čuvanja tajnosti.[10] Ako se klasificirani podatak uništi, otuđi ili učini dostupnim neovlaštenim osobama, vlasnik podatka poduzima sve da otkloni moguće štetne posljedice, pokreće postupak za utvrđivanje odgovornosti i istodobno izvještava Ured Vijeća za nacionalnu sigurnost.[10] Ako se klasificirani podatak uništi, otuđi ili učini dostupnim neovlaštenim osobama u tijelu koje nije vlasnik podatka, odgovorna osoba tog tijela dužna je odmah o tome izvijestiti vlasnika podatka koji pokreće postupak iz stavka 1. ovoga članka.[10]

Ukoliko se govori o elektroničkoj zaštiti podataka na dokumentima, dokument se može zaštititi postavljanjem lozinke, standardiziranim davanjem imena mapama i imena dokumentima unutar mapa, te pravilnom organizacijom dokumenata u mapama.



Slika 1. Enkripcija dokumenata

Slika 1. prikazuje postupak enkripcije word dokumenata. Svi alati za obradu teksta u dokumentima trebali bi imati mogućnost enkripcije zbog zaštite podataka koje dokument sadrži. Enkripcija dokumenata može se učiniti i pomoću programa za enkripciju kao što su WinZIP i WinRAR. Kada je riječ o prijenosu dokumenata koji se stavljaju kao privitci putem internetske usluge elektroničke pošte, najbolje bi bilo da se primatelju dokument spremi u formatu koji je uobičajen, da bi ga primatelj lakše čitao. Korištenje standardnih formata zapisa omogućuje lakšu razmjenu dokumenata, a zatim i podataka s primateljima, te lakše čitanje dokumenata pomoću različitih programa. Podaci od gubitka mogu se zaštititi učestalim stvaranjem sigurnosne kopije podataka.

3.1. Zaštita podataka na internetu

Sve učestalije korištenje podataka s interneta potaknulo je pitanje zaštite baze podataka i njihovih sadržaja, odnosno prava njihovih autora. Internet je donio mogućnost prikupljanja velike količine podataka iz različitih područja ljudske djelatnosti, kao što su pravo, sport, ekonomija, informatika, promet,

kultura, graditeljstvo, školstvo itd. Internet je doveo do uspostavljanja nevidljivog nadzora pomoću uređaja sposobnih da presreću prijenos svih podataka u komunikaciji. Za presretanje podataka putem interneta nije dovoljno biti spojen na računalnu mrežu, već je potrebno imati odgovarajući alat kojim će se moći vidjeti paketi koji se prenose određenim komunikacijskim kanalom, od pošiljatelja prema primatelju.

3.1.1. Stavljanje podataka na NET

Prije stavljanja podataka na internetske servise treba dobro promisliti. Jednom stavljeni podaci na internet ostaju zauvijek na internetu. Podaci koji se prenesu na udaljeno računalo, tj. na server, oni zauvijek ostaju kod vlasnika servera. Danas postoje servisi na internetu koji vraćaju podatke koji su bili objavljeni na nekim stranicama prije više od 10 godina. Primjer takvog arhivskog servisa za vraćanje podataka je Waybackmachine. Waybackmachine može vratiti sve podatke koji su bili objavljeni na službenim web stranicama, npr. Filozofskog fakulteta iz Zagreba (slika 2.) prije 12 i više godina, te se može „surfati“ po web stranicama fakulteta.

Slika 2. Stranica Filozofskog fakulteta od 21. veljače 1999. godine

Slika 2. prikazuje stranicu Filozofskog fakulteta od 21. veljače 1999. godine. Stranica je pronađena pomoću web alata Waybackmachine i na njoj se mogu naći podaci koji su bili tada na toj web stranici. Waybackmachine omogućuje izradu prikaza, kako se neki internetski portal razvijao kroz povijest, te koje su tehnologije korištene za izradu web stranica. Osim Waybackmachinea postoje i druge internetske arhive koje sadrže manje podataka i web stranica. Waybackmachine je internetska arhiva koja omogućuje da se za unesenu adresu web stranice prikažu povijesni podaci koji su bili objavljeni na njoj. Sve što se nalazilo i nalazi se na internetu bit će zauvijek zapamćeno, zato ne smijemo stavljati osjetljive podatke na internet.

3.1.2. Društvene mreže

Danas je najpopularniji internetski servis Facebook, pogotovo kod mlađeg uzrasta u dobi od 13 do 18 godina, što je jedan od razloga zašto su anketirane osobe u toj dobi. Razlog zbog čega je Facebook popularan je želja da korisnici saznaju što više o prijateljima, poznanicima i drugim javnim osobama koje su korisnici tog servisa, a upravo to im omogućava Facebook. Preko Facebooka dogovaraju se sastanci, prosvjedi, skupovi, promoviraju se koncertni događaji itd. Društvene mreže se danas sve više koriste za oglašavanje. Korištenje društvenih mreža ponekad može biti opasno. Pet opasnosti društvene mreže Facebook koje navodi Joan Goodchild su:

- podaci korisnika se dijele trećim stranama
- postavke o privatnosti vratit će se na početne nakon svakog redizajna sustava
- Facebook oglasi mogu sadržavati zlonamjerni software
- Vaši prijatelji nesvjesno vas mogu učiniti ranjivim
- Spameri mogu kreirati lažne profile [5]

Osim spomenutih opasnosti Joana Goodchilda potencijalna opasnost su i neodgovorni zaposlenici unutar Facebooka. Facebook je otkrio nekoliko svojih zaposlenika koji su prodavali imena korisnika i njihove popise kontakata kako bi zaradili novac. [5] Zaposlenici su podatke prodavali raznim tvrtkama koje bi na taj način promovirale sebe, svoje proizvode i usluge na Facebooku.

Slika 3. Stranica Facebooka

Slika 3. prikazuje stranicu Facebooka te mogućnost organiziranja raznih događaja na web servisima. Društvene mreže trebale bi se iskoristiti za razmjenu dobronamjernih ideja, za rješavanje problema, razmjenu znanja i informacija, za jednostavan pristup resursima, za stjecanje novih poznanstava i poslovnih kontakta, za osnivanje novih udruga i tvrtki, stupanje u kontakt sa starim prijateljima itd. Danas Facebook nastoji uvesti mogućnost koja će trajno brisati sve podatke o osobi koja je imala profil na istoimenom servisu i to trajno, što je nezamislivo, a IT stručnjaci za sigurnost i zaštitu podataka sumnjaju u to.

3.1.3. Brisanje povijesti pregledavanja

Kada se pregledava web, internet preglednik pohranjuje informacije o web mjestima koja se posjećuju i podacima koji su uneseni preko web preglednika (npr. naše ime i adresu). Internet preglednik pohranjuje sljedeće vrste podataka: privremene internetske datoteke, kolačiće, povijest

web mjesta koja smo posjetili, podatke koje smo unosili na web stranicama ili u adresnu traku, te pohranjene web lozinke. Ponekad je korisno povijesne podatke imati na računalu jer se tako web može pregledavati većom brzinom. Također, informacije koje se često unose ne moraju biti iznova unesene. Podaci se trebaju brisati ako se npr. koristi javno računalo na kojem se ne žele ostaviti osobni podaci. Povijest pregledavanja i dopisivanja može se brisati tako da se izbrišu podaci unatrag dva tjedna, jedan mjesec, tri mjeseca i svi podaci koji su zabilježeni u povijesti.

