UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

NEVARNOSTI PRI ELEKTRONSKEM POSLOVANJU NA INTERNETU

Ljubljana, junij 2002 **ANDREJ ŽUPAN**

IZJAVA

Študent/ka _____ izjavljam, da sem avtor/ica tega diplomskega dela, ki sem ga napisala pod mentorstvom_____ in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne_____Podpis: _____

KAZALO

1. UVOD

Globalni informacijski splet, internet, medmrežje so imena, ki označujejo v mrežo povezane strežnike, delovne postaje in osebne računalnike. Postal je, ne samo ena od možnosti, temveč čedalje bolj nujnost za moderno komuniciranje med ljudmi, bodisi v poslovne, sprostitvene namene ali za ohranjanje stikov na osebni ravni. Kakor je razvoj tehnologije skozi zgodovino uveljavil v vsakdanji rabi kot nujnost telefon, televizor, osebni avtomobil in v zadnjem času mobilne telefone, tako je tudi na področju informacijskih storitev zaradi hitrosti, praktičnosti in nizkih stroškov internet izpodrinil običajne oblike poslovanja, komuniciranja in sorodnih storitev.

Internet se je razvil iz informacijskega omrežja ARPANET, ki so ga ZDA leta 1969 razvile za obrambne namene in se je kasneje, zlasti v poznih 1980-tih in 1990-tih razvil v globalni informacijski splet, ki omogoča dvosmerno povezavo med računalniki povezanimi v omrežje. Ta revolucija je omogočila nepojmljive možnosti, ki jih ta splet ponuja na klik miške oziroma tipke iz udobnega domačega naslonjača vsakemu uporabniku osebnega računalnika.

Internet, ki se je tako zlasti v zadnjem desetletju prejšnjega stoletja razvil v ˝gigantsko mesto˝ z milijoni uporabnikov dnevno, je postal izjemen medij za izvajanje različnih poslov, marketinških prijemov, poštnih storitev, zabavne industrije idr. Pred običajnimi potmi nudi številne prednosti od hitrosti, anonimnosti, nizkih stroškov, izjemne fleksibilnosti do visokega števila potencialnih ciljnih uporabnikov storitev.

Prav zaradi naštetih prednosti pa je internet postal tudi idealno gojišče za nepridiprave, ki so na vedno bolj kompleksnem in težko obvladljivem spletu uporabnikov in storitev, našli svojo priložnost bodisi za lahek zaslužek ali zgolj za izživljanje nad uporabniki in ponudniki storitev ter kaljenje svojega računalniškega znanja. Tako je v vsakdanje namene vedno bolj potrebna uporaba interneta postala vedno bolj tvegana dejavnost, ki zahteva uvajanje številnih etičnih načel pri njegovi uporabi, vpeljavo varnostne tehnologije in zakonsko regulacijo uporabe interneta podkrepljeno s strogo kazensko zakonodajo, ki mora zajemati izjemen obseg potencialnih kršitev in zlorab internetnih storitev, če hočemo vzdrževati sorazmerno visoko varnost za uporabnike in ponudnike spletnih storitev.

Cilj te diplomske naloge je osvetliti te šibke točke pri elektronskem poslovanju preko interneta in opozoriti na potencialne nevarnosti, ki na nas prežijo ob njegovih storitvah. Največji izziv pa bo spremljanje razvoja regulativne zakonodaje in kazenske zakonodaje za tovrstni kriminal, ki je še vedno v povojih in zahteva ponovno opredelitev pristojnosti regulativnih inštitucij, pomena termina svoboda govora in tiska ter varnosti osebnih podatkov, avtorskih pravic na področju digitalnih medijev, in še vedno naraščajoč obseg različnih oblik kršitev na spletu. V zadnji točki diplomske naloge pa se bom dotaknil perspektivnosti razvoja spleta kot varnega medija za prenos

elektronskih informacij, elektronskega poslovanja in drugih oblik komuniciranja po elektronski poti.

2. Šibke točke interneta pri zagotavljanju varnosti uporabnikov

Najpogostejše oblike tveganja pri uporabi interneta niso tiste, ki pritegnejo največjo pozornost medijev. Večina od nas ne bo nikoli imela opravka z zlobnimi crackerji[1], hackerji[2], vohuni, pedofili, itd. V resnici predstavljajo le-ti zelo majhen delež populacije na internetu.

