VIŠJA STROKOVNA ŠOLA ACADEMIA MARIBOR

DIPLOMSKO DELO

VARNOST ELEKTRONSKEGA POSLOVANJA FIZIČNIH OSEB V SLOVENIJI IN SVETU

Študent: Boris Ješovnik
Naslov: Ob Dravi 5a, Maribor
Številka indeksa: 11190122457
Program: Komercialist
Mentor: mag. Andrej Tomšič

Maribor, junij 2009

IZJAVA O AVTORSTVU DIPLOMSKE NALOGE

Podpisani Boris Ješovnik, št. indeksa 11190122457, sem avtor diplomske naloge z naslovom Varnost elektronskega poslovanja fizičnih oseb v Sloveniji in svetu,

katero sem napisal pod mentorstvom mag. Andreja Tomšiča.

S svojim podpisom zagotavljam, da:

- je ta diplomska naloga izključno rezultat mojega dela,
- so dela in mnenja drugih avtorjev, ki jih uporabljam v nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia.
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli kot svojih lastnih – kaznivo po Zakonu o avtorskih in sorodnih pravicah, UL RS, št. 16/2007 (v nadaljevanju ZASP), prekršek pa podleže tudi ukrepom VSŠ Academia skladno z njenimi pravili.
- Skladno z 32. členom ZASP dovoljujem VSŠ Academia objavo diplomske naloge na spletnem portalu šole.

Maribor, 6. 6. 2009 Podpis študenta:

ZAHVALA

Za pomoč in nasvete pri izdelavi diplomske naloge se zahvaljujem mentorju, mag. Andreju Tomšiču, ter ravnateljici Višje strokovne šole Academia Maribor, mag. Mirjani Ivanuša Bezjak. Za lektoriranje diplomske naloge se zahvaljujem gospe Bojani Samarin, prof.

Posebno zahvalo namenjam svojim najbližjim, ki so me vseskozi spodbujali in mi tako pomagali pri pisanju te diplomske naloge.

POVZETEK

V diplomski nalogi bom obravnaval tematiko elektronskega poslovanja. Osredotočil se bom predvsem na problematiko varnosti elektronskega poslovanja fizičnih oseb ter na možnosti računalniške zaščite pred različnimi medmrežnimi prevarami.

V zadnjih nekaj letih se je dostopnost do informacijske tehnologije razširila na uporabnike iz celega sveta. Danes sta računalnik in dostop do interneta prisotna že skoraj v vsakem gospodinjstvu in vedno več fizičnih oseb predvsem zaradi tempa življenja, ki ga narekuje današnji čas, svoje delo, študij, nakupe in plačevanje položnic opravlja kar prek domačega računalnika s pomočjo interneta. Stroka takšen način poslovanja imenuje elektronsko poslovanje s končnimi uporabniki.

Z vse večjim številom posameznikov, ki uporabljajo e-poslovanje, lahko pričakujemo tudi povečanje ogroženosti e-poslovanja. Oblik ogroženosti e-poslovanja in računalniškega kriminala je veliko. K prvim prištevamo splošne grožnje in nevarnosti ter nesreče zaradi človeškega dejavnika in strojnih poškodb in okvar. O računalniškem kriminalu pa govorimo, kadar gre za krajo ali zlorabo (osebnih) podatkov ter odkritje virusa, črva, parazitnih programov.

Seveda za vsako grožnjo in obliko računalniškega kriminala obstaja ustrezen varnostni ukrep. Ob tem pa je vendarle treba omeniti, da varnostni ukrepi, ki so končnim uporabnikom na razpolago, ne pomenijo stoodstotne zaščite pred nevarnostmi, so pa seveda nujni za zmanjševanje števila nesreč in primerov računalniškega kriminala.

Zato je za zagotovitev varnosti in zanesljivosti uporabe e-poslovanja nujno potrebno dobro poznavanje delovanja računalniških sistemov in možnosti računalniških zaščit, ki so na razpolago. Med temi so fizičnim uporabnikom najbolj znani protivirusni programi, saj je vsak uporabnik na računalniški virus že kdaj naletel.

KLJUČNE BESEDE

e-poslovanje, internet, varnost elektronskega poslovanja, medmrežna prevara, ogroženost e-poslovanja, računalniški kriminal, varnostne komponente pri elektronskem poslovanju

ABSTRACT

The objective of the diploma paper is to discuss the thematic of electronic business processes. The focus is mainly on the security problematic of natural person-electronic business processes and the possibilities of computer protection from various internet frauds.

In the last few years the availability of information technology has spread to users from all over the world. Nowadays computer and internet access are present in almost every household and, mainly because of the life pace directed by present-day, more and more people conduct their work, studies, shopping and manage money-orders with the help of the internet. The general term used for such business conduction is the electronic business process with end-users.

With the numbers of e-business users rising, the rise of e-business endangerment is to be expected as well. There are many forms of e-business endangerment and a lot of computer-related crime. Among the first, general threats are to be mentioned as well as dangers and accidents because of the human factor and hardware damage. We refer to computer-related crime when data (personal) are stolen or misused, or a virus, worm or parasitic programs are discovered.

Of course, there is a suitable security measure to be undertaken for every threat and computer-related crime. It has to be mentioned that security measures, available to end-users, don't offer a 100 % danger protection, but are necessary for reducing the number of accidents and computer-related crime.

To ensure the security and reliability of e-business use, it is necessary to have a thorough knowledge of computer systems operation and the possibilities of available computer

protection. Among those, natural persons are most familiar with antivirus programs, as each of them has encountered at least one computer virus.

KEY WORDS

e-business, internet, electronic business security, internet fraud, e-business endangerment, computer-related crime, electronic business security components

KAZALO VSEBINE

KAZALO GRAFIKONOV

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

1. UVOD

1.1. Opredelitev obravnavane zadeve

V diplomski nalogi obravnavam tematiko elektronskega poslovanja. Osredotočam se predvsem na problematiko varnosti elektronskega poslovanja fizičnih oseb ter na možnosti računalniške zaščite pred različnimi medmrežnimi prevarami.

V novejšem času se je dostopnost do informacijske tehnologije razširila na uporabnike iz celega sveta. Moje mnenje je, da sta danes računalnik in dostop do interneta prisotna že skoraj v vsakem gospodinjstvu in vedno več fizičnih oseb predvsem zaradi tempa življenja, ki ga narekuje današnji čas, svoje račune plačuje kar iz domačega fotelja. Zato je za zagotovitev varnosti in zanesljivosti uporabe e-poslovanja nujno potrebno dobro poznavanje delovanja računalniških sistemov in možnosti računalniških zaščit, ki so na razpolago.

Poleg osnovnih dejavnosti za zmanjševanje števila nesreč in primerov računalniškega kriminala se dotikam tudi standardov za obvladovanje varnosti, in sicer standarda ISO/IEC 27001:2005 in ISO/IEC 27002:2005 ter CobiT 4.1, pri katerih gre predvsem za testiranje novih verzij programske opreme na testni strojni opremi, različne antivirusne rešitve, požarne zidove, varnostne kopije ter izobraževanje upravljavcev omrežij.

1.2. Namen, cilji in osnovne trditve diplomskega dela

Namen:
V diplomski nalogi podrobno opisujem nevarnosti pri uporabi elektronskega poslovanja, predvsem pa predstavljam varnostne ukrepe in rešitve pred medmrežnimi prevarami, ki so fizičnim osebam na razpolago.

Ugotavljam, v kolikšnem številu se pojavljajo primeri medmrežnih prevar in kakšen je njihov vpliv na uporabo e-poslovanja.

Cilji:

Predstavljam elektronsko poslovanje fizičnih oseb v Sloveniji in po svetu. S pomočjo študije virov in literature sem proučeval varnostno tehnologijo v elektronskem poslovanju ter dejavnike nevarnosti elektronskega poslovanja in načine medmrežnih prevar. Izpostavljam morebitne kritične pomanjkljivosti varnosti elektronskega poslovanja. Opisujem vpliv medmrežnih prevar na uporabo e-poslovanja ter varnostne ukrepe za zaščito pred njimi.

Z analizo statistike mednarodnih raziskav ugotavljam morebiten porast medmrežnih prevar v zadnjih letih. Z analizo rezultatov ankete pa ugotavljam, kaj za fizične osebe predstavlja največjo nevarnost e-poslovanja in kateri varnostni ukrep najpogosteje uporabljajo.

Osnovne trditve-hipoteze:

1. Medmrežne prevare pri fizičnih osebah doma in po svetu v zadnjih letih strmo naraščajo.

Hipotezo bom potrdil v primeru, če bom z analizo statistike mednarodnih raziskav ugotovil, da se pojav medmrežnih prevar doma in po svetu v letih od 2000 do 2009 postopoma viša za 10 %.

2. Največja nevarnost e-poslovanja danes so virusi .

Hipotezo bom potrdil v primeru, če bom z analizo rezultatov ankete ugotovil, da so anketiranci v več kot 50 % odgovorili, da virusi predstavljajo največjo nevarnost e-poslovanja danes.

3. Za varovanje pred medmrežnimi prevarami fizične osebe najpogosteje uporabljajo protivirusne programe.

Hipotezo bom potrdil v primeru, če bom z analizo rezultatov ankete ugotovil, da so anketiranci v več kot 50 % odgovorili, da za varovanje pred medmrežnimi prevarami uporabljajo protivirusne programe.

1.3. Predpostavke in omejitve raziskovanja

V diplomski nalogi sem se omejil na študijo statistike mednarodnih raziskav o medmrežnih prevarah pri fizičnih osebah od leta 2000 do leta 2009. Anketo sem opravil med naključno izbranimi 100 fizičnimi osebami.

1.4. Predvidene metode raziskovanja

Metode dela, ki sem jih uporabljal pri pisanju diplomske naloge, bodo različne. Zaradi tematike sem se oprl predvsem na študijo literature in virov s področja informatike, navedene v seznamu.

V teoretičnem delu naloge sem na osnovi prebrane literature in virov z metodo opisovanja predstavil elektronsko poslovanje fizičnih oseb v Sloveniji in po svetu. Izpostavil sem glavne oblike in načine medmrežnih prevar in njihov vpliv na uporabo e-poslovanja fizičnih oseb. Prav tako pa sem se osredotočil na opisovanje varnostnih ukrepov pri elektronskem poslovanju.

Tudi v praktičnem delu sem za razlago statistike primerov mednarodnih raziskav in razlago rezultatov analize uporabil metodo opisovanja. Pregledal in analiziral sem statistike, ki se nanašajo na elektronsko poslovanje doma in po svetu od leta 2000 do 2009, ter ankete, opravljene med 100 naključno izbranimi fizičnimi osebami v Sloveniji.

2. INTERNET IN ELEKTRONSKO POSLOVANJE

2.1. Kako deluje internet

Internet je največje svetovno omrežje, v katerega je povezanih na milijone računalnikov z vsega sveta. Je sklop podatkov, informacijskih procesov in ljudi, ki te podatke nudijo ali uporabljajo. Gre torej za informacijsko-komunikacijsko infrastrukturo, ki jo z določenimi programi uporabljamo za komuniciranje.

Internet je možno opredeljevati iz različnih vidikov. Strokovnjaki ga opredeljujejo kot samostojen, avtonomen kibernetski prostor, ki uporabnikom omogoča prenos datotek, pošiljanje elektronske pošte in uporabo svetovnega spleta (Toplišek, 1998, 8).

Pri prenosu podatkov po internetu velja, da med pošiljateljem in prejemnikom sporočila ni potrebna sočasna zveza. Da lahko podatki v internetu pravilno prispejo, ima vsak računalnik v omrežju svoj naslov, ki se nedvoumno razlikuje od naslova drugih računalnikov. To imenujemo IP naslov, ki ga moramo poznati, če želimo z določenim računalnikom vzpostaviti zvezo.

Osnovno delovanje internetnega omrežja je naslednje:

- strežnik, ki upravlja z viri in ponuja storitve,
- stranka, ki se priključi na strežnik in uporablja vire,
- komunikacijska linija, ki skrbi za povezavo,
- računalnik, ki je lahko hkrati strežnik in stranka.

Ko uporabnik potrebuje informacijo ali dostop do določenega računalnika, požene program, ki deluje kot stranka, in se priključi na računalnik s programom, ki deluje kot strežnik in nadzoruje prenos podatkov v računalnik. Pogovor med obema teče s posebnimi protokoli, ki so definirani znotraj omrežja internet in veljajo za vse tipe računalnikov enako (Emeršič, B., Ivanuša-Bezjak, M., Vinter, M., 2005, 69 - 70).