Slika 4. Postupak brisanja povijesti

Slika 4. prikazuje način brisanja povijesti podataka o dopisivanju sugovornika na Skypu i način brisanja povijesti pregledavanja internetskih stranica u internetskom pregledniku IE8. Poželjno je da korisnik briše povijest pregledavanja u internetskim preglednicima nakon pregledavanja, kako sljedeći korisnik istog računala ne bi mogao zloupotrijebiti podatke o pretraživanju i pregledavanju stranica osobe koja je prethodno koristila računalo.

3.2. Zaštita podataka od upada s interneta

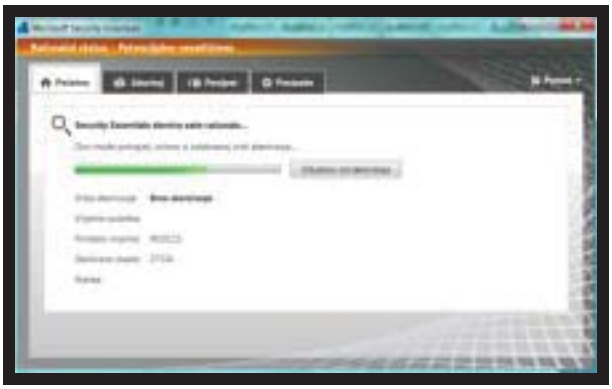
Podatke od upada s interneta možemo zaštititi antivirusnim programima, stijenkama koje filtriraju komunikacijske pakete (eng. Packet filter), stijenkama koje djeluju kao prividni poslužitelji (eng. Proxy server), te stijenkama koje djeluju kao stvarni poslužitelji (eng. Full server).

3.2.1. Antivirusni programi

Antivirusni programi štite operacijski sustav računala i samo računalo od zlonamjernih programa virusa. Neki od poznatijih antivirusnih programa su Microsoft Security Essentials, ESET NOD 32 Antivirus 4, ESET Smart Security 4, ESET Mobile antivirus (antivirus namijenjen korisnicima mobilnih uređaja), AVG, McAffee, Norton antivirus (Symantec) i mnogi drugi.

Virusi su mali programi koji su napravljeni tako da se mogu ugraditi u datoteke koje sadrže druge veće programe. Nakon što se pokrenu takvi programi, aktivirat će se računalni virus koji će izazvati štetu. [7] Računalni virusi su najčešća i najopasnija vrsta od svih malicioznih računalnih programa. S obzirom na brzinu širenja i brojnost, uvelike će obilježiti budućnost razvoja interneta i usluga koje on pruža, te će sigurno biti glavni problem korisnicima i administratorima informacijskih sustava. [1]

Prije korištenja operacijskog sustava računala poželjno je ažurirati antivirusni program kako bi zadobio nove datoteke. Viruse sastavljaju zlonamjerne osobe koje nemaju ništa „pametno“ raditi. Takvi ljudi se trude nanijeti štetu korisnicima računala, proizvođačima programa i operacijskih sustava. Oni nastoje dokazati kako proizvođači računalnog programa nisu izradili aplikaciju na odgovarajući način sa zaštitnim i sigurnosnim mehanizmima, te da antivirusni programi ne pružaju dovoljnu zaštitu. Zlonamjerne osobe koje razvijaju viruse nemaju prevelike koristi od proizvodnje virusa.



Slika 5. Skeniranje diska antivirusnim programom

Slika 5. prikazuje skeniranje diska antivirusnim programom kako bi se utvrdilo postoje li neželjene datoteke na njemu. Računalni status je potencijalno nezaštićen, što se vidi iz gornje slike. Da bi se zaštitio sustav, u ovom slučaju potrebno je ažurirati antivirusni program.

3.2.2. Sigurnosna stijenka

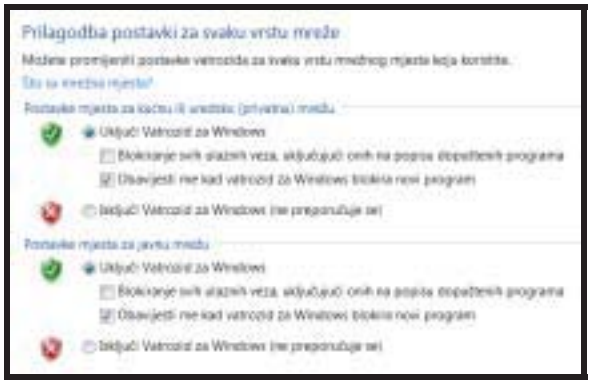
Sigurnosna stijenka je kombinacija softvera i hardvera koja izolira unutarnju mrežu organizacije od interneta, dopuštajući nekim paketima da prođu blokirajući ostale. Sigurnosna stijenka dopušta administratoru da kontrolira pristup resursa unutar mreže upravljanjem tijekom prometa prema resursima i od tih resursa.[6] Stijenka se može postaviti između interneta i intraneta, između intraneta i ekstraneta te između interneta i ekstraneta. [2] Sigurnosna zaštitna stijenka je računalo ili neka druga komunikacijska nakupina koja fizički razdvaja dvije mreže. Sigurnosna stijenka ograničava pristup nekoj privatnoj lokalnoj mreži. Drugo ime koje se najčešće upotrebljava za ovaj naziv je vatrozid. Vatrozid je softver ili hardver kojim se provjeravaju podaci pristigli putem interneta ili mreže, a zatim ih, ovisno o postavkama, odbacuju ili propuštaju do računala. Vatrozid može poboljšati zaštitu računala od hakera ili zlonamjernih programa (kao što su *crvi*),

koji se pokušavaju pohraniti u računalu putem mreže ili interneta. Vatrozid može spriječiti računalo da drugim računalima pošalje zlonamjerne programe. Po svom načinu djelovanja, stijenke se mogu podijeliti u tri skupine:

- stijenke koje filtriraju komunikacijske pakete (eng. Packet filter)
- stijenke koje djeluju kao prividni poslužitelj (eng. Proxy server)
- stijenke djeluju kao stvarni poslužitelj (eng. Full server)

Filtarske sigurnosne stijenke djeluju na nižim razinama komunikacijskih protokola i obavljaju funkciju na temelju podataka koje nalaze u komunikacijskim paketima. Na temelju podataka kao što su npr. adresa pošiljatelja, adresa primatelja i smjer kretanja paketa, stijenka može neke podatke propuštati, a neke blokirati. Takve se stijenke nazivaju blokirajuće stijenke. Sigurnosne stijenke koje djeluju kao proxy server prihvaćaju zahtjeve za obavljanje usluga, obave sigurnosnu provjeru, te također prosljeđuju zahtjeve za obavljanje te usluge stvarnom zaštićenom poslužitelju. Stvarni poslužitelji ne dopuštaju kontakt vanjskih klijenata i unutarnjih poslužitelja.

Danas mnogi mrežni prolazi nude opcije sigurnosne stijenke koje dopuštaju filtriranje određene vrste prometa, npr. onog koji je usmjeren prema određenom internet servisu. Neki mrežni prolazi mogu filtrirati promet u oba smjera. Mnogi su jednostavniji i omogućuju samo blokiranje onog prometa koji nije odgovor na zahtjev poslanog putem nekog internet servisa kao što je FTP.[4] Napredni tipovi zaštitnih stijenki uočavaju specifične uzorke podataka. Kada prepoznaju napad blokiraju pristup IP adresi s koje napad stiže, te obavješćuju korisnika o tome.