Obstajajo pa bolj vsakdanje in praktične oblike tveganja pri uporabi interneta (Barrett, 1996, str. 2-3):

- Zasebna elektronska sporočila, ki jih pošiljate svojim prijateljem so lahko prestrežena in brana s strani nezaželenih posameznikov (ang. snooping).
- Nepošteni uporabniki lahko v vašem imenu zlorabljajo internetne storitve s tem, da se pretvarjajo, da ste to vi (ang. spoofing).
- Zavajajoči in lažni marketing se na internetu distribuira vsakodnevno.
- Nadležni uporabniki lahko tratijo vaš čas in denar s polnjenjem vašega elektronskega poštnega predala z nezaželeno in nenaročeno pošto (ang. spamming, junk mail).

Obstajajo številni razlogi, zakaj je internet tako atraktiven za številne prevarante. Ti razlogi izhajajo predvsem iz lastnosti interneta, ki jih ta poseduje in so tudi razlog za njegov razcvet (Barrett, 1996, str. 4).

1. Anonimnost

Osebe, ki zlorabljajo internet, lahko uspešno prikrijejo svojo identiteto, tako da se skrivajo za številnimi psevdonimi, zaradi česar jih je težko izslediti.

2. Veliko število novih uporabnikov

Internet stalno preplavljajo novi in novi uporabniki. Mnogi so v začetnem zagonu nepripravljeni in se ne zavedajo potencialnih nevarnosti. Če prevarant naredi napako in si pridobi slab renome,

[1] Cracker je navadno mladoletnik s povprečnim računalniškim znanjem, ki vdre v program ali sistem z ugibanjem gesla ali zlomom programske kode.

[2] Hacker-jem pa je, za razliko od cracker-jev, vdiranje v zasebna omrežja izziv, pri čemer ne kradejo, uničujejo ali spreminjajo podatkov. Posedujejo širok spekter računalniškega znanja in stremijo k izpopolnjevanju le-tega.

se zaveda, da bo splet v nekaj mesecih preplavljen z novimi uporabniki, ki niso zanj nikoli slišali.

3. Nizki stroški

Prvič v zgodovini lahko nekdo razširi neznanske količine ˝smeti ˝ v različnih oblikah, ki jih internet omogoča z neznatnimi stroški za pošiljatelja. Stroške in trpljenje navadno nosijo prejemniki.

4. Neskončna fleksibilnost interneta

Mnoge prevare poznane iz vsakdanjega življenja se lahko na podoben ali celo identičen način prenesejo na internet, pri čemer so mnoge zelo pretkane in rafinirane. Ko se le-te pojavijo na relativno mladem in težko obvladljivem mediju, kot je internet, jih je navadno težko hipoma prepoznati.

5. Lažen občutek skupnosti

Mnogi uporabniki interneta se med seboj praviloma poznajo le preko ekrana ali bolje rečeno preko tipkovnice. Rado jih zavede, da so si med seboj podobni in si lahko zaupajo, čeprav se niso nikoli osebno srečali. To zaupanje je v mnogočem temelj ugleda, ki ga internet uživa, vendar pa omogoča tudi ugodno okolje za številne potegavščine.

Večina ljudi in storitev, ki jih srečamo na internetu so legitimne. Vendar, če se lotimo interneta, ne da bi se zavedali potencialnega tveganja pri njegovi uporabi smo lahko nekega dne neprijetno presenečeni, ko ugotovimo, da smo postali žrtev prevare. Temna plat interneta je sicer skromna, vendar obstaja.

Internet pozna številne oblike komuniciranja, ki predstavljajo potencialno tveganje za uporabnike internetnih storitev. Najbolj razširjeni obliki uporabe interneta pa sta gotovo elektronska pošta in svetovni splet, katerima v nadaljevanju tudi posvečam največ pozornosti.

2.1 Tveganja pri uporabi elektronske pošte

Elektronska pošta predstavlja najbolj razširjeno obliko komuniciranja preko interneta. Lahko bi rekli, da je križanec med običajno pošto in telefonskim klicem (Barrett, 1996, str. 6). Glavna prednost elektronske pošte pred običajno (ang. snail-mail) je predvsem hitrost.

V ustreznem programu ali pa na spletnih straneh servisov, ki ponujajo storitve elektronske pošte, sestavimo sporočilo, ki ga želimo poslati nekemu drugemu uporabniku internetnih storitev.