Na internetu je na voljo veliko različnih storitev, ki se uporabljajo za elektronsko poslovanje. Najbolj znane in razširjene so elektronska pošta, prenos datotek in svetovni splet. Svetovni splet je najbolj priljubljena storitev na internetu in najpogosteje uporabljena pri elektronskem poslovanju. V njem je možno najti informacije, ki pokrivajo vsa področja človeškega delovanja (Jerman - Blažič, 2001, 16).

2.2. Opredelitev e-poslovanja

Razvoj sodobne informacijske tehnologije in interneta je močno zaznamoval sodobno poslovanje. Njuna uporaba je omogočila nove načine poslovanja.

Danes se tako neredko srečamo s spletnimi trgovinami, spletnim bančništvom, spletnimi dražbami, ki omogočajo poslovanje preko interneta kar od doma.

Obstajajo različne definicije elektronskega poslovanja. Po mnenju Evropske komisije je elektronsko poslovanje katerakoli oblika poslovne transakcije, v kateri stranke delujejo elektronsko, namesto da bi si pošiljale »telesna« sporočila ali da bi bile v neposrednem stiku (Toplišek, 1998, 4).

Vsebinsko gre pri e-poslovanju za elektronsko izmenjavanje podatkov, prodajo blaga in storitev, plačevanje, storitve trženja in komuniciranja, elektronsko zavarovalništvo, finančne prenose, bančne transakcije, elektronsko naročanje, delo na daljavo, pouk na daljavo ter storitve državne uprave na daljavo.

Nekatere raziskave so pokazale, da največji del elektronskega poslovanja predstavlja elektronsko poslovanje med podjetji. Gre za izvajanje naročil, plačil, reklamacij ter različnega poslovnega sodelovanja med podjetji preko svetovnega spleta.

Preko svetovnega spleta lahko posamezniki in podjetja poslujejo tudi z državno upravo. Lahko registrirajo vozilo, opravijo registracijo novoustanovljenega podjetja, posredujejo in pridobivajo različne obrazce.

Pri elektronskem poslovanju s končnimi porabniki, ki je tudi temelj moje diplomske naloge, pa gre v glavnem za elektronsko poslovanje z uporabo svetovnega spleta. Uporabnik lahko od doma preko interneta poravna svoje račune in položnice, kupi nov avto, študira in dela.

Obstaja več vrst elektronskega poslovanja, zato je za poimenovanje določene vrste bolje uporabiti izraze, ki takšno poslovanje označujejo bolj funkcionalno, kot so na primer (Toplišek, 1998, 4 - 5):

- elektronsko trgovanje,
- elektronsko bančništvo,
- elektronsko plačevanje,
- elektronski finančni prenosi,
- delo na daljavo,
- elektronsko založništvo,
- elektronska arbitraža, posredovanje, sojenje,
- elektronska ponudba,
- elektronske vloge,
- elektronsko zavarovalništvo,
- elektronsko naročanje,
- nematerializirano poslovanje z vrednostnimi papirji,
- elektronsko borzno poslovanje,
- elektronska prodaja,
- notranje elektronsko poslovanje (npr. v organizaciji),
- poprodajne dejavnosti.

2.3. Prednosti in slabosti e-poslovanja

E-poslovanje je s svojim razvojem uporabniku prineslo predvsem prednosti. Obstaja pa tudi nekaj slabosti. Oboje prikazuje spodnja tabela.

PREDNOSTI	SLABOSTI
preprosta, enostavna uporaba	vprašanje varnosti transakcij
preprost dostop do informacij	vprašanje tajnosti podatkov
preprosta objava informacij	nujnost stalnega posodabljanja
možnost raznovrstnih storitev	nujnost hitrega odzivanja
nižji stroški	neosebni kontakti
globalnost	
prihranek časa	

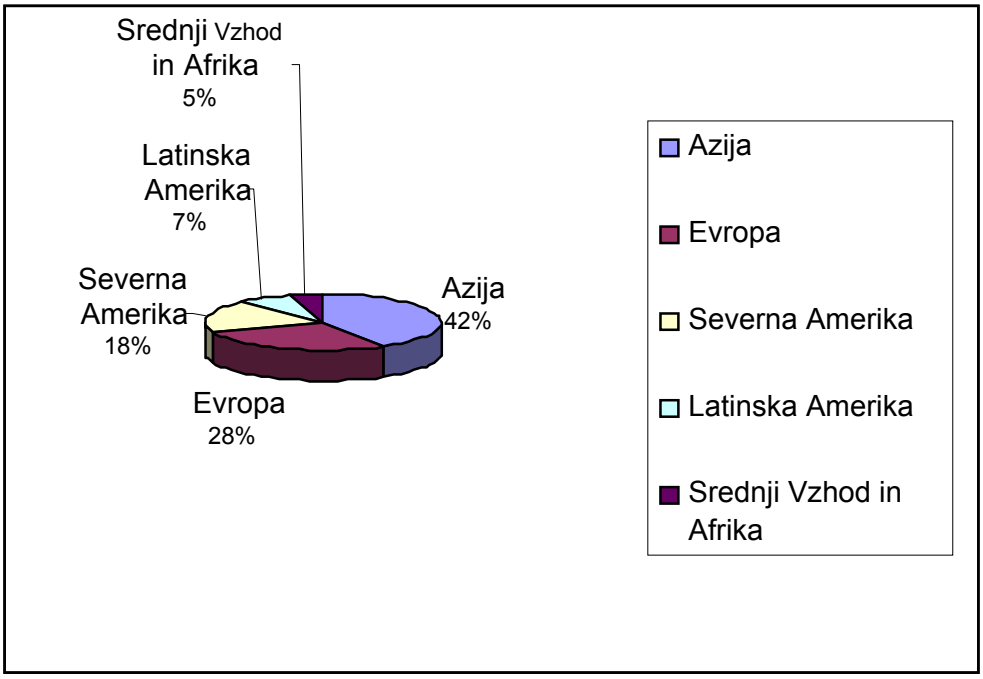
Tabela 1: Prednosti in slabosti e-poslovanja (Vir: Lasten)

2.4. Prihodnost interneta in uporaba e-poslovanja

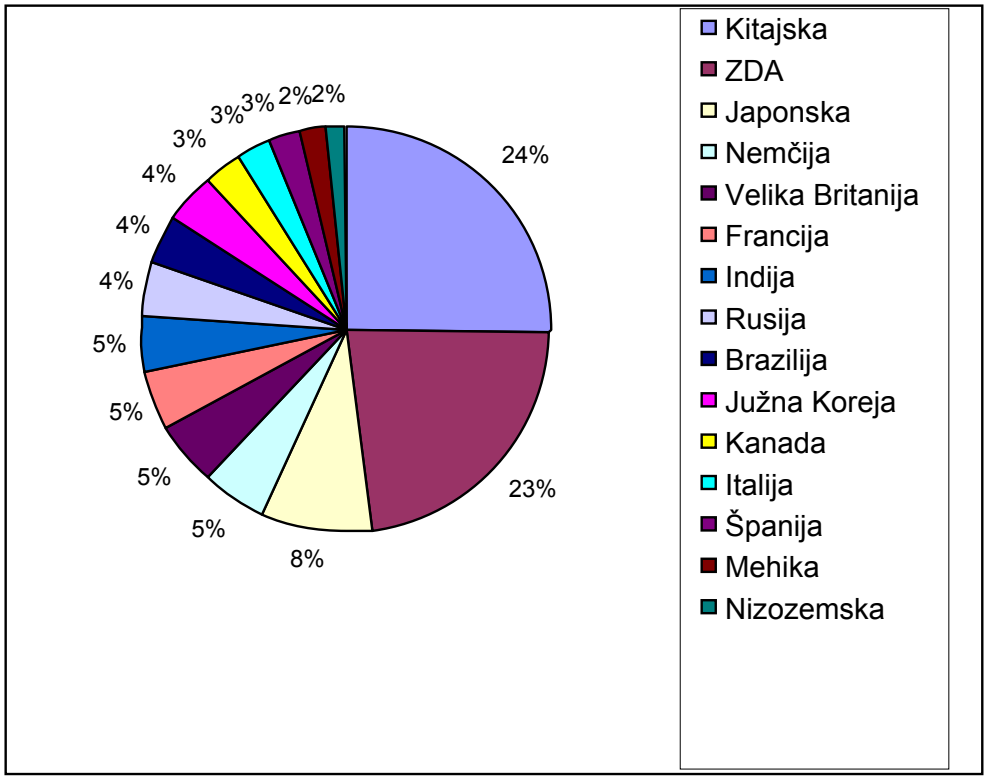
Vpliv interneta je čutiti v vseh pogledih našega življenja. Njegova uvedba je spremenila naš način dela, izobraževanja pa tudi zabave. Internet je najhitreje rastoči in razvijajoči se medij. Njegov hiter razvoj pa zahteva stalno posodabljanje sistemov, saj so razvite telekomunikacije in informacijska infrastruktura pogoj za razmah elektronskega poslovanja. Nenehno povečevati se bo morala tudi hitrost prenosa podatkov. Na internet se bo začelo priključevati vedno več naprav, povečala se bo uporaba brezžičnih omrežij. Z leti in razvojem bo e-poslovanje postalo edina oblika poslovanja.

2.5. Trendi razvoja e-poslovanja

Precej pomemben vidik razvoja e-poslovanja je opremljenost uporabnikov z dostopom do interneta. Spodnja grafikona prikazujeta, da je opremljenost uporabnikov z dostopom do interneta v primerjavi z ostalim svetom največja, to je 42 % v Aziji. Največji delež uporabnikov interneta po posameznih državah pa s 24 % zavzema Kitajska.



Grafikon 1: Uporaba interneta po svetu (vir: http://www.internetworldstats.com/, 30. 4. 2009)



Grafikon 2: Uporaba interneta po državah (vir: http://www.internetworldstats.com/, 30. 4. 2009)

Razvoj e-poslovanja narašča. Statistike so pokazale približno 68 % letno rast. Z vse večjim številom posameznikov, ki uporabljajo e-poslovanje, lahko pričakujemo tudi povečanje števila zlorab in prevar.

Kot zanimivost pa naj omenim, da internet uporablja le med 15 in 22 % svetovne populacije, zato je potencial razvoja e-poslovanja še zelo velik.

Tudi v Sloveniji se elektronsko poslovanje vse bolj uveljavlja. Izobraževanje preko interneta ni več nikakršna novost. Marsikatera zasebna šolska institucija že vrsto let zaposlenim, staršem, športnikom omogoča možnost študija preko interneta. Na enak način tudi javni sektor omogoča državljanom dostop do informacij in izvajanja storitev (zdravstvo, državna uprava). Velika pričakovanja so tudi v finančnem sektorju, saj velika večina bank že ponuja storitve preko interneta. Toda uporabnikov je razmeroma malo, saj bankam še ni uspelo najti prave poti, kako prepričati stranke, da bi vse transakcije opravile preko interneta. Zanimivo pa je, da je stranke uspelo prepričati veliko število spletnih prodajalcev, saj je uporaba spletne trgovine v velikem porastu.

3. OGROŽENOST E-POSLOVANJA

3.1. Grožnje in nevarnosti – splošno

Informacijski sistem je obsežen in zapleten ter zato občutljiv in ranljiv. Grozijo mu nesreče in različne oblike računalniškega kriminala.

Nezakonita ravnanja z računalniškimi sistemi imenujemo računalniški kriminal. Njegova glavna področja so kraja, vandalizem in sabotaža ter zlorabe sistema. Obstajajo pa še druge oblike ogroženosti e-poslovanja, to so splošne grožnje in nevarnosti ter nesreče zaradi človeškega dejavnika, strojne okvare, napake v programih, napake v podatkih, poškodbe računalniške opreme, neprimerne tehnične karakteristike in neodgovornost.

Posledice nesreč in računalniškega kriminala so lahko zelo hude. Tveganje, da pride do neželenih dogodkov, lahko zmanjšamo s sistematičnimi ukrepi za varnost in nadzor, ki jih bom podrobneje opisal v četrtem poglavju (Gradišar, 2003, 262 - 263.).

3.2. Nesreče

3.2.1. Človeški dejavniki računalniških operaterjev

Med vzroki za nesreče je na prvem mestu napačno ravnanje človeka. Kljub vsem varnostnim mehanizmom še vedno velja, da se največ vdorov v sisteme zgodi zaradi napak, nepozornosti ali nepremišljenosti uporabnikov.