Slika 6. Mogućnosti uključivanja vatrozida za Windows 7 operacijski sustav

Slika 6. prikazuje mogućnosti uključivanja vatrozida za Windows 7 operacijski sustav. Uključeni vatrozid može blokirati sve ulazne veze, uključujući i one koje se nalaze na popisu dopuštenih programa. Računalni sustav može prikazivati obavijesti kada Windows 7 blokira novi program. Vatrozid u Windows 7 operacijskom sustavu može biti isključen kao što se vidi iz slike. U današnje vrijeme nisu rijetki napadi na vatrozid. Postoji napad na vatrozid koji se odmah isključi ako prepozna korisničko računalo i onemogući korisniku računala da pristupi internetu. Takva vrsta napada naziva se System Event Notification Service napad i može u određenom trenutku izazvati veliku neugodnost. Ona se pojavljuje u Windows Vista operacijskom sustavu i Windows 7. Da bi se računalo ponovno spojilo na internet kod Windows 7 ili Windows Viste operacijskog sustava, moramo napraviti sljedeće:
Pokrenuti opciju -> start -> svi programi -> pomagala -> naredbeni redak ->
cd.. -> cd.. -> cd windows -> cd system32 -> netsh -> winsock reset .

3.2.3. Mobilni uređaji korisnika

Mobilna telefonija se u posljednjih dvadeset godina brzo razvila. Mobilni uređaji postaju sve manji, lakši, s puno više mogućnosti i s različitim tehnologijama prijenosa podataka. Mobilni uređaji danas koriste digitalnu tehnologiju. Mobilna tehnologija se razvijala brzo i još se razvija (1)zbog profita i (2)kako bi pogodovala poslovnim ljudima koji često putuju. Danas se manje-više svi mobilni uređaji mogu povezati s računalom, prijenosnim računalom, pa čak i telefaks uređajima.

Neki pružatelji mobilnih usluga nude šifrirane opcije koje omogućavaju potpuno privatne prijenose glasa i podataka. Nedostatak sigurnog kanala prijenosa uništava povjerenje u telefonsku konverzaciju. Neki pružatelji mobilnih usluga nude bežične kartice za povezivanje koje služe kao zamjena za modem na prijenosnim računalima. Spomenuti pojam je poznat kao Wi-Fi. Kartica za povezivanje olakšava povezivanje na internet kroz uslugu poslužitelja mobilne mreže. Jedanput kada se uspostavi veza, korisnici mogu raditi sve što je potrebno na svojim računalima, kao što bi radili u uredima na uredskim računalima.[8]
Međutim, ovdje postoje problemi. Neki mobilni uređaji nemaju sigurnosnu stijenku, tako da može doći do krađe podataka ili stvaranja dodanih troškova na računu korisnika mobitela ili tvrtke. Neki mobilni uređaji nemaju zaštitu od virusa, pa im virusi mogu jako naštetiti. Mobilni uređaji koji nemaju zaštitu od virusa mogu se zaštititi isključivanjem pristupa internetu ili dodatnom instalacijom antivirusnog programa. Povećanjem usluga mobilnih uređaja i standardizacijom povećao se rizik od napada i zloupotrebe podatka s mobilnog uređaja. Danas se izrađuju antivirusni programi namijenjeni zaštiti mobilnih uređaja koji pružaju zaštitu od virusa, trojanaca, crva i drugih poznatih virusa.

3.3. Zaštita podataka fizičkim postupcima

Osnova fizičke sigurnosti je zaštita medija za pohranu podataka i komunikacijske opreme. Fizička sigurnost obuhvaća sve obrambene mjere

kojima je svrha zaštita računalne infrastrukture i podataka. Fizička sigurnost važan je dio svake obrane računalne infrastrukture i podataka. Kod istraživanja računalnog kriminaliteta treba misliti o sljedećem: ako je kriminalna aktivnost počinjena u računalnom centru, bez probijanja ulaznih lozinki izvana, znači da je bila ugrožena fizička sigurnost ili da su probijene mjere zaštite fizički ili da ih uopće nije bilo. Nužno je točno utvrditi na koji način je probijena fizička sigurnost računalnog okružja. Ako je počinitelj zaobišao tehnički sofisticirane sustave zaštite, onda je nužno potražiti pomoć eksperata za određeno područje.[1] Ukoliko se snažno fizički oštete računala i medij za pohranu podataka velika je vjerojatnost da će se izgubiti i podaci na mediju. U današnje vrijeme u većini slučajeva podaci i programi su znatno veće vrijednosti nego sama računala (tj. infrastruktura).

3.3.1. Fizička zaštita

Fizička zaštita obuhvaća skup metoda i sredstava koji se koriste zbog zaštite materijalne osnovice ili hardvera informacijskog sustava od neovlaštenog fizičkog pristupa samom sustavu i korištenja njegovih resursa, te njegovu zaštitu od vanjskih događaja koji se ne mogu predvidjeti [3]. To su zaštita od udara groma, od prekida rada zbog nestanka električne energije, zaštita od poplave, potresa, od prevelike prašine, eksplozivnih naprava, zaštita od krađe računala itd. Kod zaštite miševa i ostalih ulaznih i izlaznih naprava od krađe koriste se sigurnosni sustavi, tzv. *kensington lock*. Nakon što zlonamjerna osoba želi otuđiti ulaznu napravu, npr. miš, ona to ne može jer je miš pričvršćen za prijenosno računalo *kensington lock* sustavom. Kako bi se zaštitili podaci u prijenosnim računalima i sama računala, potrebno je pobrinuti se o tome gdje ostavljamo računala. Preporuka je da se prijenosno računalo ne ostavlja na javnim mjestima, učionicama, kabinetima i drugim mjestima gdje je svima dostupno, pogotovo kada ta mjesta nisu zaključana. Danas postoje držači koji zaključavaju prijenosna računala na način da ih zlonamjerna osoba ne može otvoriti niti ih može pomaknuti s mjesta, te posebni ormarići izrađeni od čvrstog materijala u koje se pospremaju prijenosna računala tako da ih nitko osim ovlaštenih osoba ne može otvoriti.

U današnje vrijeme razvijeni su sustavi kojima je cilj povećati razinu fizičke sigurnosti, a to su nadzorne kamere, posebni sustavi za zaključavanje, alarmni sustavi, sustavi za praćenje lokacije (RFID) itd.