Ker se zdi, da elektronsko sporočilo potuje neposredno od pošiljatelja k naslovniku, ljudje mnogokrat napačno predpostavljajo, da je le-to opravljeno diskretno. Vendar temu ni tako, saj je lahko sporočilo na svoji poti prestreženo, brano, modificirano ali uničeno s strani drugih uporabnikov spleta. Prav tako se lahko zgodi, da nekdo v vašem imenu pošilja elektronsko pošto in se tako pretvarja, da ste to vi. Nezaželena pošta vam lahko ukrade veliko časa, denarja in računalniških virov (prostor na disku npr.). Zasipavanje predalov elektronske pošte nič hudega slutečih lastnikov z nezaželeno oziroma nenaročeno pošto imenujemo spamming. Elektronska pošta se lahko kdaj tudi izgubi v tranzitu in s tem povzroči nesporazum med uporabniki, ki skušajo skleniti posel. S posebnim programom (ang. packet sniffer) lahko vsakdo že med tipkanjem sporočila pridno prebere vašo pošto, seveda, če ste pri tem priključeni na internet.

Pri vsem tem upravičeno predpostavljamo, da se ponudniki internetnih storitev in/ali upravljalci na spletnih straneh, ki ponujajo elektronske poštne predale vedejo odgovorno in ne berejo pošte oziroma sporočil njihovih uporabnikov. Glede na to, da je internet izjemno obsežen, je verjetnost, da bo posamezna elektronska pošta tarča nepovabljenih bralcev izjemno majhna. Kljub temu pa ne smemo predpostavljati, da je zato pošiljanje elektronske pošte popolnoma diskretno. Če smo prisiljeni po elektronski pošti pošiljati zaupne osebne podatke nam popolne diskretnosti elektronska pošta ne more zagotavljati. To velja tako za pošiljanje osebnih podatkov kot podatkov o kreditni ali plačilni kartici. Še največjo varnost nam omogoča šifriranje elektronskih sporočil.

Druge oblike nevarnosti, ki predstavljajo večjo grožnjo za uporabnike elektronske pošte in lahko pustijo za sabo pravo opustošenje na programski opremi uporabnika in mu onemogočajo opravljanje njegove dejavnosti so tako imenovani virusi, črvi in trojanski konji. Ti omogočajo tretji osebi spremljanje uporabnika, dostop do računalnika prejemnika elektronske pošte, povzročajo izgubo podatkov in ustvarjajo varnostne luknje v sistemu. Ti se navadno skrivajo v pripetih datotekah v elektronski pošti ali številnih prosto dostopnih programih na spletnih straneh interneta.

2.1.1 Anonimno pošiljanje elektronske pošte

Problem diskretnosti pri pošiljanju elektronske pošte lahko razrešimo, če pošiljamo le-to anonimno. Na ta način lahko preprečimo, da se naš poštni predal zasuje s številnimi nezaželenimi elektronskimi sporočili. Relativno varno rešitev predstavljajo brezplačni servisi za elektronsko pošto, ki jih najdemo na spletnih straneh.

Popolno anonimnost pa po drugi strani zagotavljajo strežniki za elektronsko pošto, ki posredujejo sporočila elektronske pošte pri čemer odstranijo podatke o njihovem pošiljatelju (ang. remailer). Sporočilo se s takšnega poštnega strežnika pošilja naprej na številne strežnike elektronske pošte, ki spreminjajo vnose v glavi sporočila. Ker je tudi povezava na spletno stran zakodirana smo tako varni tudi pred radovednimi očmi sodelavcev, nadrejenih, upravljalca v podjetju, kjer delamo ali ponudnika internetnih storitev (ISP).

2.1.2 Kriptiranje elektronske pošte s programskim paketom PGP (Preety Good Privacy)

Kadar nam je v interesu popolnoma zaščititi izvor elektronske pošte in njegovo vsebino, je idealna rešitev kriptiranje elektronske pošte. Najbolj učinkovita in najširše uporabljena tehnologija za kriptiranje je PGP (Shimmin, 1997, str. 240).

Avtor PGP tehnologije kriptiranja podatkov je Phil Zimmerman. Prvo verzijo svoje tehnologije, tedaj le za kriptiranje elektronskih sporočil, je predstavil junija leta 1991.

PGP je tehnologija asimetričnega kriptiranja podatkov in spada v domeno tehnologij kriptiranja z javnim ključem (ang. Public key Cryptography). Pri kriptiranju te oblike se uporabljata zasebni (ang. private key) in javni ključ (ang. public key), pri čemer se javni ključ uporablja za kriptiranje poslanih sporočil, kar je tudi značilno za vse tehnologije kriptiranja z javnim ključem. Ker pa gre hkrati tudi za tehnologijo asimetričnega kriptiranja podatkov, sta ključa za kriptiranje in dekriptiranje podatkov med seboj različna

Prednosti kriptiranja podatkov s PGP tehnologijo so v zagotavljanju varnostnih storitev, ki omogočajo sledeče (Schneier, 1995, str. 134):

- zaupnost in tajnost podatkov,
- zanesljivo identifikacijo pošiljatelja,
- ohranjanje celovitosti podatkov ter
- nezatajljivost izvora / pošiljatelja.