Ljudje so navadno hitro zadovoljni in preveč zaupljivi do sistema, ko na začetku kaže, da le-ta pravilno deluje. Mislijo, da bo tako deloval tudi v prihodnje in posvečajo manj pozornosti preverjanju sistema in iskanju napak (Gradišar, 2003, 249 - 250). Načeloma bi se moral vsak uporabnik elektronskega poslovanja držati vsaj osnovnih varnostnih zapovedi:

- nameščena najnovejša različica protivirusnega programa,
- uporaba najnovejše različice operacijskega sistema,
- zaupno ravnanje z gesli.

3.2.2. Strojne okvare

Z razvojem računalniške tehnike postaja strojna računalniška oprema vedno bolj zanesljiva. Občasno pa se zgodi, da kakšen del strojne opreme odpove in ogrozi delovanje celega sistema.

Strojne okvare imajo lahko dve vrsti posledic. Običajna posledica strojne okvare je prenehanje delovanja. Zaradi vgrajenega sistema neprestanega preverjanja pravilnosti delovanja računalniške naprave večino strojnih napak ugotovijo same in se ustavijo.

Mnogo hujše posledice strojne okvare pa so lahko takrat, kadar se računalnik kljub okvari ne ustavi, ampak napačno deluje in daje napačne rezultate (Gradišar, 2003, 250).

3.2.3. Napake v programih (programski hrošči)

V računalniškem žargonu programski napaki pravimo hrošč in je osnovni problem računalniških sistemov.

Hrošč je napaka v izvornem besedilu programa, ki jo je programer pustil nenamerno in sama po sebi ni virus, vendar vseeno predstavlja nevarnost za sistem. Takšne napake v programu namreč predstavljajo šibke točke sistema, ki jih lahko zlonamerneži preprosto in hitro izkoristijo za vdor v sistem in povzročanje škode (www.metaling.si/varnost.php).

Odpravljanje napak ali razhroščevanje poteka v fazi testiranja programa. Program testira najprej programer, nato pa še uporabnik v fazi poskusnega delovanja programa. Kljub temu pa se lahko zgodi, da ostanejo v programu neodkrite napake, saj v večini primerov ne

moremo preveriti prav vseh možnih kombinacij vhodnih podatkov (Gradišar, 2003, 250 - 251).

3.2.4. Napake v podatkih

Vnos podatkov v računalnik je pretežno ročen. Pri vnosu podatkov se človek lahko zmoti, zato računalnik preverja podatke na vhodu. Preveri lahko:

- tip podatka,
- ali je vrednost podatka znotraj dovoljenih mej,
- ali ima eno izmed množice možnih vrednosti.

Npr. računalnik lahko preveri, ali je vnesena starost delavca med 18 in 70, ne more pa samodejno odkriti napake, ki je nastala, ker je bilo pomotoma vneseno 34 namesto 43 (Gradišar, 2003, 252).

3.2.5. Poškodbe

Občutljivost računalniške opreme na vplive iz okolja najbolje ilustrira dejstvo, da so vsi računalniki še pred nekaj leti za delovanje potrebovali prostore z natančno določeno stalno vlago in temperaturo. Čeprav danes predpisane tolerančne meje fizičnih parametrov za normalno delovanje opreme niso več tako ozke, pa je računalniška oprema še vedno relativno občutljiva na toploto, vlago in tresljaje. Nevaren je lahko električni udar zaradi strele, požara, poplave ali potresa.

Računalniška oprema je zelo občutljiva na mehanske poškodbe. Enote računalniške opreme (geografsko oddaljene) povezujejo številni električni vodniki. Prekinitev takega vodnika lahko povzroči prenehanje delovanja računalniškega sistema v posameznem delu ali kot celote. (Gradišar, 2003, 249 - 250).

3.2.6. Neprimerna oprema

Nekateri uporabniki imajo računalnike starejše izdelave in uporabljajo starejšo programsko opremo, ki ne podpira vseh modernih varnostnih standardov. Elektronsko poslovanje preko interneta zahteva stalno posodabljanje računalniškega sistema in opremljenost računalnika z ustreznimi tehničnimi karakteristikami, da lahko računalnik izvede zahtevane naloge.

3.3. Računalniški kriminal

Računalniški kriminal je splošni izraz za kakršnokoli uporabo računalniških sistemov pri nezakonitih dejanjih. Obstajajo številne dejavnosti, ki so povezane z različnimi oblikami računalniškega kriminala. Pri tem niso najbolj ranljive točke v informacijskih sistemih le strojna in programska oprema ter podatki, ampak največje tveganje, da pride do kriminalnega dejanja, predstavlja pomanjkljivo ali nepravilno izvajanje določenih procedur in malomarnost ljudi pri delu s pomembnimi dokumenti (Gradišar, 2003, 254 - 255).

3.3.1. Kraja

V mnogih primerih kraje so storilci uporabili računalnik kot orodje. Take primere razdelimo v tri skupine:

- kraja z vnosom goljufivih podatkov,
- sprememba programov,
- neposredna kraja podatkov.

(Gradišar, 2003, 256).

3.3.1.1. Vnos goljufivih podatkov

Gre za najenostavnejšo in najpogostejšo metodo kraje z računalnikom. Goljufive podatke storilci posredujejo z lažnim predstavljanjem ali poneverjanjem dokumentov (čeki,

identifikacijske kartice, denar). V teh primerih storilci ne potrebujejo mnogo računalniškega znanja, bolj pomembno je, da vedo, kako deluje organizacijski sistem (Gradišar, 2003, 257).

3.3.1.2. Sprememba programov

Programerji spremenijo programe na nedovoljeni način in s tem pridobijo korist. Programe spremenijo tako, da npr. posebej obravnavajo določeno številko bančnega računa, ali tako, da spremenijo pogoje za krmiljenje poteka programa (Gradišar, 2003, 257 - 258).

3.3.1.3. Kraja podatkov

Storilec ukrade podatke, ki se nahajajo na fizičnih medijih (papir, zgoščenke, diskete). Krajo je težko odkriti, če podatke le prekopira. Eden od načinov kraje podatkov je tudi kraja s prisluškovanjem telefonskim in radijskim zvezam (Gradišar, 2003, 258).

3.3.2. Vandalizem in sabotaža

Značilnost vandalizma in sabotaže je, da storilec navadno nima materialne koristi, pač pa iz različnih drugih motivov povzroča škodo na strojni in programski opremi ter podatkih. Storilec je lahko računalniški »obsedenec«, nezadovoljen delavec ali vohun. Čeprav storilci ne želijo vedno povzročiti škode, pa včasih do nje pride pomotoma. Za vandalizem in sabotažo uporabljajo storilci različne programske tehnike. Podrobneje jih opisujem v naslednjih petih podpoglavjih.

3.3.2.1. Virusi

Računalniški virus je program, ki se lahko širi preko računalnikov in omrežij z razmnoževanjem samega sebe, ponavadi brez uporabnikove vednosti. Virus okuži druge

računalniške programe in datoteke tako, da vanje shranjuje kopije svoje programske kode. Ko takšen okuženi program ali datoteko uporabimo, se hkrati aktivira tudi virus. Virusi zelo pogosto uničujejo podatke (brišejo, spreminjajo datoteke) in povzročajo škodo (izgubo podatkov, izgubo časa), v hujših primerih pa lahko uničijo tudi strojno opremo. Kopije so pogosto namenoma nekoliko drugačne, da jih protivirusni programi teže odkrivajo, zato moramo protivirusne programe vedno sproti nadgrajevati z informacijami o novih virusih (Gradišar, 2003, 258 - 259).

3.3.2.2. Črvi

Črv je program, ki se z razpošiljanjem samega sebe razmnožuje običajno preko interneta, pri čemer uporablja poštne naslove iz poštnih programov. Zaganja lahko druge programe, se razpošilja na druge računalnike ter hkrati razpošilja tudi dokumente iz okuženega računalnika, sam po sebi pa ne spreminja datotek. Hkrati lahko vsebuje kateri drugi virus, ki ob okužbi omogoči oddaljen dostop do okuženega računalnika preko interneta. Črvi so nevarni predvsem zato, ker ne potrebujejo gostitelja, ampak se razširjajo samostojno in nenadzorovano, zato lahko močno obremenijo internet (Gradišar, 2003, 259).

3.3.2.3. Trojanski konji

Program je sicer uporaben in koristen, vendar vsebuje skrite ukaze. V nasprotju s splošnim prepričanjem navadno ne spada v skupino računalniških virusov. Za razliko od virusov zanj ni značilno samorazmnoževanje, temveč je njegov namen usmerjen k zlorabi končnega uporabnika.

Uporabniku se predstavlja kot neki drugi program (npr. kot odstranjevalec neželenih poštnih sporočil). Od zunaj ne opazimo, da v sebi skriva škodljivo jedro oziroma uničevalno kodo. V trenutku, ko ta program zaženemo, virus poškoduje ali uniči podatke na diskih, omogoči oddaljen dostop, onemogoči zaščito računalnika. Zasledil sem izjavo strokovnjaka, da so lahko ti programi tudi popolnoma nedolžni ter uporabnikovemu računalniku sploh ne škodujejo.

3.3.2.4. Parazitni programi

So samostojni računalniški programi, ki so pripeti k programom, ki smo jih prenesli v lastni sistem. V naš sistem se namestijo skupaj z znanim programom.

Ločimo dve kategoriji parazitnih programov. To so oglasna programska oprema in vohunski programi, ki poskušajo ugotoviti področja, ki nas zanimajo, da bi nam reklamne agencije lahko pošiljale reklamne oglase. Vohunski programi aktivno spremljajo naše celotno brskanje po spletu in poročajo oglaševalskemu strežniku tako, da pregledajo datoteke z zgodovino brskanja, priljubljene povezave ter začasne internetne datoteke (Radetič, 2006, 13).

3.3.2.5. Verižna pisma

So elektronska pisma, ki jih uporabniki razpošiljajo na več elektronskih naslovov. Gre za pisma, ki obljubljajo določene vsote denarja, srečo ipd., če pismo uporabnik pošlje na čim več naslovov. Internet omogoča, da se pisma množijo z eksponentno hitrostjo, neomejenost na državne meje pa pomeni, da se problem širi v še večjem obsegu. V zadnjem času se ta pisma pogosto na hitro prevedejo in spremenijo ter tako čim bolje prilagodijo prejemnikom, ne glede državo, v kateri živijo. Priredijo se imena, kraji in fraze, in to tako, da vsebina ustreza kulturnemu kontekstu prejemnika in tako postane bolj verodostojna. Verižna pisma solidarnosti, ali bolje, pisma potegavščin, so pojav, s katerim se redni uporabniki interneta srečujejo vse pogosteje (Radetič, 2006, 11).

3.3.3. Zlorabe sistema

3.3.3.1. Neželeno oglaševanje po e-pošti

Je vsako sporočilo, ki je poslano večjemu številu naslovnikov in jim je tako vsiljeno določeno sporočilo. Večinoma gre za oglaševanje različnih storitev, izdelkov ipd. Pošiljatelji takšnih sporočil uporabnike večinoma želijo zavesti ali celo ogoljufati (Radetič,

2006, 10). Uporabniki sprejemajo e-pošto od podjetij, s katerimi že imajo zgrajen odnos, medtem ko ostala vsiljena pošta in podobne stvari le večajo nezaupanje v oglaševanje po e-pošti.

3.3.3.2. Zloraba zaupnih ali osebnih podatkov

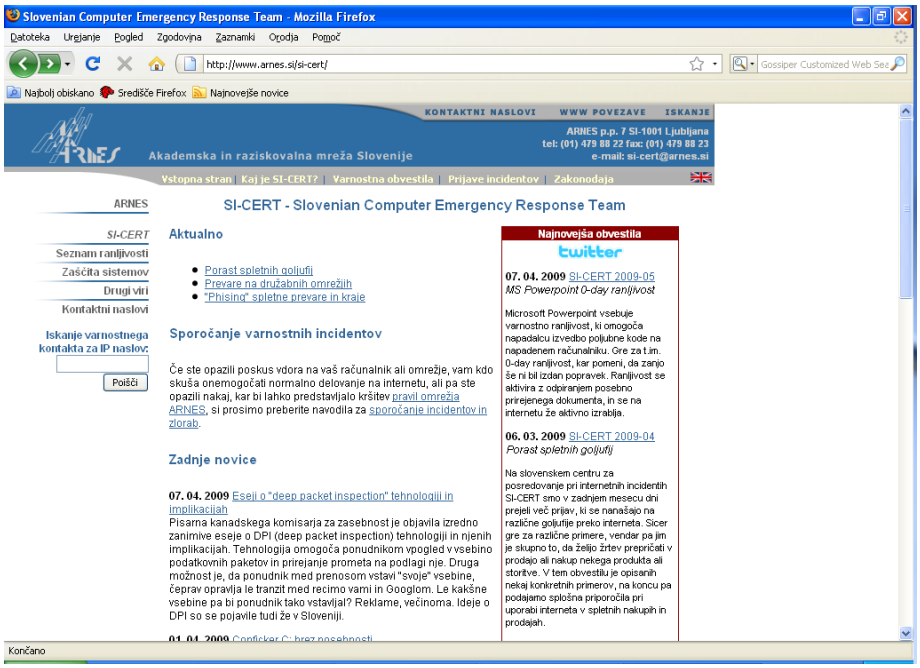
Do mnogih zlorab pride zaradi neprevidnosti ali naivnosti uporabnikov, ki zaupajo identifikacijske podatke napačnim osebam, ali jim preveč olajšajo dostop do teh podatkov. Potrebna je velika previdnost pri posredovanju gesel in drugih identifikacijskih sredstev tretjim osebam. Do zlorab prihaja, ker ljudje svoje odgovornosti v praksi ne uresničujejo, oziroma se obnašajo neodgovorno.