3.3.2. Optimalne lozinke

U tvrtkama je organiziran pristup korisnika određenim aplikacijama. Rukovoditelj odjela u koji dolazi novi zaposlenik šalje molbu za otvaranjem korisničkog računa s podacima o razini i pravima pristupa. Pored ostalih osnovnih podataka, molba treba sadržavati i naziv radnog mjesta, opis rada i potrebna prava pristupa. Nakon što korisnik dobije lozinku od rukovoditelja odjela, može je promijeniti tako da on i administrator mogu pristupiti određenim podacima. Svaki zaposlenik mora imati lozinku da bi imao pristup određenom dijelu aplikacije, tj. određenom modulu. Lozinka se mijenja obično svakih mjesec dana, a po potrebi bi se trebala i više puta mjesečno. Optimalna lozinka bi trebala imati minimalno sedam znakova. Za lozinku bi bilo poželjno da sadrži kombinaciju velikih i malih slova, te brojeve. Nikako se ne preporuča za lozinku koristiti osobna imena, prezimena, imena roditelja, djece, datum rođenja, naziv mjesta boravišta, naziv ulice i sl. Za lozinku nije dobro koristiti skup istih znakova. Promjena lozinke na UNIX operacijskom sustavu obavlja se tako da korisnik unosi naredbu *password* na početak naredbenog retka UNIX operacijskog sustava. Nakon što se ta naredba pokrene, korisnik mora prvo unijeti postojeću lozinku, a nakon toga dva puta novu lozinku, što je vidljivo iz primjera:

barok> password
Changing password for mavarga.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
barok>

Nakon što se unese nova lozinka, ona se mora još jedanput ponoviti kako bi bila pravovaljana i da bi se mogla dalje koristiti. U slučaju da korisnik zaboravi novu lozinku, jedina osoba koja može promijeniti lozinku i ima ovlaštenje za to je administrator. Ako je riječ o uredskom poslovanju, zbog sigurnosti se lozinka ne smije zapisivati na papir i stavljati u ladicu da treća osoba ne dođe do tajnih podataka. Najčešći napad na lozinke je ispitivanje ili pogađanje lozinki. Ispitivanje ili pogađanje lozinki napad je u kojem počinitelj pokušava pristupiti određenom sustavu nasumičnim pogađanjem lozinke, pri čemu se u većini slučajeva koristi metoda pokušaja i pogreške. Iako ovaj napad izgleda malo naivan ponekad može biti učinkovit, pogotovo kada jako dobro poznajemo osobu koja je postavila lozinku. Drugi najčešći napad na lozinke je tzv. Phishing. Korisnik korisničkog računa od napadača dobiva neželjeni mail u kojem se traži dostavljanje korisničkog imena i lozinke korisnika u sljedećih nekoliko dana, te piše: „ukoliko se ne pošalje korisničko ime i lozinka možete trajno izgubiti account“. Primatelj takve elektroničke pošte misli da mu je mail poslao internet poslužitelj koji daje samu uslugu korisniku. Napadač koristi naziv ISP pružatelja internet usluga tako da pošta bude uvjerljivija. Preporuka je da se ne nasjeda na takve mailove te da se ne šalju osobni korisnički podaci kao odgovor na njih. Pružatelj internet usluga može sam promijeniti lozinku i ne treba mu vaša stara lozinka. Kada dobijete elektroničkom poštom mail

To spriječiti

račun od zatvaranja, morat ćete
ažurirati u nastavku kako
biste znati da je status
kao trenutno koristi račun.
POTVRDIO svoju adresu e IDENTITET NIŽE
E-mail Korisničko ime:
Email Lozinka:
Upozorenje! Svaki račun vlasnika koji odbija
ažurirati svoj
korisnički račun u roku od
Tri dana ovog ažuriranja obavijest će
izgubiti njegov / njen
račun
trajno.
Hvala Vam

nemojte nasjesti, samo se zapitajte biste li zaista slali nekome osjetljive detalje korisničkog računa samo zato jer vas je „napadač“ lijepo zamolio.

Anti-Phishing zaštitu ima npr. programski alat Mozilla Thunderbird. To je besplatan program za zaštitu korisnika od Phishing napada. Phishing napad može biti poslan bilo kome. E-mail računi zaposlenika u bankama su također vrlo često meta napadača. Osim Phishing prijevara elektroničkom poštom, one mogu biti i prijevare aukcijskom prodajom te putem lažnih web mjesta. Phishing napad je vrlo ozbiljan i težak napad na korisnika interneta pogotovo ako korisnik ima teže financijske posljedice napada. Podaci o Phishing prijevarama koje su otkrivene nalaze se na internetskim stranicama kao npr. na web mjestu s adresom: http://www.antiphishing.org/phishing_archive.htm.

Phishing prijevare se učestalo prate kako bi korisnici interneta bili sigurniji. Phishing prijevara može biti u obliku lažne dobrotvorne akcije. Ova vrsta prijevare zahtijeva od korisnika internetskih usluga da uplati novčanu donaciju na račun zlonamjerne osobe. U takvom slučaju zlonamjerne osobe žele iskoristiti vašu darežljivost. U Phishing prijevaru možemo svrstati lažne web stranice koje su jako slične pravim web stranicama. Kada posjetimo takve web stranice računalo u većini slučajeva velikom brzinom preuzme zlonamjerni softver koji snima lozinku prilikom prijave na internetske račune.

Uobičajeni slučaj Phishing prijevare elektroničkom poštom je kada poruka počinje s „dragi kupci“ ili „dragi korisniče“, umjesto s našim imenom i prezimenom ili korisničkim imenom. To bi trebao biti dovoljan razlog da nas potakne na razmišljanje i duboko proučavanje poruke ili treba poruku jednostavno obrisati.

3.4. Kriptiranje

Kada govorimo o kriptografiji općenito mislimo na zaštitu podataka pomoću matematičkih postupaka ili algoritama i kriptografskih ključeva.[13] Skrivanje i enkripcija predstavljaju drugi način ograničavanja pristupa povjerljivim podacima. Enkripcija je posebno važna kada se podaci šalju računalnom mrežom. Tehnike ili pravila enkripcije određuju koliko će biti složen proces transformacije.[1] Digitalni potpis znači skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta.[2] Digitalni potpis se koristi za provjeru identiteta pošiljatelja informacija i osiguranje da informacija nije bila promijenjena nakon potpisivanja. Digitalni potpis se stvara tako [2] da se izračuna sažetak poruke korištenjem javno poznatog algoritma koji garantira da se isti sažetak ne može dobiti ni iz jedne druge poruke. Nastali sažetak kriptira se tajnim ključem pošiljatelja, nakon toga se dodaje poruci kao jedinstveni potpis te poruke od toga pošiljatelja. Navedena poruka se cijela s potpisom kriptira tajnim ključem pošiljatelja i šalje primatelju. Primatelj dekriptira poruku koristeći javni ključ pošiljatelja, nakon toga dobiva sadržaj poruke s potpisom. Na temelju sadržaja poruke primatelj generira sažetak poruke i uspoređuje ju s potpisom koji je došao uz poruku. Potencijalni sudionici u komunikaciji moraju na neki način doznati javne ključeve svojih partnera s kojima komuniciraju. Osim toga, oni se moraju uvjeriti da partneri nisu sudionici koji se lažno predstavljaju. U nekim zatvorenim sustavima svi se potencijalni sudionici moraju prijaviti i tada im se dodjeljuje par ključeva. Svoj privatni ključ oni čuvaju kod sebe, a njihov se javni ključ pohranjuje zajedno s njihovim identifikatorom u tablicama pouzdanog poslužitelja kojeg možemo nazvati menedžerom za raspodjelu javnih ključeva, skraćeno MJK (menadžer javnih ključeva). Kada sudionik A želi uspostaviti vezu sa sudionikom B sigurnim kanalom, on će zatražiti od MJK njegov javni ključ. Postoje modeli protokola za otkrivanje javnih ključeva, te protokoli za jednostranu ili dvostranu autentifikaciju uz pomoć MJK. Tablica u MJK koja identifikatorima pridružuje pripadne javne ključeve naziva se javnom datotekom. Ovo je rješenje prikladno za manje zatvorene sredine kao što su banke. Ako se u komunikaciju želi uključiti sudionik iz različitog okruženja i želi uspostaviti sigurno komuniciranje u širim razmjerima, onda jedan jedini centar za raspodjelu ključeva nije dobro rješenje određenog problema. Kako bi se otklonile poteškoće zatvorenog sustava, predlaže se koncept digitalnog certifikata. Svaki sudionik S se prijavljuje u jedan certifikacijsko-autorizacijski centar, pri čemu mu se dodjeljuje javni ključ K_{ES} i privatni ključ K_{DS}. Certifikacijski centar C također ima svoj javni ključ K_{EC} i privatni ključ K_{DC}. U postupku prijave certifikacijski centar izrađuje i potpisuje certifikat sudionika: $CERT^{S}c= (SD_S , K_{ES} , E (H(SD_S , K_{ES}), K_{DC}))$, gdje je H neka funkcija sažimanja, a E neka funkcija kriptiranja. Prikazani model certifikata sastoji se od para S_{DS}-K_{ES} i digitalnog potpisa kojim certifikacijski centar C garantira da javni ključ K_{ES} pripada sudioniku S. Certifikat povezuje javni ključ