PGP tehnologija, ki jo mnogi imenujejo že kar OpenPGP standard, so na široko sprejela številna podjetja in servisi za elektronsko pošto kot je Hushmail (Hushmail. [URL: http://www.hushmail.com], 15.2.2002). Uporaba teh storitev je brezplačna, zahteva pa nalaganje (ang. download) manjšega programa s spletne strani, ki je namenjen za kriptiranje in dekriptiranje elektronske pošte in ustreza OpenPGP standardu, ki ga servis na svoji spletni strani uporablja. Potencialni uporabnik storitev mora v naslednjem koraku ročno ali avtomatsko kreirati svoje uporabniško ime in določiti svoje geslo. Hushmail nato kreira posebna ključa za kriptiranje ali

podpisovanje elektronske pošte uporabnika, ki sta edinstvena. Če kdorkoli prestreže sporočilo, ki je kodirano s ključem pošiljatelja in ključem prejemnika bo razbral zgolj nerazumljivo sporočilo. Enkripcijski program PGP celo omogoča pošiljatelju, da z javnim ključem, ki je značilen samo zanj, digitalno podpiše poslano sporočilo, tako, da ga lahko prejemnik nedvoumno identificira, kot pošiljateljevega. Edina omejitev, ki jo tak enkripcijski program predstavlja je, da morata biti tako pošiljatelj kot prejemnik kriptiranega sporočila uporabnika programskega paketa PGP.

Vendar pa je tudi tak asimetrični način kriptiranja podatkov deležen precejšnjih kritik, glede patentnih pravic v zvezi s kriptografijo z javnimi ključi (ang. public key cryptography), ter zaradi njegove neustreznosti glede prilagajanja zunanjetrgovinski zakonodaji ZDA. Do leta 1999 se je PGP tehnologija, kakor tudi vsa kriptografska tehnologija, obravnavala kot potencialno nevarno orožje, ki bi v nepravih rokah lahko ogrožalo nacionalno varnost in je zanj veljala prepoved izvoza iz ZDA, sam avtor pa je bil kar tri leta podvržen sodni obravnavi.

2.1.3 Nenaročena in nezaželena elektronska pošta

Eden najbolj pestečih problemov vseh uporabnikov elektronskih poštnih predalov, upravljalcev strežnikov ponudnikov internetnih storitev in spletnih strani so prav gotovo neželena elektronska sporočila, zlasti reklamna sporočila, verižna pisma in različna zlonamerna elektronska pošta.

Nič hudega slutečim žrtvam troši čas, živce in računalniške kapacitete, zlasti pomnilniške, kot je prostor v elektronskem poštnem predalu. Zaščita pred tovrstno nadlogo je sila težavna, saj praviloma taka sporočila ne nosijo nekega skupnega imenovalca, po katerih jih je moč prepoznati in ukiniti.

Praviloma učinkuje le prilagoditev programske opreme s tako imenovanimi filtri. V ustreznih programih za elektronsko pošto družb Microsoft in Netscape, deluje tako filtriranje tako, da določimo pravilo (ang. rule). Tako lahko sprejeta sporočila omejimo npr. na tista, ki v svoji glavi ali vsebini ne vključujejo določenih besed ali znakov. Lahko pa tudi kar konkretno blokiramo naslove neželenih pošiljateljev.

Take oblike filtriranja prejetih sporočil pa navadno niso najboljša rešitev, saj lahko s tem nehote preprečimo sprejem sporočil, ki niso nezaželena.

Povprečni uporabnik, ki ima poštni predal na kakšnem brezplačnem strežniku, se sam sicer težko bojuje proti zasipavanju z neželeno pošto, čeprav so nekateri poštni strežniki že precej dobro izpopolnili filtrirni sistem, ki ga vsak uporabnik lahko tudi prikroji svojim potrebam.

Najboljša zaščita pred neželeno pošto je prav gotovo previdnost pri tem, komu vse razkrivamo svoj elektronski naslov. Najučinkoviteje se otepamo neželene pošte, če se držimo sledečih napotkov (Shimmin, 1997, str. 217):

- ne odgovarjajmo na verižna pisma,
- ne odgovarjajmo na reklamna sporočila,
- ne vključujmo predogleda neželenih sporočil, ki so v obliki HTML, saj s tem potrdimo veljavnost svojega naslova,
- Pri naročanju na biltene z novicami (ang. newsletters) uporabljajmo po možnosti kak brezplačen naslov in ne svojega zasebnega,
- na svojih spletnih straneh ne objavljajmo osebnih elektronskih naslovov in
- čim manj obiskujmo in se zadržujmo na pornografskih in piratskih straneh.