4. VARNOSTNI UKREPI PRED GROŽNJAMI V E-POSLOVANJU

4.1. Opredelitev in pomen varnosti

V novejšem času se je dostopnost do informacijske tehnologije razširila na uporabnike iz celega sveta. Moje mnenje je, da sta danes računalnik in dostop do interneta prisotna že skoraj v vsakem gospodinjstvu in vedno več fizičnih oseb predvsem zaradi tempa življenja, ki ga narekuje današnji čas, svoje račune plačuje kar iz domačega fotelja. Zato je za zagotovitev varnosti in zanesljivosti uporabe e-poslovanja nujno potrebno dobro poznavanje delovanja računalniških sistemov in možnosti računalniških zaščit, ki so na razpolago, saj so posledice nesreč in računalniškega kriminala lahko zelo hude.

Organizacija, ki se ukvarja za obravnavanjem nesreč in računalniškega kriminala v Sloveniji, se imenuje SI-Cert. Njene glavne naloge so reševanje varnostnih problemov v računalniških omrežjih v Sloveniji in obveščanje o zlorabah in vdorih v računalniške sisteme. Služi predvsem kot kontaktna točka za prijave incidentov, hkrati pa poskrbi tudi za povezavo s sorodnimi organizacijami doma in v tujini in spremlja reševanje opaženega poskusa vdora ali zlorabe.



Slika 1: Spletna stran SI-CERT (Vir: http://www.arnes.si/si-cert/, 26. 5. 2009)

4.2. Pravna ureditev e-poslovanja

Z razvojem informacijske tehnologije in uveljavitvijo interneta dobiva elektronsko poslovanje na gospodarskem in upravnem področju kakor tudi v domačih gospodinjstvih vedno močnejši zagon. Zato je nujno zagotoviti pravno varnost najširše uporabe elektronskega poslovanja v domačem in mednarodnem okolju. Na to dejstvo opozarjajo različna priporočila vseh pomembnejših mednarodnih organizacij, kot so Organizacija združenih narodov, Evropska unija, Svet Evrope.

Elektronsko poslovanje v Evropski uniji urejajo naslednje direktive:

- Direktiva 1999/93/EC, 13. december 1999 o elektronskem podpisu
- Direktiva 2002/58/EC, 12. julij 2002 o varovanju osebnih podatkov
- Direktiva 2000/31/EC, 8. junij 2000 o spletnem marketingu

Elektronsko poslovanje v Republiki Sloveniji urejajo naslednji zakonodajni predpisi, ki so skladni z direktivami EU:

- Kazenski zakonik RS
    - 154. člen: Zloraba osebnih podatkov
    - 225. člen: Neupravičen vstop v informacijski sistem
    - 243. b člen: Organiziranje denarnih verig in nedovoljenih iger na srečo
    - 242. člen: Vdor v informacijski sistem
    - 309. člen: Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje
- Zakon o elektronskih komunikacijah
    - 109. člen: Neželene komunikacije
- Zakon o elektronskem poslovanju in elektronskem podpisu
- Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

4.3. Standardi za obvladovanje varnosti

Poleg osnovnih dejavnosti za zmanjševanje števila nesreč in primerov računalniškega kriminala, ki jih bom obravnaval v nadaljevanju diplomske naloge, se bom v tem poglavju dotaknil tudi standardov za obvladovanje varnosti, in sicer standarda ISO/IEC 27001:2005 in ISO/IEC 27002:2005 ter CobiT 4.1, pri katerih gre predvsem za testiranje novih verzij programske opreme na testni strojni opremi, različne antivirusne rešitve, požarne zidove, varnostne kopije ter izobraževanje upravljavcev omrežij.

4.3.1. Standard ISO/IEC 27001:2005

Ob vedno večji odvisnosti od informacijskih tehnologij, odprtosti organizacij in povečevanju pomena informacij v sodobnem poslovanju je iz želje po ureditvi in poenotenju razmer v organizaciji na področju informacijske varnosti nastal standard za vodenje varovanja informacij **ISO/IEC 27001**. Standard je poslovodno in od posameznih tehnoloških rešitev neodvisno orodje, ki ponuja celovit pregled varovanja informacij pri poslovanju organizacije.

Standard določa zahteve za vzpostavitev, izvajanje, upravljanje, spremljanje, pregledovanje, vzdrževanje in izboljšanje varnostnih ukrepov informacijskega sistema (http://www.estandard.si/index.php?option=com_content&task=view&id=19&Itemid=28).

4.3.2. Standard ISO/IEC 27002:2005

Standard določa smernice in splošna načela za začetek, izvajanje, vzdrževanje in izboljšanje upravljanja varnosti informacij v organizaciji. Vsebuje najboljše prakse nadzora in kontrole ciljev na naslednjih področjih upravljanja varnosti informacij: varnostna politika, ureditev varnosti informacij, upravljanje premoženja, človeški viri, fizična in okoljska varnost, nadzor dostopa.

Predstavlja skupno podlago za učinkovito upravljanje varnosti in praktične smernice za razvoj organizacijskih varnostnih standardov in praks (http://www.e-standard.si/index.php?option=com_content&task=view&id=19&Itemid=28).

4.3.3. CobiT 4.1.

Leta 1996 je organizacija revizorjev informacijskega sistema (ISACA) izdala publikacijo Cobit in jo v kasnejših letih še izpopolnila v naslednjih izdajah. V Cobitu so zbrani in urejeni cilji in postopki revidiranja informacijskih sistemov.

Cobit je mednarodno priznan standard za varnost in kvaliteto v informacijski tehnologiji. Namenjen je predvsem informacijskemu menedžmentu za razumevanje in pravilno upravljanje ter izvajanje novih informacijskih tehnologij ter revizorjem za kontrolo informacijskih sistemov.

Cobit 4.1 določa smernice za nadzor, upravljanje in merjenje vsakega od 34 IT procesov. Zagotavlja okvir za nadzorne zahteve, tehnična vprašanja in poslovna tveganja v zvezi z informacijsko tehnologijo upravljanja. Ta okvir je namenjen za uporabo strokovnjakom v podjetjih.

4.4. Najpogosteje uporabljani varnostni ukrepi za zmanjševanje števila nesreč in primerov računalniškega kriminala pri e-poslovanju

4.4.1. Previdnost uporabnikov

Med vzroki za nesreče je na prvem mestu napačno ravnanje človeka. Prvi korak, ki ga lahko stori posameznik, je vzdrževanje fizične varnosti. To se začne z enostavnimi ukrepi, kot je prepoved uživanja hrane in pijače ter kajenje v bližini računalniške opreme. Tveganje, da pride do neželenih dogodkov, lahko zmanjšamo s sistematičnimi ukrepi za varnost in nadzor. Nekaj osnovnih pogojev za varnost informacijskega sistema, ki bi jih

moral poznati vsak uporabnik elektronskega poslovanja, je: razumevanje in upoštevanje varnostnih ukrepov, skrb za fizično zaščito strojne opreme in podatkov, preprečevanje dostopa neveščim uporabnikom, previdnost pri odpiranju datotek, pripetih k elektronski pošti, uporaba programov, ki so zaščiteni proti virusom.

4.4.2. Protipožarna pregrada

Gre za kombinacijo strojne in programske opreme, ki nadzira pretok podatkov z interneta ter ščiti sistem pred neavtoriziranim dostopanjem ali spreminjanjem podatkov v uporabnikovem sistemu. Požarni zidovi delujejo neprekinjeno in ne ovirajo običajnega dela z računalniki. Vse dogodke zapisujejo v posebne dnevnike, ki jih lahko po potrebi pregledamo, hkrati pa blokirajo vse nedovoljene aktivnosti ter uporabnika opozorijo na nepravilnosti ali morebitne poizkuse vdora. Poleg zaščite požarni zidovi omogočajo tudi izsledite v izvora nedovoljenih aktivnosti ter s tem posredno tudi osebe, ki izvaja nedovoljene aktivnosti (http://www.cert.org).

4.4.3. Protivirusni programi

Danes je na voljo precej učinkovitih protivirusnih programov, ki jih je možno nastaviti tako, da samodejno in sproti preverjajo celoten računalnik. Ti programi zagotavljajo zelo dobro zaščito našega sistema, vendar le, če jih sproti nadgrajujemo z informacijami o novih virusih, kar omogoča proizvajalec programa ponavadi samodejno preko interneta – program se samodejno poveže z ustreznim strežnikom in v naš računalnik prenese najnovejše baze podatkov s svežimi informacijami o virusih (http://www.cert.org).

Protivirusni programi delujejo tako, da v računalniku iščejo viruse, jih prepoznajo in odstranijo brez škodljivih posledic za računalnik. Ko programsko opremo posodobimo, hkrati prenesemo tudi podatke o vseh najnovejših virusih. Ker novi načini za okužbo računalnikov nenehno nastajajo, je potrebno čim pogostejše posodabljanje programske opreme.

4.4.4. Posodobitve operacijskega sistema

V izogib računalniškim zlorabam strokovnjaki priporočajo čim bolj pogosto posodabljanje operacijskega sistema. Mnogi proizvajalci operacijskih sistemov in programov ponujajo samodejno posodabljanje operacijskega sistema preko interneta. Z namestitvijo posodobitev zakrpamo varnostne luknje v operacijskem sistemu in občutno zmanjšamo možnost zlorabe.

4.4.5. Programi za odstranjevanje parazitnih komponent

Programa, ki omogočata odstranjevanje parazitnih komponent, sta Ad-Aware in Spybot Search& Destroy. Programa sta namenjena odstranjevanju in ubranitvi protisistemskih minerjev, parainternetnih strani ter preprečujeta prikazovanje oglasov na zaslonu (pop - up), nepooblaščenim preprečita opazovanje naših navad pri spletnem brskanju (http://www.cert.org).

4.4.6. Šifriranje

Zaupni podatki predstavljajo priložnost, ki potencialnega storilca vzpodbujajo k nedovoljenim dejanjem. Eden izmed ukrepov za nadzor dostopa do podatkov računalnikov je šifriranje podatkov. Cilj tega ukrepa je varovanje podatkov in zaupnih informacij. Podatke lahko pred nedovoljenimi posegi zaščitimo tako, da jih zapišemo v šifrirani obliki. Take podatke lahko razumemo samo, če jih znamo dešifrirati. Zapletene metode, kjer se pravila šifriranja menjavajo, je skoraj nemogoče razvozlati, in verjetnost, da bi nekdo na nedovoljen način prišel do podatkov, se zelo zmanjša.

Danes se najpogosteje uporabljata simetrični sistem zasebnih ključev in asimetrični sistem javnih ključev. Ključ je skrivni podatek (parameter šifre), v katerem je zajeta vsa skrivnost pri šifriranju.

Simetrični sistem uporablja en sam sorazmerno kratek zasebni ključ, ki ga poznata pošiljatelj in prejemnik. Preden pošiljatelj pošlje sporočilo, ga šifrira s tem ključem, prejemnik pa z istim ključem potem sporočilo dešifrira. Pomanjkljivost simetričnega šifriranja je, da ključ poznata najmanj dva, in da za vsakega, s katerim komuniciramo, potrebujemo drugačen ključ. Poleg tega lahko ključ kdo ukrade, medtem ko ga pošiljatelj pošilja prejemniku.