sudionika s njegovim imenom. Istinitost te veze može se provjeriti na temelju digitalnog potpisa, ali je potrebno poznavati javni ključ K_{EC} određenog certifikacijskog centra. U certifikacijskom centru C čuva se tablica certifikata svih sudionika koji su u njemu prijavljeni i čiji je identitet prilikom prijave bio utvrđen. Poznatiji alati za enkripciju diskova i stvaranje virtualnih diskova su TrueCrypt, PGP, GnuPG i mnogi drugi.

3.5. Zaštita transakcija

Zaštita transakcija na internetu nužna je kako bi se korisnici stimulirali za kupovanje preko interneta. Osnovni zahtjevi za zaštitu transakcija su: privatnost predstavlja zaštitu prenošenih podataka od neovlaštenog čitanja, identifikacija korisnika predstavlja zaštitu od krivog predstavljanja korisnika, integritet transakcija označava da sadržaj poruka mora ostati neizmijenjen tijekom prijenosa kroz mrežu, nemogućnost osporavanja osigurava da pošiljalac poruke ne može osporiti da je poslao određenu poruku. Mehanizmi koji jamče sigurnost transakcija su, osim kriptiranja, digitalni potpis i digitalni certifikat.[2] Najčešća kupovina i plaćanje koje se odvija putem interneta je kupnja tzv. avionskih karata. Poznato je da se isplati kupiti avionsku kartu putem interneta nekoliko mjeseci prije samog putovanja, te da je takav način plaćanja najpraktičniji za osobe mlađe i srednje dobi. Kupovanje i korištenje e-karte je vrlo jednostavno i u potpunosti sigurno. Danas većina zrakoplovnih kompanija u svojoj ponudi nudi e-karte. E-karta ima brojne pogodnosti uz minimalni rizik. Ne može se izgubiti budući da se ona sastoji od broja potvrde i fotografske identifikacije. U slučaju da se zaboravi broj potvrde koju je kupac zaprimio, bit će dovoljno navesti samo broj leta. Broj potvrde u većini slučajeva se sastoji od 6 ili 7 znakova. Određene avionske kompanije šalju zajedno s brojem potvrde 2D bar koda. Bar kod je smisleni niz crnih crta i kvadratića, te svijetlih međuprostora koji daju informaciju o objektu na kojem je bar kod nalijepljen. Učitava se pomoću elektroničke naprave koji se naziva čitač bar koda. Na taj način je osigurana zaštita prilikom kupovanja e-karte.

U današnje vrijeme transakcije se obavljaju pomoću uređaja za plaćanje, tzv. platomata. Uređaji za plaćanje osiguravaju zaštitu osobnih podataka. U nekim organizacijama se uvode takvi sustavi plaćanja da zaposlenici koji rade na naplati ne vide iznos koji potrošač uplaćuje, što uplaćuje, odakle dolazi itd. Nije tajna da takve sustave plaćanja imaju pružatelji telekomunikacijskih usluga i pružatelji usluga opskrbe plinom distribucijskim kanalima. Platomat je samouslužni uređaj namijenjen automatiziranju potprocesa uplate i isplate koji su dio procesa blagajničkog poslovanja. Sve hardverske i softverske komponente moraju imati vrlo visoku pouzdanost jer se radi s gotovim novcem pa moraju nesmetano i sigurno obavljati sve korisničke i novčane transakcije. Hardverske komponente koje čine uređaj za plaćanje su kućište platomata u koje se ugrađuje stolno računalo s internim dijelovima visoke pouzdanosti, ekran osjetljiv na dodir, mehanički uređaji za prihvat papirnatog novca, mehanički uređaji za prihvat i vraćanje kovanica, unutarnje i vanjske sabirnice. Drugi važan dio platomata je softver kojim upravlja korisnik preko ekrana osjetljivog na dodir. Softver platomata mora omogućiti da se prilikom uplate i isplate evidentiraju nastali poslovi.

4. PRIKAZ REZULTATA ANKETE NA TEMU SIGURNOST I ZAŠTITA ELEKTRONIČKIH PODATAKA

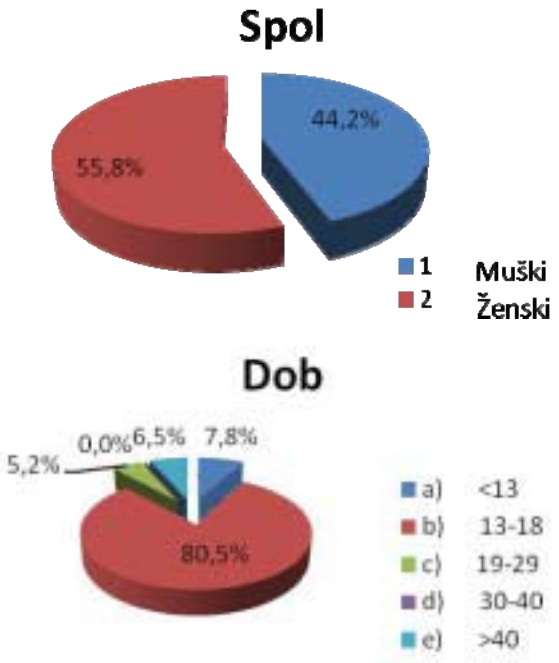
Danas je anketiranje najučestaliji proces prikupljanja podataka u različitim vrstama ispitivanja i društvenih istraživanja. Pod anketiranjem se podrazumijevaju svi istraživački postupci i aktivnosti kojima se prikupljaju podaci, te se dobiju informacije o karakteristikama pojedinca, društvenih skupina, programskih alata, o društvenim mrežama, računalima, učestalosti korištenja određenih vrsta internet preglednika itd. Anketom na temu sigurnosti i zaštite elektroničkih podataka prikupljeni su podaci o spolu, dobi, korištenju društvenih mreža, sigurnosti podataka na internetu, privatnosti na internetu, identitetu na internetu i o količini primanja neželjene pošte. Da je anketa optimalne dužine, pokazuje vrijeme koje je trebalo da ju ispitanici popune, 15-20 minuta.