Po podatkih spletne strani Computer mail services je ekonomska škoda, ki jo utrpijo podjetja zaradi nezaželenih in nenaročenih sporočil, odvisna od števila osebnih računalnikov v lokalnem omrežju podjetja oziroma zaposlenih in od števila dnevno prejetih neželenih sporočil. Povzročena škoda vključuje izgubljene delovne ure zaradi odpravljanja posledic in finančno izgubo ali strošek zaradi onemogočanja poslovanja podjetja.

Tabela 1: Prikaz odvisnosti stroškov podjetja od števila prejetih neželenih sporočil

ŠTEVILO ZAPOSLENIH	ŠT.DNEVNO PREJETIH NEŽELENIH SPOROČIL	ŠT. IZGUBLJENIH UR LETNO	LETNA IZGUBA (V USD)
100	500	160	4,000
1000	5000	1600	40,000
5000	25000	8000	200,000

Vir: Computer mail services: Spam cost calculator.
[URL: http://www.cmsconnect.com/Marketing/spamcalc.htm], 10.5.2002.

2.1.4 Zasipavanje strežnikov z neželeno pošto

Z Dos napadi (ang. Denial of Service attack) se označuje zasipavanje strežnikov z različnimi zahtevki po opravljanju storitev, informacijami ali elektronskimi sporočili z namenom onemogočiti delovanje strežnika in s tem onemogočanje izvajanja storitev upravljalcem strežnika.

V primeru Dos napadov z elektronsko pošto je cilj napadalcev z verižnimi pismi, sporočili, ki vsebujejo opozorila pred virusi, pismi, ki iščejo sočutje in podporo, in ostalimi pismi, katerih

namen je izzvati množenje elektronskih sporočil, da onesposobijo poštni strežnik ali delovanje katere izmed spletnih strani.

Pri distribuiranih napadih na tuje sisteme (ang. Distributed Denial of Service attack) pa je žrtev praviloma več, saj napadalec najprej okuži in komprimitira delovanje več strežnikov, ki nato družno zasipavajo ciljno spletno stran ali poštni strežnik z množečo se elektronsko pošto z namenom onesposabljanja delovanja le-tega.

2.1.5 Virusi, črvi in trojanski konji v pripetih datotekah elektronskih sporočil

Računalniške programe, ki so namenoma napisani za ustvarjanje škode delimo na štiri skupine (Ahuja,1997, str. 18-19):

- računalniški virusi,
- črvi,
- trojanski konji,
- programske bombe.

Računalniški virusi in trojanski konji potrebujejo gostitelja, ostala dva pa ne, saj sta samostojna programa. Kot gostitelj, v katerem lahko domuje virus, lahko služi programska ali podatkovna datoteka, zagonski sektor na disketi ali disku. Značilno za računalniške viruse in črve je tudi, da se razmnožujejo sami. Trojanski konji in programske bombe se navadno same ne razmnožujejo.

Virusi so tako samorazmnoževalni programi, ki lahko okužijo in uničujejo druge programe. Za viruse je značilno, da se na svojem uničevalnem pohodu ob vsaki okužbi množijo.

Črv (ang. worm) je programček, ki se s kopiranjem samega sebe razmnožuje po računalniških sistemih običajno preko omrežja. Črv zaganja druge programe, ne spreminja pa datotek ali sektorjev na diskih. Značilno zanj je, da ne napada drugih programov, vendar pa lahko zasede veliko količino računalniških virov.

Trojanski konj je koda, navadno uničevalna, ki je vsajena v nek računalniški program (običajno črva) z namenom opravljanja prikrite dejavnosti. Kot tak, se trojanski konj skriva v jedru drugega programa in ni samostojen program. Tako kot pri mitološkem trojanskem konju, tudi pri teh računalniških programih od zunaj ne opazimo, da programi vsebujejo škodljivo jedro. Običajno se sami ne razmnožujejo. Primeri škodljivega delovanja:

- poškodujejo ali uničijo podatke na pomnilniških pogonih,

- omogočajo skrivno upravljanje žrtvinega računalnika na daljavo (preko interneta),
- upravljalec od daleč briše, kopira, ustvarja, nadzoruje strojno opremo, itd.