Asimetrično šifriranje je, ko uporabimo dva šifrirna ključa, javnega in zasebnega, ki sta v matematičnem razmerju. Računsko je nemogoče določiti, kateri ključ je kateri, če sta ključa dovolj dolga. Postopek je asimetričen zato, ker se ključ za šifriranje razlikuje od ključa za dešifriranje. Zasebni ključ je zaupen, tako da ga pozna samo lastnik. Javni ključ pa je na voljo vsem možnim dopisnikom. Sporočilo, šifrirano z zasebnim ključem, lahko dešifriramo z javnim, in obratno (Gradišar, 2003, 267 - 268).

4.4.7. Elektronski podpis

Temelji na sistemu javnih ključev in je funkcionalno enak ročnemu podpisu ter se enako obravnava pred zakonom. Izveden je elektronsko.

Pri šifriranju oziroma dešifriranju besedila se na strani pošiljatelja oziroma prejemnika uporabita tako javni kot zasebni ključ. Dva ključa na vsaki strani sta potrebna, ker enega uporabimo za šifriranje oziroma dešifriranje sporočila, drugega pa za šifriranje oziroma dešifriranje podpisa. Podpis je zaporedje znakov, izbranih iz besedila s posebno tehniko razprševanja. Ta tehnika zagotavlja, da tako dobljeni podpis ne velja več ob kakršnikoli spremembi besedila (pri podpisu v tem primeru torej ne gre za ime in priimek).

Elektronski podpis ne bi veljal, če ne bi bilo možno dokazati, da pripada par javnega in zasebnega ključa točno določeni osebi. Obstajajo posebne agencije za overjanje, ki dodeljujejo pare ključev določeni osebi (Gradišar, 2003, 268 - 269).

4.4.8. Digitalni certifikati

Uporabljajo se za overjanje javnih ključev, kar je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetričnem šifriranju. Za to skrbijo posebne ustanove, agencije za certificiranje javnih ključev, ki izdajo lastniku javnega ključa digitalno podpisano potrdilo, ki potrjuje avtentičnost ključa. S pomočjo tega potrdila lahko lastnik dokazuje lastništvo ključa in tudi svojo identiteto (Jerman - Blažič, 2001, 109 -111).

4.4.9. Geslo

Identiteto uporabnika lahko preverimo na podlagi nečesa, kar uporabnik ve, kar ima, ali na podlagi njegovih fizičnih sposobnosti. Najpogostejši način je preprosto z geslom. Za elektronsko poslovanje niso primerna gesla, ki jih je možno preprosto uganiti (boris123 ipd.). Boljši je sistem z enkratnimi gesli, ki veljajo le za trenutno povezavo ali aktivnost. Obstaja več variant, najpogostejša je s pomočjo kartic, ki vsebujejo mikroprocesor, majhen zaslon in uro, ki je sinhronizirana z uro v strežniku. Kartica generira novo geslo na podlagi časa, lastnik kartice, ki želi dokazati svojo identiteto, pa ga pretipka z zaslona in ga pošlje strežniku, ki nato preveri, če je geslo pravo. Obstaja tudi preverjanje na podlagi biometričnih lastnosti (prstni odtisi, očesna roženica) (Jerman - Blažič, 2001, 115 - 116).

4.4.10. Varnostni protokoli

Za zaščito transakcij v svetovnem spletu se najpogosteje uporablja protokol SSL (Secure Socket Layer). Uporabnik se najprej prepriča, ali res komunicira s pravim bančnim strežnikom, hkrati pa lahko strežnik tudi preveri identiteto stranke. Po vzajemnem overjanju SSL zagotovi neokrnjenost izmenjanih podatkov.

Protokol SSL je sestavljen iz dveh delov. SSL Handshake Protocol omogoči usklajevanje algoritma, prenos digitalnih certifikatov in določitev skupnega ključa za simetrični kriptoalgoritem. SSL Record Protocol pa definira osnovni format izmenjanih podatkov in zagotavlja neokrnjenost in šifriranje.

Uporabo protokola SSL v svetovnem splet spoznamo po predponi https v naslovu spletne strani namesto običajnega http (Jerman - Blažič, 2001, 119 - 120).

4.4.11. Varna elektronska pošta

Elektronska pošta je v zadnjem času zagotovo najbolj uporabljena storitev interneta. Prav zato je nujno potrebno dobro poznavanje varnostnih mehanizmov.

Standard, ki se uporablja za varno elektronsko pošto na internetu, se imenuje S/MIME (Security/Multipurpose Internet Mail Extension). Standard omogoča varno dostavo elektronskih dokumentov po e-pošti ter zagotavlja večino varnostnih storitev. Zaupnost sporočil dosežemo s šifriranjem, ostalo pa z digitalnim podpisovanjem.

5. STATISTIKA MEDNARODNIH RAZISKAV

V tem poglavju sem analiziral statistike o spletnih prevarah, ki jih je objavil CERT. Gre za center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih. Glavna naloga, ki jo CERT opravlja, sta sprejem in posredovanje obvestil o zlorabah in vdorih v računalniške sisteme.

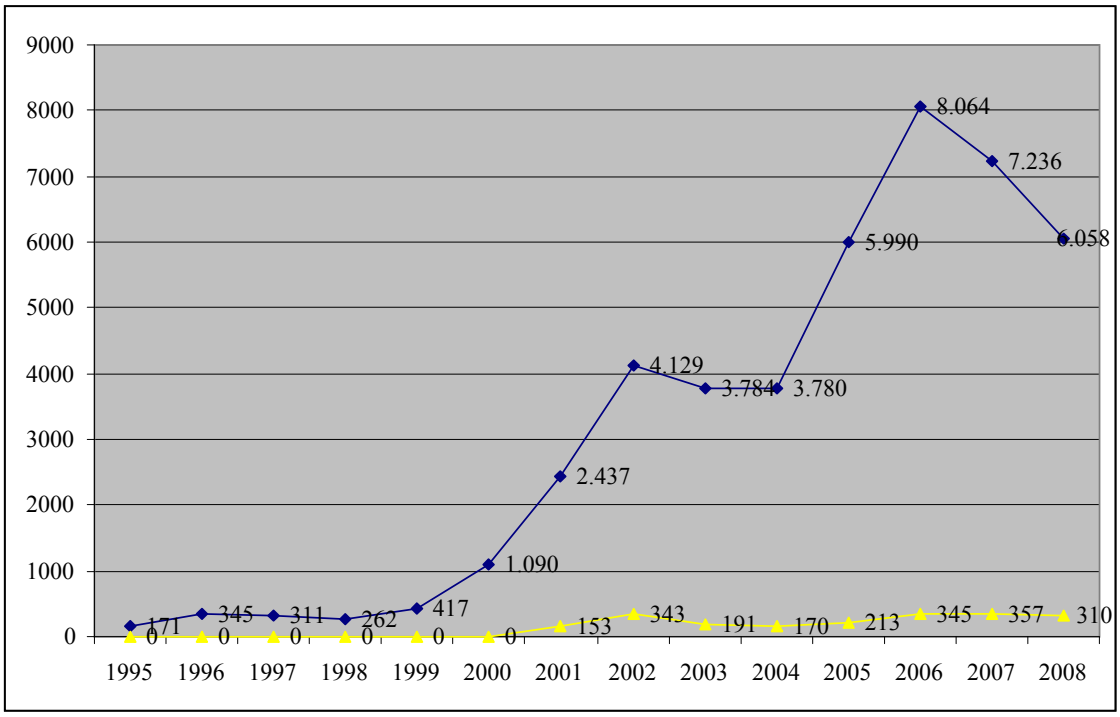
Statistika zajema prijavljene in zabeležene spletne prevare v letih 1995 do 2008. V spodnji tabeli so prikazani podatki. Sicer sem za potrditev prve hipoteze o naraščanju medmrežnih spletnih prevar v analizo želel vključiti še leto 2009, vendar podatkov za to leto še ni.

leto	zabeležene spletne prevare	prijavljene spletne prevare
2008	6.058	310
2007	7.236	357
2006	**8.064**	**345**
2005	5.990	213
2004	3.780	170
2003	3.784	191
2002	4.129	343
2001	2.437	153
2000	1.090	-
1999	417	-
1998	262	-
1997	311	-
1996	345	-
1995	171	-
SKUPAJ	44.074	

Tabela 2: Statistika spletnih prevar po letih (vir: http://www.cert.org, 30.4.2009)

Komentar k tabeli 2:

Stolpec zabeleženih spletnih prevar zajema število javno objavljenih, znanih spletnih prevar, in števila spletnih prevar, ki so jih CERT-u prijavili fizični uporabniki. Stolpec prijavljenih spletnih prevar pa zajema samo število spletnih prevar, ki so jih CERT-u prijavili fizični uporabniki. Podatki so strukturirani po številu spletnih prevar po letih, in sicer od leta 1995 do leta 2008. Krivuljo naraščanja števila medmrežnih prevar prikazujem v spodnjem grafikonu.



Grafikon 3: Krivulji spletnih prevar po letih (Vir: tabela 2, lasten)

Komentar h grafikonu 3:

Iz grafikona 3, ki prikazuje krivuljo zabeleženih spletnih prevar od leta 1995 do leta 2008, je razvidno, da so zabeležene spletne prevare v letih 1995 do 1999 v porastu, vendar v bistveno manjšem številu kot v naslednjem desetletju, ko se število zabeleženih spletnih prevar povzpne na tisoče. Krivulja od leta 2000 do 2006 zelo strmo narašča, nato se obrne navzdol. Razlika med zabeleženimi spletnimi prevarami v letu 2006, ko je bilo največ zabeleženih prevar, to je 8064, in v letu 2008, ko je bilo zabeleženih spletnih prevar 6058, je velika.

Padec števila zabeleženih spletnih prevar je rezultat vedno večje osveščenosti uporabnikov o nujnosti zagotovitve varnosti e-poslovanja in dobrega poznavanja delovanja računalniških sistemov. Rezultati ankete v poglavju 6 kažejo, da večina uporabnikov za zaščito pred medmrežnimi prevarami uporablja protivirusne programe. Ker obstaja veliko število računalniških virusov (spletnih prevar) in ker je vsak uporabnik na tovrstno prevaro že naletel, uporabniki to obliko računalniške zaščite zelo dobro poznajo, veliko bolj kot ostale. Zelo malo pa je tistih uporabnikov, ki so prepričani, da medmrežna spletna prevara

ne bi pustila nobenih posledic v njihovem računalniku. Prav tako je iz različnih raziskav in ankete mogoče zaslediti, da večina uporabnikov zaupa v storitev e-poslovanja, saj so postopki uporabe zelo preprosti. Programi za zaščito računalnikov zagotavljajo dobro zaščito. Različni proizvajalci to ponavadi omogočajo samodejno in vsakodnevno preko interneta. V internet je danes povezanih na milijone najrazličnejših uporabnikov z vsega sveta in internet kot največja svetovna informacijsko-komunikacijska infrastruktura uporabnikom različnih starostnih skupin in različnih interesov omogoča uporabo storitev, ki jim ustrezajo. Raziskava, ki jo je opravil RIS (raba interneta v Sloveniji) kaže, da sta danes računalnik in dostop do interneta prisotna že skoraj v vsakem domu. Vendar pa lahko z vse večjim številom posameznikov, ki uporabljajo e-poslovanje, pričakujemo tudi povečanje števila zlorab in prevar.

Iz krivulje, ki prikazuje gibanje števila prijavljenih spletnih prevar, je razvidno, da je njihovo število izredno nizko. Menim, da zato, ker spletne prevare prijavljajo v glavnem pravne osebe, pa še te v zelo majhnem številu, saj želijo ohraniti dobro ime, ne pa javno izpostaviti svoje računalniške ranljivosti.

Fizični uporabniki pa v prijavljanju spletnih prevar ne vidijo nobenega pozitivnega učinka in niti niso s tovrstnimi možnostmi seznanjeni.

5.1. Rezultati analize statistike

Rezultati analize statistike mednarodnih raziskav o zabeleženih in prijavljenih spletnih prevarah so pokazali postopno, tudi do dvakratno višanje števila zabeleženih in prijavljenih spletnih prevar glede na prejšnje leto v letih 2000 do 2006. Od 2006 do 2008 so pokazali postopno padanje števila zabeleženih in prijavljenih spletnih prevar.