Anketa je trebala dati sljedeće povratne informacije: broj ispitanika koji koriste određenu društvenu mrežu, informaciju o razini znanja o sigurnosti na internetu, mišljenje korisnika interneta o ugroženosti njihove privatnosti na internetu, informaciju o potencijalnoj opasnosti na internetu od lažnog predstavljanja, podatke o broju krađe identiteta, informaciju o tome koliko se ispitanici javno ocrnjuju na internetu (pošto je internet javna računalna mreža), informaciju o broju SPAM-ova koje korisnici primaju elektroničkom poštom (na temelju informacije može se preporučiti određeni alat za filtriranje SPAM-ova), podatke o tome koliko često ispitanici koriste opciju u internet pregledniku za brisanje povijesti pregledavanja (dobro je za korisnika interneta u javnim organizacijama, da mu brisanje povijesti pregledavanja prijeđe u naviku), koje mogućnosti najčešće koriste ispitanici za zaštitu elektroničkih podataka te podatke o vrsti korištenog antivirusnog programa. Može se zaključiti da najčešće korišteni antivirusni program pruža veću zaštitu ili je „free“, tj. za sve je korisnike besplatan i ovisno o kapacitetu kanala brzo je dostupan.

Naše istraživanje odnosi se na onu populaciju koja jako puno koristi internet, a to su oni od 13 do 18 godina, te od 19 do 29 godina starosti. Ljudi te

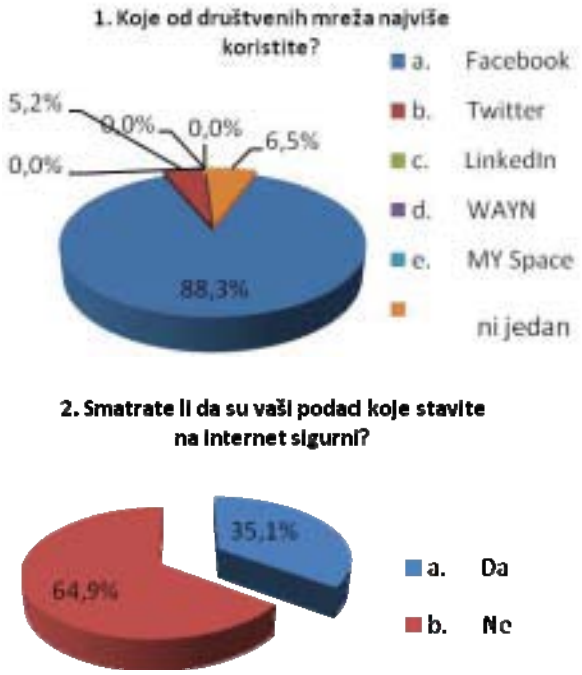
dobi su terenski uzorak populacije. On je reprezentativan, što znači da ima svojstva koja su relevantna za predmet istraživanja. Veličina uzorka je 154 (N=154).

Rezultati su obrađeni i prikazani u postocima 3D tortnim rascijepanim grafikonima u MS Excelu, alatu za analitičku obradu podataka. Ovaj alat je praktičan za analitičku obradu podataka prikupljenih anketom, te za izradu 2D i 3D prikaza podataka. Osim spomenutih prikaza, rezultati mogu biti dani linijskim, stupčastim, trakastim, tortnim, XY raspršenim grafikonima, piramidnim, površinskim, polarnim, plošnim, mjehuričastim grafikonima itd. Za obradu rezultata ankete korištena je funkcija COUNTIF. Funkcija COUNTIF broji ćelije koje unutar raspona ispunjavaju zadani kriterij. Sintaksa COUNTIF funkcije je COUNTIF(domet;kriterij). Kriterij je u ovom slučaju bio zaokruženo slovo i upisivao se u navodnicima. Iz tog razloga je odlučeno da se podaci obrade u MS Excelu. U većini slučajeva korišteni grafikon za prikaz rezultata ankete je 3D tortni grafikon, pa se on koristio tijekom cijelog istraživanja.



Slika 7. Broj anketiranih i njihova dob

Slika 7. prikazuje broj anketiranih muškaraca i žena, te njihovu dob. Vidi se da su podaci prikupljeni najviše od osoba starosti 13-18 godina, jer su oni najčešći korisnici internetskih servisa. Od žena 18 ih je više anketirano nego muškaraca. Od ukupnog broja anketiranih, 80,5% osoba je u dobi 13-18 godina, dok je 6,5% anketiranih starijih od 40 godina. Brojka od od 5,2% anketiranih je u dobi od 19 do 29 godina.

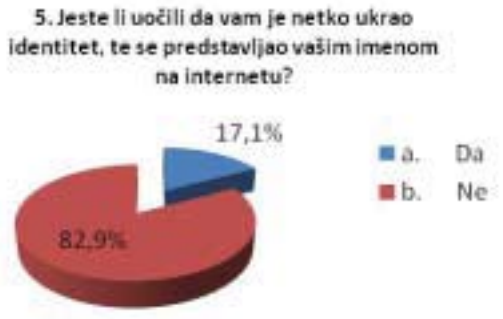


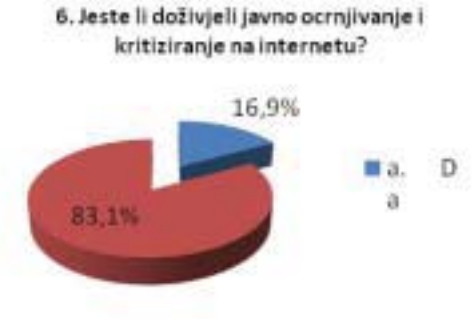
Slika 8. Najviše korištene društvene mreže i sigurnost podataka na internetu

Od društvenih mreža najviše se koristi Facebook, bez obzira na njegove nedostatke. Prema istraživanju na terenskom uzorku od 154 ispitanika, 136 ispitanika izjasnilo se da koristi Facebook, njih 10 uopće ne koriste društvene mreže, dok je 8 ispitanika zaokružilo da koristi Twitter. Rezultati pokazuju da je najpopularniji internetski servis Facebook. Kada je posrijedi sigurnost interneta 100 ispitanika misli da njihovi podaci nisu sigurni na internetu, dok 54 ispitanika misli da su sigurni, što je previše u odnosu na broj mogućih opasnosti i napadača koji su prisutni u virtualnom i stvarnom svijetu. Društvene mreže na kojima je prijavljeno najviše korisnika su i najopasnije, jer je veća vjerojatnost da postoje korisnici okarakterizirani kao zlonamjerne osobe. Slika 8. prikazuje rezultate u postocima: 88,3% od ukupnog broja ispitanika koristi Facebook, 6,5% je reklo da uopće ne koriste društvene mreže, dok 5,2 % ispitanika koristi Twitter. Ispitanici, njih 64,9% smatra da njihovi osobni podaci nisu sigurni na internetu, dok 35,1% smatra da su osobni podaci sigurni na internetu.

Slika 9. Odgovori ispitanika na pitanja 3. i 4.