Programske bombe so samostojni programi, sicer namenjeni opravljanju nekega koristnega dela, ki pa imajo nekje v svojem jedru skrito škodljivo kodo, ki se aktivira, ko so izpolnjeni neki pogoji. Glede na tip teh pogojev jih delimo na časovne in logične. Napisane so lahko zaradi maščevanja in izsiljevanja ali pa zgolj iz nagajivosti. Bombe se ob izpolnitvi določenega pogoja (logične bombe) ali pa ob določenem času (časovne bombe) sprožijo in povzročijo uporabniku podatkovno škodo ali pa mu vsaj načnejo živce.

Na tem mestu bom omenil še programe imenovane bakterije (ang. bacteria), ki niso napisani z namenom povzročati fizično škodo na programih, vendar pa zaradi svoje narave brezmejnega razmnoževanja lahko povzroči tako imenovane Dos napade (ang. Denial of Service), pri čemer zaradi zasedanja računalniških zmogljivosti onemogoča ali resno ovira izvajanje dejavnosti uporabnikom, ki postanejo žrtve takega napada.

Potencialno nevarnost za zlorabo predstavljajo tudi stranska vrata (ang. trapdoor) v programih, ki jih programerji ustvarijo za osebno rabo z namenom kasnejšega preoblikovanja ali izpopolnjevanja programa (odpravljanje napak). So prikrite narave in razen programerja nihče ne ve zanje. Taka vrata zaobidejo običajne zaščite, ki jih program uporablja, in s tem lahko postanejo potencialna tarča za vdore v sistem.

Najnevarnejše oblike računalniških programčkov z namenom povzročanja škode ali vdiranja v sisteme so kombinirani vsiljivci. To so npr. črvi, ki v svojem jedru nosijo uničevalno kodo oz. trojanskega konja. Če pa na svojem pohodu delajo še škodo na programski opremi, imate pred sabo popoln hibrid virusa/črva/trojanskega konja.

Poleg zlonamernih škodljivcev obstajajo tudi drugi, ki občasno povzročijo škodo nenamerno. Sem spadajo hrošči (ang. bug). Le-ti so napaka v izvornem besedilu programske opreme, ki jo je programer nenamerno zagrešil.

Ekonomsko škodo, ki jo vsakoletno na svetovni ravni povzročijo virusi, črvi in trojanski konji, vrednotijo v milijonih in celo milijardah dolarjev. Tako so npr. po podatkih raziskav spletne strani Computer Economics v letih od 1999 do 2001 sledeči virusi ali črvi povzročili naslednjo ekonomsko škodo:

Tabela 2: Ekonomska škoda povzročena zaradi virusnih okužb

Leto	Vrsta okužbe	Ekonomska škoda v svetu (v mia USD)
2001	Nimda	0.64
2001	Code Red	2.62
2001	SirCam	1.15
2000	Love Bug	8.75
1999	Melissa	1.10
1999	Explorer	1.02

Vir: Computer economics security review 2002.
[URL: http://www.computereconomics.com/article.cfm?id=356], 10.5.2002.

Tabela 3: Rast ekonomske škode v svetu povzročene zaradi virusnih okužb v letih od 1995 do 2001

Leto	Ekonomska škoda v svetu (v mia USD)
2001	13.2
2000	17.1
1999	12.1
1998	6.1
1997	3.3
1996	1.8
1995	0.5

Vir: Computer economics security review 2002.
[URL: http://www.computereconomics.com/article.cfm?id=356], 10.5.2002.

Metod, ki jih je Computer economics uporabljal pri meritvah ekonomske škode, ne navaja, se pa ponekod sklicuje na poročila podjetij, ki so ekonomsko škodo zaradi okužb utrpela.

2.1.6 Preventivni ukrepi pred virusi, črvi in trojanski konji v pripetih datotekah elektronskih sporočil

V primeru, da z elektronskim sporočilom dobite pripete k le-temu številne datoteke, katerih izvor vam ni znan, je potrebna velika previdnost pri odpiranju teh datotek, saj lahko predstavljajo viruse, črve, trojanske konje, ki omogočajo tretjim osebam dostop do vašega računalnika. V kolikor ne veste, zakaj dobivate neko datoteko, je bolje povprašati pošiljatelja, kaj vam je poslal, kot pa imeti težave. Pri tovrstnih vdorih so različne oblike zaščite dokaj neučinkovite, zato le-ti letno napravijo na svetovni ravni največ škode, npr. virus ILOVEYOU, črv NIMDA, itd.

Najbolje se zavarujemo, če redno posodabljamo kvaliteten antivirusni program, ki je naložen na našem računalniku in je vedno delujoč v ozadju, tako, da lahko tekoče opozarja ob morebitnih vdorih virusov, črvov, trojanskih konjev. Kljub temu pa nastajajo skoraj dnevno novi škodljivci, katerim antivirusni programi ne bodo kos.