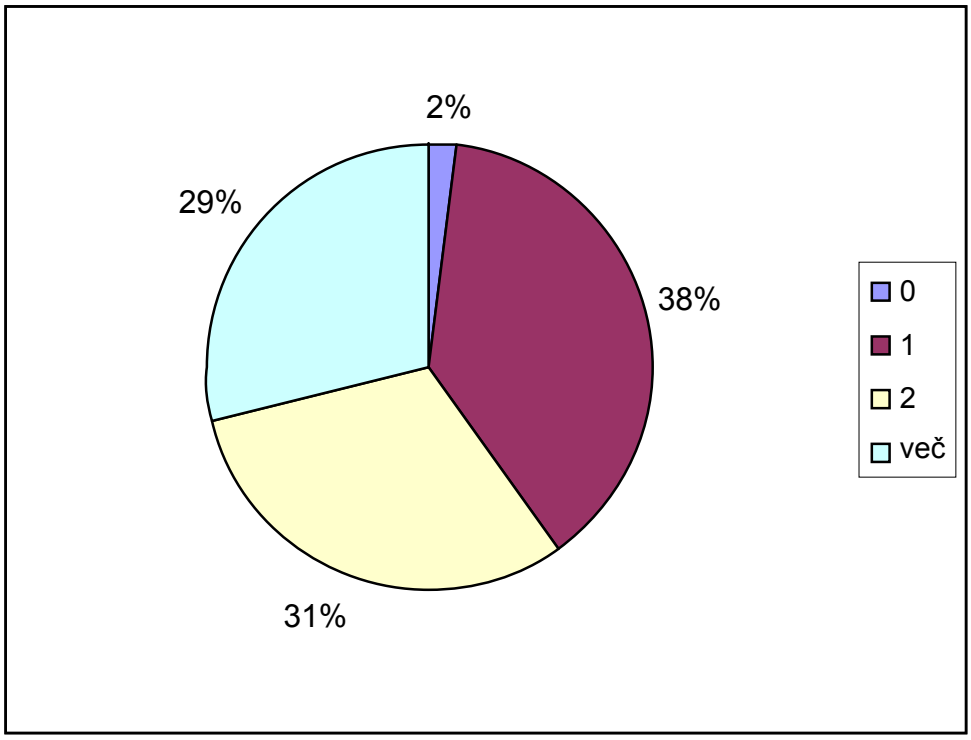
Hipoteza, da medmrežne prevare pri fizičnih osebah doma in po svetu v zadnjih letih strmo naraščajo, **je delno potrjena**, saj je število zabeleženih in prijavljenih spletnih prevar od leta 2006 do 2008 postopoma padalo.

6. ANKETA

Anketo sem opravil v drugi polovici meseca aprila 2009 med naključno izbranimi 100 fizičnimi osebami. Dobil sem 42 pravilno izpolnjenih vrnjenih anket. Anketa je priložena diplomski nalogi kot priloga 1.

6.1. Rezultati ankete

1. vprašanje: Koliko računalnikov imate v vašem gospodinjstvu?

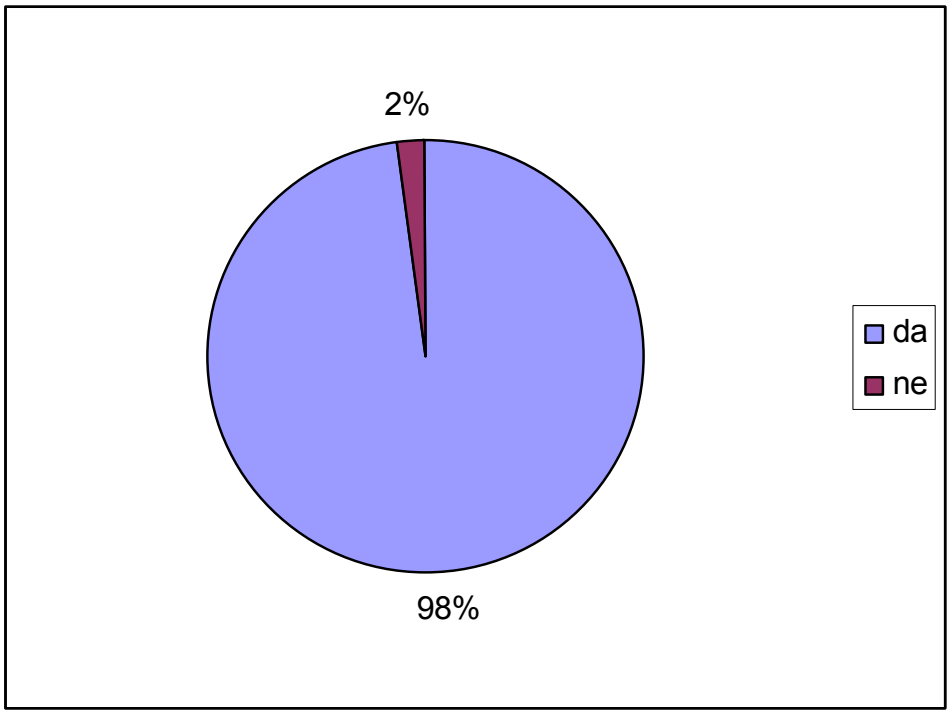


Grafikon 4: Prikaz rezultatov 1. vprašanja

Komentar h grafikonu 4:

Iz grafikona je razvidno, da ima od skupno 42 anketirancev 38 % v svojem gospodinjstvu samo en računalnik. Računalnika nima samo en anketiranec. Ugotavljam, da v današnjem času vsako gospodinjstvo premore vsaj enega, če že ne več računalnikov.

2. vprašanje: Ali imate v vašem gospodinjstvu dostop do interneta?

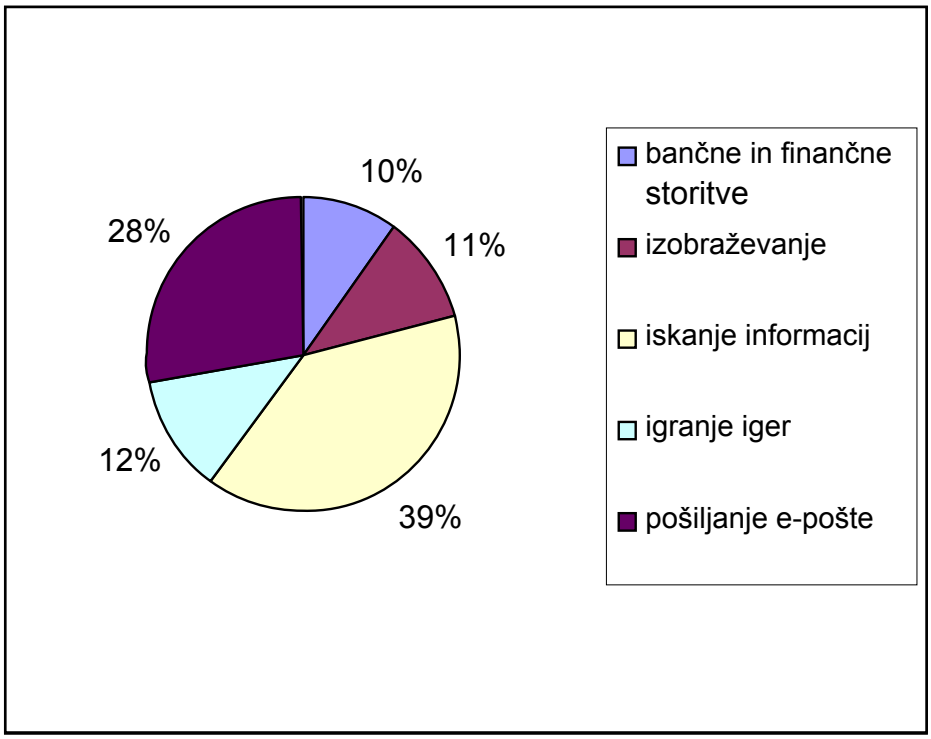


Grafikon 5: Prikaz rezultatov 2. vprašanja

Komentar h grafikonu 5:

Po pričakovanju ima 41 od skupno 42 anketirancev, kar predstavlja 98 %, dostop do interneta. Ugotavljam, da sta danes računalnik in dostop do interneta prisotna že skoraj v vsakem domu.

3. vprašanje: Za katere storitve uporabljate internet?



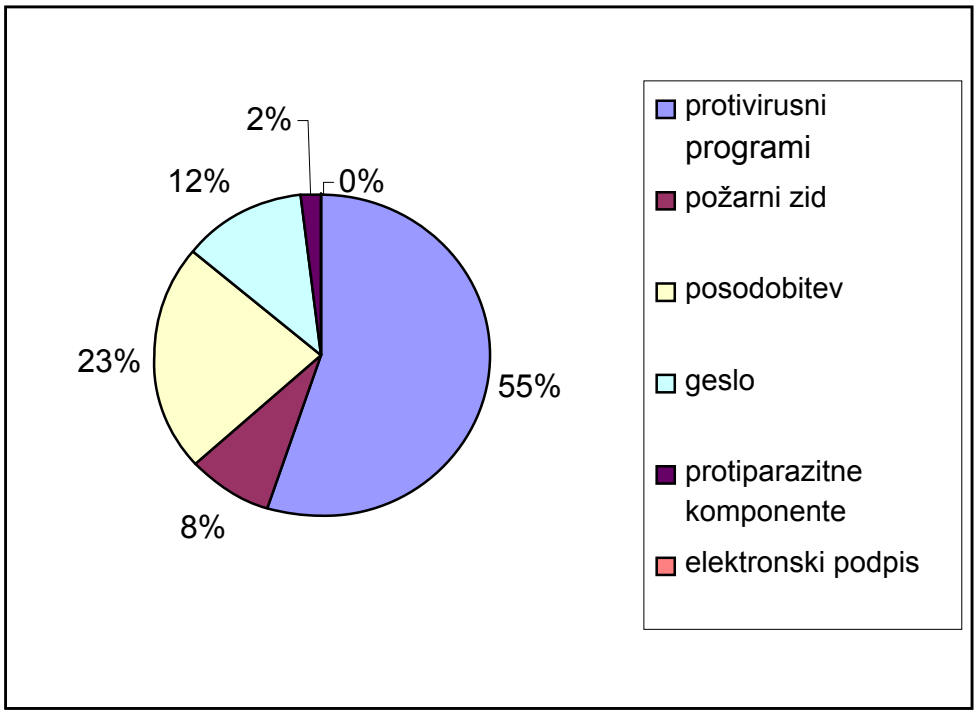
Grafikon 6: Prikaz rezultatov 3. vprašanja

Komentar h grafikonu 6:

V internet je danes povezanih na milijone najrazličnejših uporabnikov z vsega sveta in internet kot največja svetovna informacijsko-komunikacijska infrastruktura uporabnikom različnih starostnih skupin in različnih interesov omogoča uporabo storitev, ki jim ustrezajo.

Tudi rezultat ankete potrjuje moje mnenje, da uporaba interneta ne prevladuje zgolj za eno storitev, temveč je njegova uporaba zelo razgibana.

4. vprašanje: Katere oblike računalniške zaščite uporabljate v svojem gospodinjstvu?



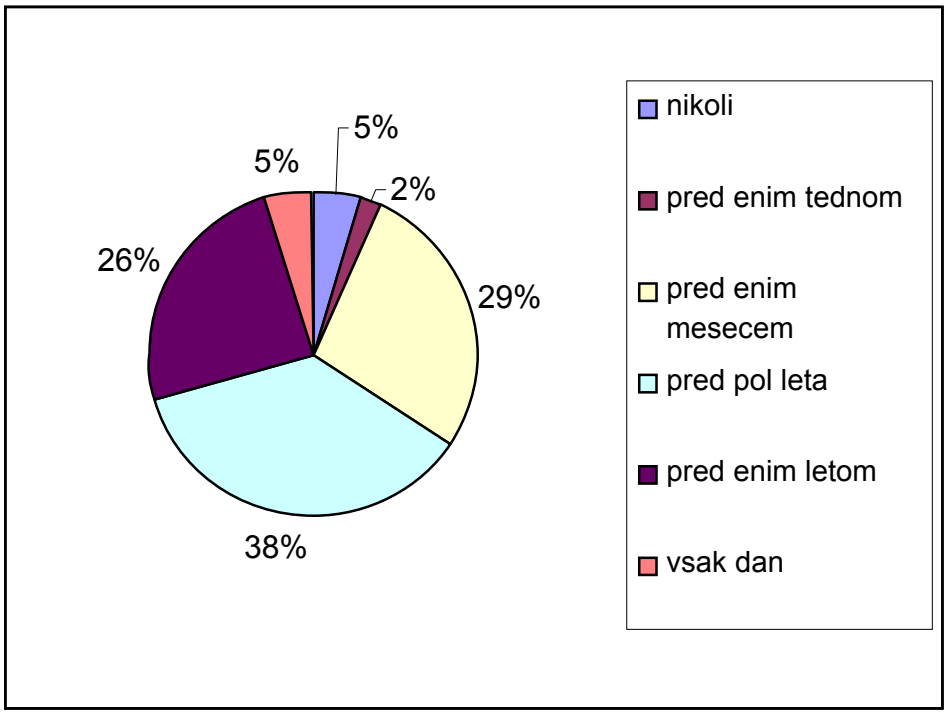
Grafikon 7: Prikaz rezultatov 4. vprašanja

Komentar h grafikonu 7:

Rezultati kažejo, da anketiranci za zaščito svojih elektronskih podatkov v večini uporabljajo protivirusne programe. Izmed petih ponujenih oblik računalniške zaščite je 33 anketirancev, kar predstavlja 55 %, izbralo odgovor protivirusni programi. S tem se je **potrdila** moja **hipoteza**, da za varovanje pred medmrežnimi prevarami fizične osebe najpogosteje uporabljajo protivirusne programe.