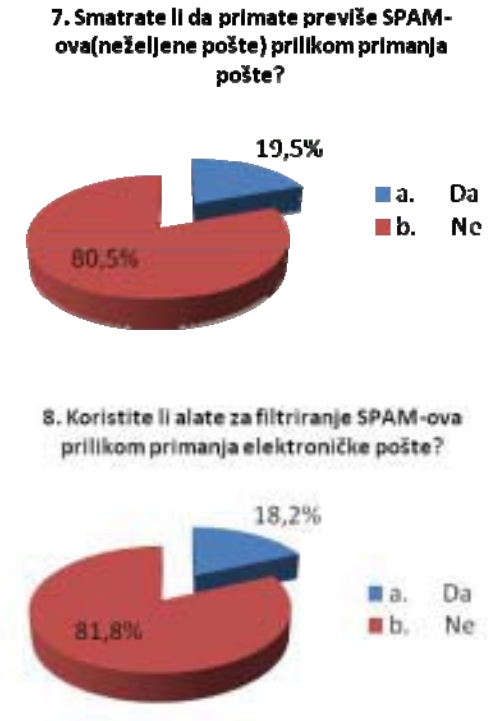
Slika 9. prikazuje odgovor ispitanika na 3. i 4. pitanje. Na temelju te slike može se vidjeti da se 86 ispitanika izjasnilo, tj. 55,8%, da im je privatnost na internetu ugrožena. Vidi se da su ispitanici tražili sredinu prilikom odgovaranja na 3. pitanje. Privatnost korisnika interneta nije ugrožena. Lako se može dogoditi da korisnik dopusti zlonamjernim osobama objavljivanje osobnih i drugih podataka. Većina anketiranih se ne predstavlja lažno na društvenim mrežama i to je dobro. Od ukupnog broja ispitanika 77,9% izjasnilo se da se nikada nisu lažno predstavljali na internetu, dok se njih 22,1% lažno predstavljalo.





Slika 10. Odgovori ispitanika na 5. i 6. pitanje

Slika 10. prikazuje odgovore ispitanika na 5. i 6. pitanje. Od 100% ispitanih 82,9% njih odgovorilo je da im nitko nije ukrao identitet na internetu, niti se nitko nije predstavljao njihovim imenom. Njih 17,1% doživjelo je to da je netko drugi (napadač) pisao i komunicirao na internetu u njihovo ime, bez njihovog znanja. Javno ocrnjivanje na internetu nije doživjelo 83,1% ispitanika, dok je 16,9% doživjelo ocrnjivanje i kritiziranje.



Slika 11. Odgovori ispitanika na 7. i 8. pitanje

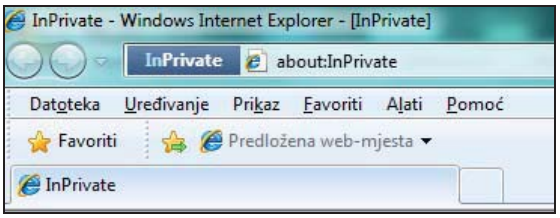
Slika 11. prikazuje 3D rezultate odgovora na 7. i 8. pitanje. Na temelju grafikona može se vidjeti da korisnici elektroničke pošte ne dobivaju previše SPAM-ova prilikom preuzimanja pošte. Odmah se može zaključiti da većina ispitanika ne koristi alate za filtriranje SPAM-ova, na što pokazuju i rezultati odgovora na 8. pitanje. Ispitanici, njih 81,8% izjasnilo se da ne koriste alate za filtriranje SPAM-ova, dok 18,2% ispitanika koristi takve alate.

Slika 12. Prikaz upozorenja pružatelja usluge web pošte za primitak SPAM-a

Slika 12.[12] prikazuje upozorenje pružatelja internet usluge web pošte da je skinuta pošta koja možda nije od navedenog pošiljatelja, te upozorava da budemo oprezni ako namjeravamo otvoriti neke veze ili ako namjeravamo slati osobne podatke napadaču. Sa slike 12. vidi se da napadač želi saznati naše ime, zemlju, telefonski broj, starost, profesiju, ime naše banke i adresu, te broj korisničkog računa. Ovaj SPAM ne izgleda ni malo uvjerljivo. Napadač bi se na temelju spomenutog primjera trebao više potruditi da dođe do željenih podataka.

Slika 13. Odgovori ispitanika na 9. i 10. pitanje

Slika 13. prikazuje 3D grafikone izrađene na temelju prikupljenih odgovora na pitanja 9. i 10. Na temelju 9. pitanja može se zaključiti da korisnici internet preglednika ne brišu često povijest pregledavanja, što nije dobro. Sa slike 13. vidi se da većina korisnika briše povijest pregledavanja jedanput mjesečno, 40,3%. Češće bi trebalo brisati povijest pregledavanja. Ako pretražujemo internet na tuđim računalima ili javno dostupnim računalima, npr. u knjižnicama, preporuča se brisati povijest pregledavanja. Korisnik koji poslije nas koristi isto računalo može vidjeti podatke o pretraživanju, tj. koje smo web stranice otvarali internet preglednikom. Web preglednici nude mogućnost da se prilikom pretraživanja interneta ne bilježi povijest pregledavanja. Npr. tu mogućnost nudi Internet Explorer (slika 14.) pod opcijom pregledavanja web stranica na internetu InPrivate. Mogućnost InPrivate uključuje se:
pritiskom Ctrl+Shift+P ili u naredbenoj traci *sigurnost->pregledavanje Weba InPrivate.*

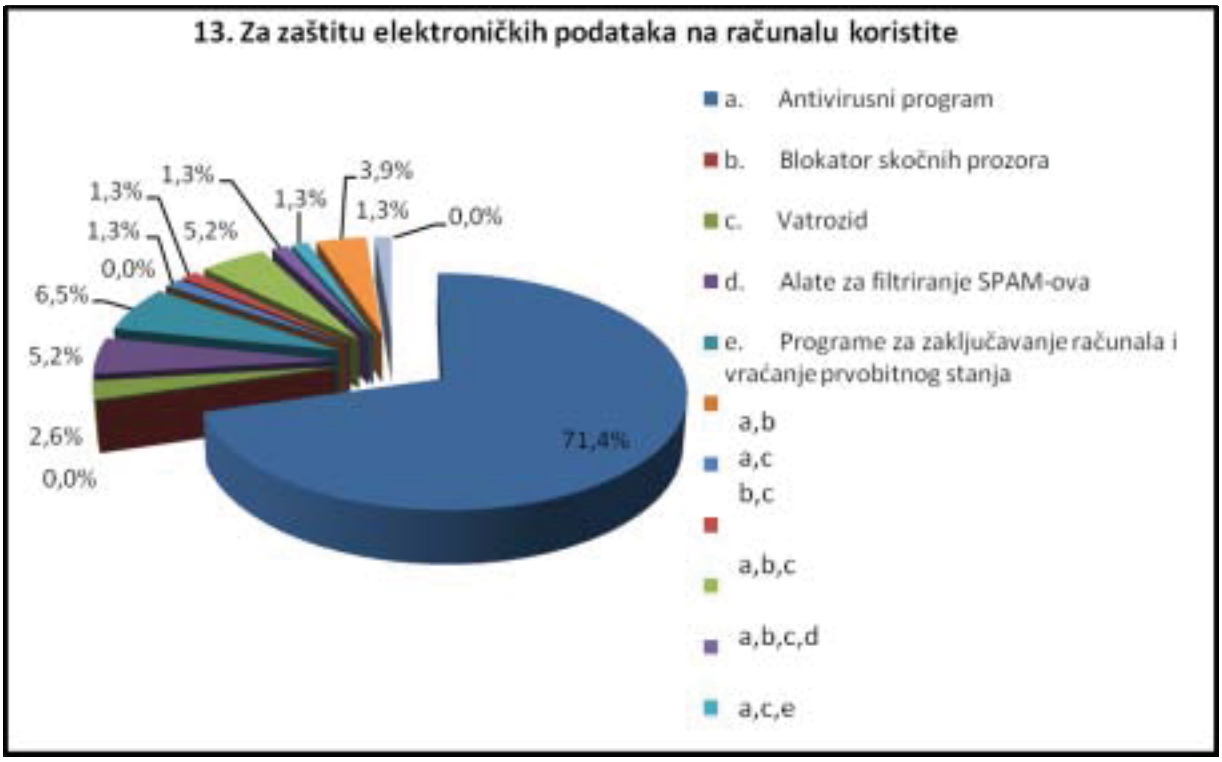


Slika 14. Pregledavanje *Weba InPrivate*

Na temelju odgovora na 10. pitanje vidi se da većina anketiranih korisnika interneta i računala „živi u zabludi“. Podaci na računalu nisu trajno izbrisani ukoliko ih se izbriše iz koša za smeće. Da bi se trajno izbrisali podaci s diska potrebno je više prolaza. Za sigurno brisanje čvrstog diska nakon prestanka njihovog korištenja koriste se dodatno određeni alati.