Dobro zaščito pred virusi predstavljajo tudi javni strežniki, ki nudijo storitev elektronske pošte, saj samodejno preverjajo sporočilom prepete datoteke s kvalitetnimi antivirusnimi programi.

Večina črvov za širjenje uporablja poštne programe družbe Microsoft. Pomembno je namestiti vse popravke programov, ki jih je objavil Microsoft na svojih spletnih straneh, saj nekateri črvi za širjenje izkoriščajo prav napake v programih.

Če je le možno, se je v elektronski pošti potrebno izogibati priponam**.** Dokumente, razen če vsebujejo oblikovanje, lahko pošljemo kot vsebino sporočila, namesto oblike .doc (MS Word dokument) pa jih lahko shranimo kot .rtf (obogateno besedilo). Pri dokumentih v formatu .rtf gre za dejansko običajen dokument v ASCII kodi, ki je obogaten s posebnimi ukazi, ki določajo obliko dokumenta.

Tvegano je zlasti odpiranje pripon s podaljški vbs, shs ali pif. Večina črvov se skriva v podaljških s takim imenom. Enako velja tudi za pripone z dvojnimi podaljški.

Na slovenskem internetnem trgu je edinstveno zaščito pred vdori virusov ponudilo podjetje KABI, ki nudi javni servis protivirusnega pregledovanja elektronske pošte. Storitev tega servisa deluje tako, da se vsa vhodna in po želji tudi izhodna pošta preusmeri čez javni protivirusni strežnik, ki preveri vsebino priponk s protivirusnim programom F-Secure Anti-Virus, ki vsebuje kar tri sočasne protivirusne pregledovalne sisteme: F-PROT, AVP in Orion. Poleg tega lahko program blokira nezaželene datoteke (*.VBS, *. PIF,…), tako, da so uporabniki varni tudi pred morebitnimi novimi virusi in črvi. Pošiljatelj in prejemnik prejmeta sporočilo z informacijo o tem, kateri virus je bil v poslanem sporočilu in kdo je pošiljatelj oziroma naslovnik. Podatki o novih virusih in črvih se osvežujejo vsako uro neposredno z osrednjega podatkovnega strežnika podjetja F-secure.

2.2 Tveganje uporabnikov svetovnega spleta

Najobsežnejši, najfleksibilnejši in najširše uporabljen način izkoriščanja internetnih virov predstavlja tako imenovani svetovni splet (www), kjer so internetni podatki organizirani v obliki spletnih strani, ki vključuje tekst, sliko in zvok. Za dobesedno listanje po neskončnem številu spletnih strani potrebujemo brskalnik (ang. browser). S pomočjo takega preprostega vmesnika lahko poljubno krmarimo skozi morje spletnih strani zgolj z uporabe miške.

Svetovni splet tako predstavlja najobsežnejše stičišče ponudnikov različnih storitev in njihovih uporabnikov. Ker tak splet predstavlja dobesedno trg ponudnikov in potrošnikov na najbolj enostaven, fleksibilen, poceni in vsestranski način, je kot tak tudi izvor številnih tveganj, ki so vsakodnevno prisotna na običajnih trgih ponudnikov in potrošnikov, pri čemer so mnoge oblike tveganja zaradi samih značilnosti svetovnega spleta še bolj raznovrstna in težje obvladljiva.

2.2.1 Zasebnost na svetovnem spletu

Med aktivnostjo na svetovnem spletu, se več ali manj izpostavljamo različnim tveganjem. Najbolj razširjena nevarnost je seveda okužba z virusom. Pogostokrat se zanemarja možnost vdora, ko nekdo prevzame nadzor nad našim računalnikom in ima tako dostop do podatkov na naših pomnilniških medijih. Še najmanj pa smo uporabniki pozorni na to, da spretni upravljalci spletnih strani beležijo podatke o naših obiskih. Varnost zasebnih podatkov na elektronskih medijih je v zadnjem času zlasti v tujini zelo vroča tema.

Splet je izredno orodje za spremljanje navad kupcev oziroma obiskovalcev spletnih strani, kar pa za kupca ni vedno slabo. Upravljalec spletnih strani lahko ugotovi, kako se obiskovalci gibljejo po straneh ter zgradbo spletne trgovine prilagodi kupcem. Prav tako lahko ugotovi nakupovalne navade kupcev in s tem kupcu lažje ponudi dodatne izdelke in storitve. Stvar je nekoliko podobna prodaji po pošti, kjer že leta uporabljajo različne profile kupcev za izboljšanje svoje ponudbe in poslovne uspešnosti. Tudi kartice zvestobe, ki jih ponujajo različni prodajni centri so namenjene temu.