Ker obstaja veliko število računalniških virusov, in ker je skoraj vsak uporabnik na računalniški virus že naletel, uporabniki to obliko računalniške zaščite zelo dobro poznajo, po mojem mnenju bolj kot ostale. Danes je na voljo veliko učinkovitih protivirusnih programov, ki zagotavljajo zelo dobro zaščito računalniškega sistema.

5. vprašanje: Kdaj ste nazadnje posodobili katero izmed oblik zaščite?

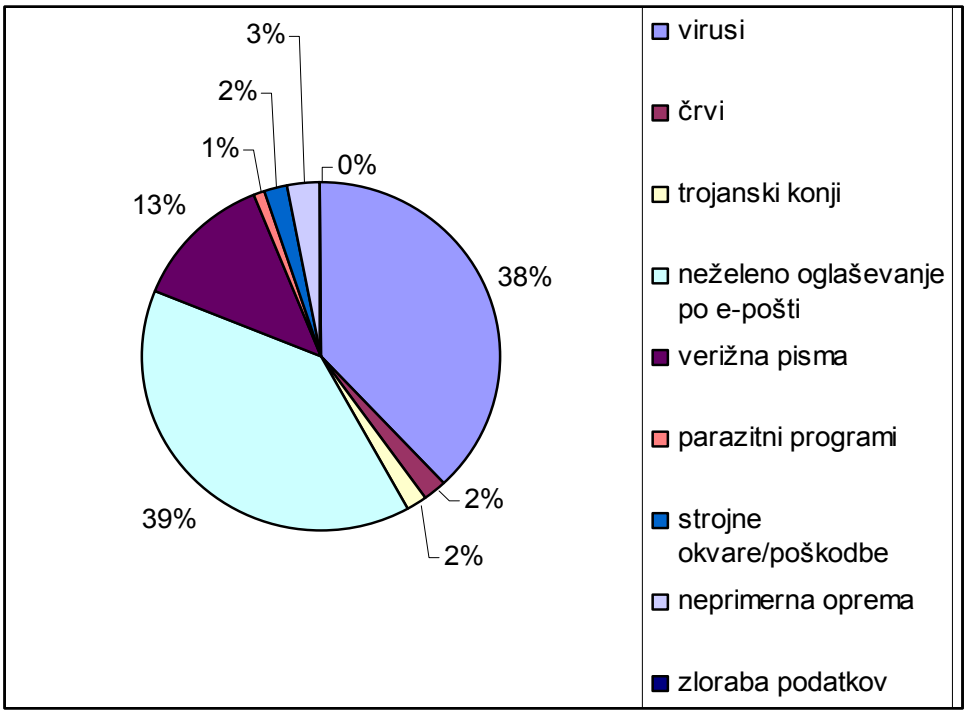


Grafikon 8: Prikaz rezultatov 5. vprašanja

Komentar h grafikonu 8:

Programi za zaščito računalnika zagotavljajo dobro zaščito, če jih sproti nadgrajujemo. Proizvajalci to ponavadi omogočajo samodejno in vsakodnevno preko interneta, zato sem v anketi naletel na odgovor, ki ga sicer nisem ponudil (posodabljanje vsak dan), pa vendar ugotavljam, da ga je bilo smiselno vključiti v grafikon, saj menim, da imajo vsakodnevno posodabljanje nameščeno skoraj vsi uporabniki (npr. protivirusnih programov), pa za to niti ne vedo.

6. vprašanje: Na katere težave v zvezi z varnostjo na medmrežju ste že naleteli?



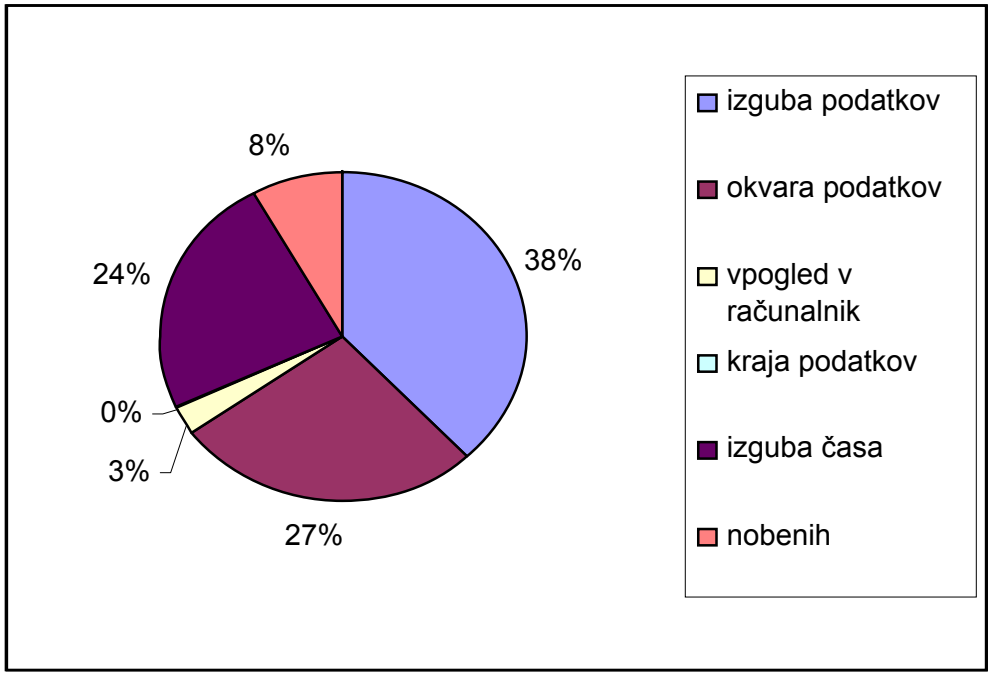
Grafikon 9: Prikaz rezultatov 6. vprašanja

Komentar h grafikonu 9:

31 anketirancem, kar predstavlja 39 %, je bila v njihov e-poštni predal že vsiljena neželena e-pošta. Pri tej e-pošti gre za zavajanje uporabnikov z oglaševanjem različnih storitev in izdelkov. Samo odstotek manj anketiranih je že naletelo na viruse. Ta rezultat **ni potrdil** moje **hipoteze**, da so največja nevarnost e-poslovanja danes virusi.

Nad tem rezultatom sem zelo presenečen, saj sem mnenja, da je vsak uporabnik na računalniški virus že naletel. Mislim, da se je večina anketiranih odločila za odgovor neželenega oglaševanja po e-pošti zato, ker jim njihove e-poštne predale dnevno polni in jih zato tudi najbolj moti.

7. vprašanje: Katere posledice bi pustila medmrežna prevara (npr. virus) v vašem računalniku?

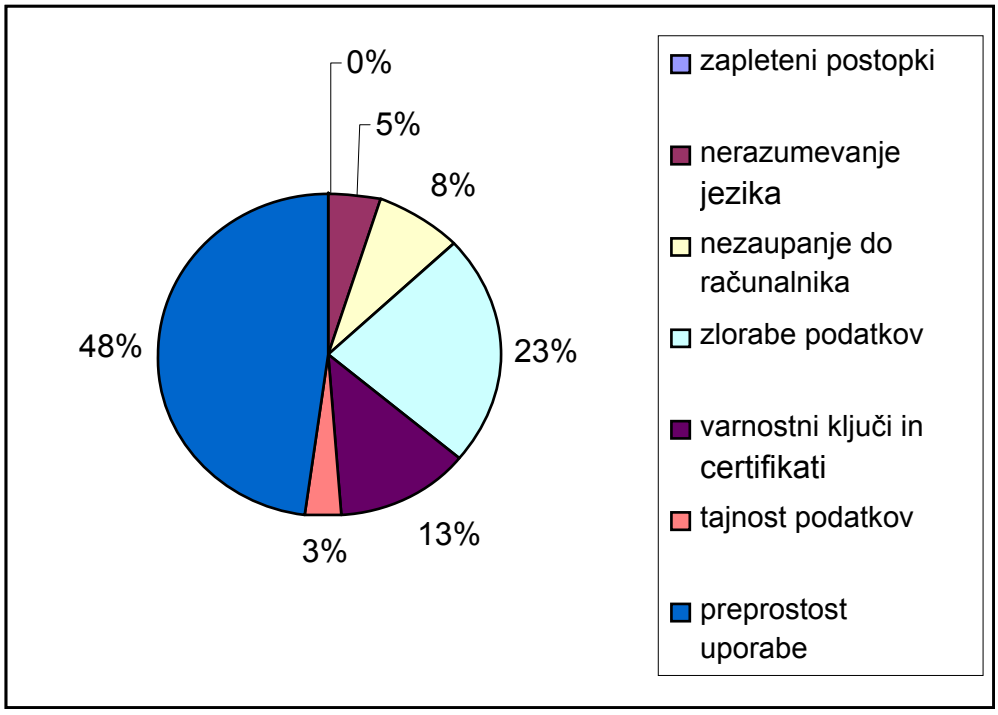


Grafikon 10: Prikaz rezultatov 7. vprašanja

Komentar h grafikonu 10:

Tokrat je pet anketirancev odgovorilo, da medmrežna prevara ne bi pustila nobenih posledic v računalniku. Gre za odgovor, ki ga v anketi nisem ponudil. 38 % anketiranih je zaradi medmrežne prevare izgubilo podatke, nikomur podatkov niso ukradli. 16 anketiranih, kar predstavlja 24 % vseh, vidi težavo predvsem v izgubi časa zaradi reševanja težav, ki jih povzroči medmrežna prevara.

8. vprašanje: Na čem temelji vaše zaupanje oziroma nezaupanje v uporabo storitev e-poslovanja?

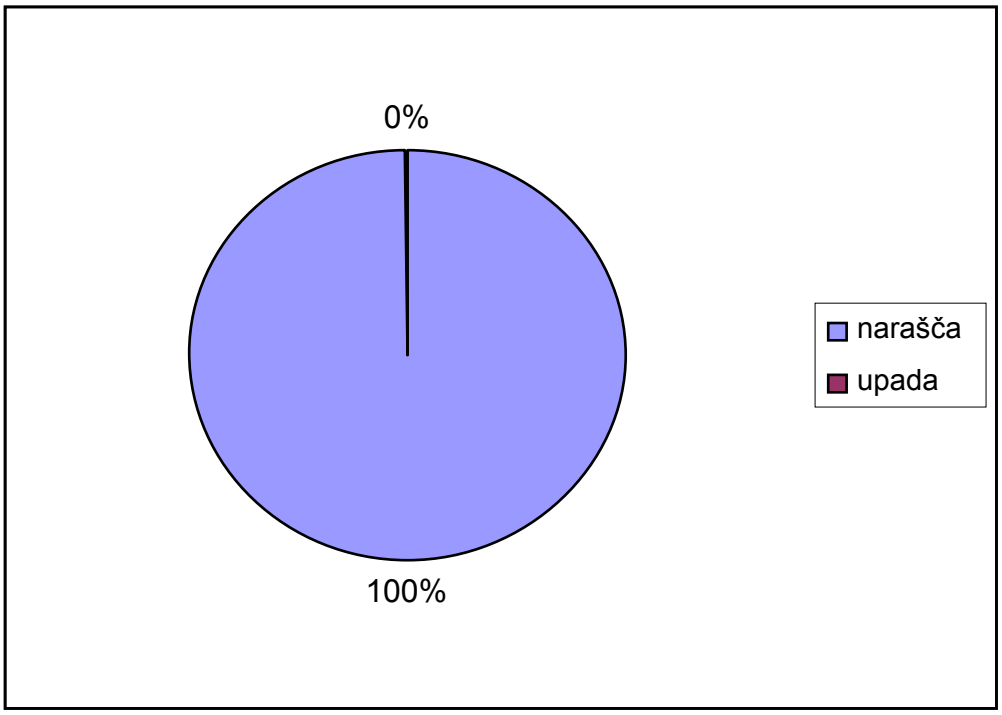


Grafikon 11: Prikaz rezultatov 8. vprašanja

Komentar h grafikonu 11:

Rezultati kažejo, da večina anketiranih zaupa v uporabo storitev e-poslovanja, saj jih je kar 28 posameznikov, oziroma 48 %, mnenja, da so postopki uporabe preprosti. Izstopajoči razlog, zakaj uporabi storitev e-poslovanja ne zaupajo, je bojazen pred zlorabo podatkov. Za ta odgovor se je odločilo 15 anketiranih, to je 23 %.