Slika 15. Odgovori ispitanika na 11. i 12. pitanje

Slika 15. prikazuje 3D grafikone. Većina ispitanika (83,1%) misli da prijenosnom računalu nije mjesto na stolu koji svi koriste. Razlozi su: (1) prijenosno računalo netko može ukrasti, (2) mogu se pregledavati podaci koji bi trebali biti tajni za pojedinca, (3) može se fizički razbiti itd. Slika 15. prikazuje da 51,9% ispitanika ne koristi lozinku prije pristupa operacijskom sustavu na vlastitom računalu, dok 48,1% ispitanika ima postavljenu lozinku.



Slika 16. Odgovori ispitanika na 13. pitanje

Kada je riječ o zaštiti elektroničkih podataka i operacijskim sustavima u računalu, ljudi najviše koriste antivirusne programe, programe za zaključavanje računala i vraćanje prvobitnog stanja, alate za filtriranje SPAM-ova, vatrozid i blokator skočnih program, a i druge alate za elektroničku zaštitu podataka.

Broj ispitanika	Korišten antivirusni program
56	Ne znam
38	AVG free
22	Avira
14	NOD Eset
10	NOD 32
6	Microsoft Security Essentials
4	Nemam (Linux)
2	Norton
2	SUPERAntiSpyware
154	Ukupno:

Tablica 1. Broj korištenih antivirusnih programa

Tablica 1. prikazuje broj ispitanika i koliko ispitanika (koji su popunili anketu) koristi određeni antivirusni program. Mnogo njih ne zna koji antivirusni program koristi, što nije pohvalno. Od 154 anketiranih, od ponuđenih antivirusnih programa najviše koriste AVG free. AVG free koriste ispitanici najčešće zato što je besplatan, jer se lako može skinuti i prepoznaje dovoljan broj virusa (trojanaca i crva). Kod 14. pitanja ispitanici su morali sami navesti koji antivirusni program koriste. Drugi najčešće korišteni antivirusni program je Avira, nakon njega slijede NOD ESET, Microsoft Security Essentials, Norton i SUPER AntiSpyware.

5. ZAKLJUČAK

Da bi što efikasnije spriječili upad u računalo nužno je osigurati njegovu fizičku zaštitu, odnosno prostoriju gdje se nalazi. Ukoliko su u prostorijama računala na kojima su pohranjeni važni podaci, te prostorije treba dodatno zaštititi video-nadzorom, pametnim karticama, karakteristikama biometrije ili na neki drugi način. Računalni kriminal se nikada neće do kraja suzbiti, ali se svakako preporuča djelovati preventivno. Treba pripaziti kome se šalju i gdje se objavljuju podaci. Za sprječavanje gubitka podataka preporuka je spremiti dokument na standardni način, tj. sa standardnom ekstenzijom datoteke, učestalo snimati promjene (Ctrl+S), često izrađivati sigurnosnu kopiju, koristiti antivirusni program s licencom i sigurnosnu stijenku, izbjegavati stavljanje osjetljivih podataka na web, često brisati povijest pregledavanja, raditi enkripciju podataka itd.

Anketa na temu sigurnosti i zaštite elektroničkih podataka daje podatke o trenutačnom mišljenju ispitanika o sigurnosti na internetu, krađi identiteta, ocrnjivanju i zaštiti podataka itd. Na temelju dobivenih rezultata prikazanih grafikonima u postocima može se zaključiti da ne postoji previše napada na osobne elektroničke podatke i upada u

računala osoba ispitanih u školama. Ispitanici su bili učenici i nastavnici. Razlog zbog kojeg napadi nisu česti su upozorenja koja se učestalo daju korisnicima interneta putem medija, tečajeva, na predavanjima u školama, fakultetima, internetu i putem projekta „Sigurnost djece na internetu“. Iz rezultata ankete, od 154 ispitanika na internetu se lažno predstavljalo njih 34. Nije teško zaključiti da će se ispitanici lažno predstavljati na onim internetskim servisima koje najviše koriste (u ovom slučaju to je Facebook). U organizacijama gdje je provedeno istraživanje nastojat će se pozitivno djelovati na ispitanike kako bi se smanjilo lažno predstavljanje. Da bi se ono spriječilo treba omogućiti da se korisnici biometrijski autoriziraju na internetskim servisima. Na taj način bi se lako mogle pronaći osobe koje se predstavljaju tuđim imenima. Jedini je problem kod uvođenja sustava za biometrijsku autorizaciju internet korisnika, financijska isplativost i mogućnosti internetskih servisa. U današnje vrijeme pružatelji internet usluga i proizvođači operacijskih sustava nude adrese elektroničke pošte na koje žrtve krađe identiteta mogu prijaviti svoj problem.

6. LITERATURA

[1] Bača, M. Uvod u računalnu sigurnost. Zagreb : Narodne novine d.d., 2004.

[2] Čerić, V.; Varga, M.; Birolla, H. Poslovno računarstvo. Zagreb : Znak d.o.o., 1998.

[3] Dragičević, D. Kompjuterski kriminalitet i informacijski sustavi. Zagreb : IBS, 2004.

[4] Engst, A.; Fleishman, G. Bežično umrežavanje. Praktični priručnik.Beograd: Peachpit Press i Kompjuter Biblioteka, Prvo izdanje. 2004.

[5] Ivanković, M.; Schatten, M.; Bača, M. Privatnost na Facebooku i drugim socijalnim mrežama. 2010.URL:http://bib.irb.hr/datoteka/493687. CZBtemplate.pdf. (27.2.2011.)

[6] Kurose, F.; Ross, W. Umrežavanje računala. Wesley: Računarski fakultet, Sveučilište Masačusets, Bruklin : Politehničko sveučilište, CET, Pearson Addison, 2005.

[7] Petrić, D. Internet uzduž i poprijeko. Zagreb: BUG & SysPrint, Kompletan vodič, 2002.

[8] Zane, K. Menadžment uredskog poslovanja. Oklahoma State: Sveučilište Oklahoma State, Osmo izdanje, 2010.

[9] Zakon o elektroničkom potpisu.

[10] Zakon o tajnosti podataka.

[11] IT revizija. 2011.URL: http://www.facebook.com/. (1.4.2011).

[12] Upozorenje. 2011. URL: https://mail.google.com /mail/?hl=hr&shva=1#inbox. (18.3.2011).

[13] Kriptografija. 2011.URL:http://www.zsis.hr /site/Kriptografija/tabid/126/Default.aspx, (1.3.2011).

Kontakt:
Matija Varga, mag. inf., univ. spec. oec.
Tehnička škola Čakovec
Sportska 5, Čakovec
E-mail: mavarga@foi.hr
Poslijediplomski doktorski studij
“Informacijske i komunikacijske znanosti“
FFZG