9. vprašanje: Kakšen je po vašem mnenju trend uporabe storitev e-poslovanja?



Grafikon 12: Prikaz rezultatov 9. vprašanja

Komentar h grafikonu 12:

Kakor prikazuje grafikon so vsi anketirani mnenja, da trend uporabe storitev e-poslovanj narašča. Statistike so pokazale približno 68 % letno rast razvoja e-poslovanja. Vendar pa lahko z vse večjim številom posameznikov, ki uporabljajo e-poslovanje, pričakujemo tudi povečanje števila zlorab in prevar.

Struktura anketiranih po spolu, starosti in izobrazbi:

Moški spol	Ženski spol
57 %	43 %

Tabela 3: Struktura anketiranih po spolu

Od 15 do 24 let	14 %
Od 25 do 44 let	36 %
Od 45 do 64 let	43 %
Nad 65 let	7 %

Tabela 4: Struktura anketiranih po starosti

Osnovna izobrazba ali manj	2 %
Nižja in srednja poklicna ali strokovna izobrazba	7 %
Srednja splošna izobrazba	44 %
Višja izobrazba	14 %
Visoka izobrazba ali več	33 %

Tabela 5: Struktura anketiranih po izobrazbi

7. SKLEP

V internet je danes povezanih na milijone računalnikov. Je največje svetovno omrežje podatkov in ljudi, ki te podatke nudijo ali uporabljajo. Vpliv interneta je čutiti v vseh pogledih našega življenja. Njegova uvedba je spremenila naš način dela, izobraževanja in zabave. Internet ponuja množico storitev, ki se uporabljajo za e-poslovanje, najbolj znani, priljubljeni in najpogosteje uporabljeni storitvi sta svetovni splet in e-pošta.

Stroka opredeljuje e-poslovanje kot elektronsko izmenjavanje podatkov med podjetji, državnimi javnimi službami in posamezniki. Nekatere raziskave so pokazale, da največji del e-poslovanja predstavlja e-poslovanje med podjetji, vendar pa se z večanjem dostopnosti fizičnih uporabnikov do interneta razvija tudi e-poslovanje s končnimi uporabniki. Internet zaenkrat uporablja 15 - 22 % svetovne populacije, zato je potencial razvoja še zelo velik.

Z uvedbo e-poslovanja je uporabnikom omogočeno opravljanje raznovrstnih storitev, kot so na primer kupovanje, prodaja, borzno poslovanje, plačevanje, izobraževanje, delo itd., kar od doma. Do informacij lahko dostopajo, jih uporabljajo in posredujejo z enostavnimi in nezapletenimi postopki. Nenazadnje zaradi tega ustvarijo velik prihranek tako časa kakor denarja.

Z vse večjim številom posameznikov, ki uporabljajo e-poslovanje, lahko pričakujemo povečanje števila računalniških zlorab in prevar. Oblik ogroženosti e-poslovanja in računalniškega kriminala je veliko. K prvim, torej oblikam ogroženosti e-poslovanja, prištevamo splošne grožnje in nevarnosti ter nesreče zaradi človeškega dejavnika, strojnih poškodb in okvar. **O računalniškem kriminalu pa govorimo, kadar gre za odkritje virusa, črva ali parazitnih programov v našem računalniku, krajo in zlorabo podatkov. Slednja za fizične uporabnike v Sloveniji predstavlja največjo nevarnost e-poslovanja. HIPOTEZA ŠT. 2, da so največja nevarnost e-poslovanja danes virusi, je na podlagi rezultata ankete ovržena.**

Seveda za vsako izmed oblik ogroženosti e-poslovanja in računalniškega kriminala obstajajo ustrezni varnostni ukrepi, ki jih morajo uporabniki dobro poznati, če želijo

zagotoviti varno in zanesljivo uporabo e-poslovanja. Kljub vsem varnostnim mehanizmom velja, da se največ vdorov v sisteme zgodi zaradi napak, nepozornosti in nepremišljenosti uporabnikov. Načeloma bi se moral vsak uporabnik e-poslovanja držati vsaj osnovnih varnostnih zapovedi. Nameščeno bi moral imeti najnovejšo različico protivirusnega programa in požarnega zidu, uporabljati bi moral najnovejšo različico operacijskega sistema ter zaupno ravnati z gesli.

Da so uporabniki po svetu dobro osveščeni o nujnosti zagotovitve varnosti e-poslovanja, in da delovanje računalniških sistemov in varnostnih mehanizmov dobro poznajo, potrjujejo rezultati mednarodnih statistik, ki kažejo, da je število prijavljenih in zabeleženih spletnih prevar v zadnjih dveh letih v strmem padanju.

HIPOTEZA ŠT. 1, da medmrežne prevare pri fizičnih osebah doma in po svetu v zadnjih letih strmo naraščajo, je delno potrjena, saj je število zabeleženih in prijavljenih spletnih prevar od leta 2006 do 2008 postopoma padalo.

Tudi domači uporabniki e-poslovanja v osveščenosti ne zaostajajo za svetom. Vsi uporabniki, ki sem jih vključil v analizo svoje raziskave, so odgovorili, da za varovanje pred medmrežnimi prevarami uporabljajo vsaj en varnostni mehanizem.

HIPOTEZA ŠT. 3, da fizični uporabniki za varovanje pred medmrežnimi prevarami najpogosteje uporabljajo protivirusne programe, je potrjena, saj večina anketiranih domačih uporabnikov e-poslovanja uporablja protivirusne programe, ki jih tudi redno nadgrajuje in posodablja.

Na koncu bi dodal še to, da bi bilo v raziskavo smiselno vključiti še ugotovitve na podlagi strukture anketiranih po starosti in stopnji izobrazbe. Podatki so zanimivi saj lahko iz le teh ugotovimo katere so ciljne skupine za osveščanje o smiselnosti varnosti elektronskega poslovanja. Raziskava je pokazala, da je e-poslovanje najpogostejše pri uporabnikih v starosti med 25 in 64 letom. Po strukturi stopnje izobrazbe pa ima večina anketirancev srednjo splošno izobrazbo in visoko izobrazbo ali več.

Iz teh rezultatov ugotavljam, da je tudi na ponujene anketne odgovore odločilno vplivala ta populacija. Tako lahko zaključim, da bi bilo o pomembnosti in smiselnosti varnosti elektronskega poslovanja osveščati predvsem to ciljno skupino uporabnikov.

Brez dvoma je internet ena izmed največjih iznajdb moderne družbe, in prišel bo čas, ko bo elektronsko poslovanje postalo edina oblika poslovanja.

8. UPORABLJENA LITERATURA, VIRI IN ELEKTRONSKI VIRI

Literatura:

1. Bratuša, T.: Hekerski vdori in zaščita. Ljubljana, Pasadena, 2006.
2. Egan, M.: Varnost informacij: grožnje, izzivi in rešitve. Ljubljana, Pasadena, 2005.
3. Emerčič, B., Ivanuša-Bezjak, M., Vinter, M.: Informatika v komercialnem poslovanju. Maribor, ACADEMIA-Višja strokovna šola Maribor, 2005.
4. Gradišar, M.: Uvod v informatiko. Ljubljana, Ekonomska fakulteta, 2003.
5. Gradišar, M., Resinovič, G.: Informatika v organizaciji. Kranj, Moderna organizacija, 1998.
6. Gradišar, M., Resinovič, G.: Informatika v poslovnem okolju. Ljubljana, Ekonomska fakulteta, 1996
7. Jerman Blažič, B.: Elektronsko poslovanje na internetu, Ljubljana, GV Založba, 2001.
8. Pavliha, M. Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. Ljubljana, GV založba, 2002.
9. Strebe, M., Perkins, C.: Firewalls-zaštita od hekera. Ljubljana, Kompjuter biblioteka, 2003.
10. Toplišek, J.: Elektronsko poslovanje. Ljubljana, Atlantis, 1998.

Viri:

11. Zakon o elektronskem poslovanju in elektronskem podpisu. Uradni list RS, št. 57/2000.
12. Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu. Uradni list RS, št. 25/2004.
13. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Uradni list RS, št. 77/2000, 2/2001.

Elektronski viri:

14. www.arnes.si/cert [28. 1. 2009]
15. www.metaling.si/varnost.php [28. 1. 2009]
16. www.netsi.net [28. 1. 2009]
17. http://www.cek.ef.uni-lj.si/u_diplome/radetic2532.pdf [25.02.2009]
18. http://www.siq.si/ [27.03.2009]
19. http://www.e-standard.si [10.03.2009]
20. http://cobit-tqmcintl.blogspot.com/ [10.03.2009]
21. http://en.wikipedia.org/wiki/COBIT [28.03.2009]
22. www.ris.org [10.03.2009]

PRILOGE

PRILOGA 1: Anketa

ANKETA

Pozdravljeni, sem Boris, študent Višje strokovne šole Academia iz Maribora. V okviru svoje diplomske naloge izvajam raziskavo z naslovom *Varnost elektronskega poslovanja fizičnih oseb v Sloveniji in svetu.* Vaše sodelovanje v anketi mi bo v veliko pomoč pri analiziranju raziskave. Anketa bo trajala 5 minut in je anonimna.

1. Koliko računalnikov imate v svojem gospodinjstvu? *(obkrožite samo en odgovor)*
   - 0
   - 1
   - 2
   - več
2. Ali imate v svojem gospodinjstvu dostop do interneta? *(obkrožite samo en odgovor)*
   - da
   - ne
3. Za katere storitve uporabljate internet? *(obkrožite lahko več odgovorov)*
   - bančne in finančne
   - izobraževanje
   - iskanje informacij
   - igranje iger
   - pošiljanje e-pošte
4. Katere oblike računalniške zaščite uporabljate v svojem gospodinjstvu? *(obkrožite lahko več odgovorov)*
   - protivirusne programe
   - požarni zid
   - posodobitev operacijskega sistema
   - geslo
   - protiparazitne komponente
   - elektronski podpis
5. Kdaj ste nazadnje posodobili katero izmed oblik zaščite? *(obkrožite samo en odgovor)*
   - nikoli
   - pred enim tednom
   - pred enim mesecem
   - pred pol leta
   - pred enim letom

6. Na katere težave v zvezi z varnostjo na medmrežju ste že naleteli? *(obkrožite lahko več odgovorov)*

- virusi
- črvi
- trojanski konji
- neželeno oglaševanje po e-pošti
- verižna pisma
- parazitni programi
- strojne okvare/poškodbe
- neprimerna oprema
- zloraba podatkov

7. Katere posledice bi pustila medmrežna prevara (npr. virus) v vašem računalniku? *(obkrožite lahko več odgovorov)*

- izguba podatkov
- okvara podatkov
- vpogled v računalnik
- kraja podatkov
- izguba časa zaradi reševanja težav

8. Na čem temelji vaše zaupanje oziroma nezaupanje v uporabo storitev e-poslovanja? *(obkrožite lahko več odgovorov)*

- zapleteni postopki
- nerazumevanje jezika
- nezaupanje do računalnika
- zlorabe podatkov
- varnostni ključi in certifikati
- tajnost podatkov
- preprostost uporabe

9. Kakšen je po vašem mnenju trend uporabe storitev e-poslovanja? *(obkrožite samo en odgovor)*

- narašča
- upada

Na koncu vas prosim še za nekaj osebnih podatkov:

10. Spol: M Ž

11. Starost:
    - od 15 do 24 let
    - od 25 do 44 let
    - od 45 do 64 let
    - nad 65 let

12. Dopolnjena izobrazba:
    - osnovna izobrazba ali manj
    - nižja in srednja poklicna ali strokovna izobrazba
    - srednja splošna izobrazba
    - višja izobrazba
    - visoka izobrazba ali več

Hvala za sodelovanje!