Težava je v tem, da se razni zasebni podatki vztrajno zbirajo. Povezuje jih lahko IP (ang. Internet Protocol) številka, vaš naslov elektronske pošte ali pa piškotki (ang. cookies). Ko nekdo poveže podatke iz različnih podatkovnih zbirk, lahko npr. ugotovi, da večkrat kupujete določeno zdravilo in s tem že sklepa o vašem zdravju. Kaj, če bi tovrstne informacije lahko kupila vaša zavarovalnica ali vaša banka? Kdor se potrudi, lahko zgolj iz podatkov o spletnih straneh, ki ste jih obiskali, ali o ključnih besedah, ki ste jih vpisali v iskalnike, sklepa o vaših interesih, aktivnostih in identiteti. Dejansko ne obstaja omejitev pri količini podatkov, ki jih je moč zbrati na internetu o uporabnikih samih.

Aktivnosti na spletu, ki ogrožajo zasebnost:

1. Članstvo na različnih brezplačnih spletnih servisih

Ti servisi velikokrat zahtevajo osebne podatke, ki jih kasneje tudi delijo z drugimi ali prodajo drugim. Preverite navedbe ponudnika servisa o varovanju podatkov. Ponavadi so ustrezno

varovane spletne strani tudi ustrezno označene, da ščitijo uporabnika pred zlorabo zasebnih podatkov (ang. privacy policy).

2. Uporaba kreditnih kartic na spletu

Uporaba kreditnih kartic na spletnih straneh, ki imajo jasno in dobro varnostno politiko, ni nevarna, zato vedno preverite, komu zaupate številko svoje kreditne kartice in kako to podjetje varuje podatke. Vedno preverite, da se pri pošiljanju podatkov o kartici vaš brskalnik nahaja v varnem načinu (SSL). To se vidi že po protokolu, ki je zapisan v lokaciji, ki jo odpirate. Varne spletne strani namesto protokola http:// uporabljajo varni https:// protokol..

3. Uporaba chata, IRC-a, itd.

Pri prijavi na spletne IRC klepetalnice vam lahko ukradejo geslo. Klasični IRC programi, kot je mIRC, pa omogočajo tudi nekaj možnosti za vdor ter sprejem nevarnih programov.

2.2.2 Prventivni ukrepi za ohranitev zasebnosti na spletu

Vsi brskalniki po spletnih straneh shranjujejo podatke o obiskanih straneh ter kopije zadnje obiskane strani. Pri nekaterih lahko izklopimo možnost shranjevanja vsebine obiskanih strani. Najenostavneje je uporabiti enega od programov za brisanje zgodovine obiskanih strani. Večina boljših tovrstnih programov omogoča tudi brisanje piškotkov. To je zelo pomembno, saj na ta način dobimo vedno znova nov piškotek in s tem naših posameznih obiskov ene strani ne morejo povezati. Najlažje bi bilo piškotke izklopiti kar v brskalniku, vendar jih uporablja vse več spletnih servisov in v določenih primerih so nujni, saj omogočajo lažje elektronsko nakupovanje (spletne košarice ipd.).

Z brisanjem piškotkov se tudi izognemo možnosti, da nas spremljajo podjetja kot so DoubleClick ali Engage Technologies. Ta podjetja namreč ponujajo spletnim oglaševalcem možnost spremljanja, katere oglase (ang. banner) gledajo obiskovalci. Pred časom je DoubleClick navedel, da želi povezati te informacije o spletnih navadah preko 100 milijonov uporabnikov z imenskimi podatki oziroma podatki o elektronski naslovih.

Najosnovnejšo zaščito omogočajo že programi za blokiranje in izklapljanje oglasov ter reklamnih sporočil. Podobne storitve nudijo mnogokrat brezplačno tudi na spletnih straneh (Guidescope. [URL: http://www.guidescope.com], 20.2.2002).

Skrajni načini zaščite vključujejo tudi brskanje po spletu preko oddaljenega strežnika (Anonymizer. [URL: http://www.anonymizer.com], 20.2.2002). Tak strežnik (ang. proxy) nam

služi kot posrednik pri krmarjenju po spletnih straneh, saj preko njega naslovimo zahtevo po brskanju na določeni spletni strani. V tem primeru, vsaj kar se tiče spletne strani, jo je obiskal zgolj oddaljeni strežnik. Sled do dejanskega brskalca je tako zabrisana. Tak način anonimnega brskanja ima tudi svojo ceno, kot je počasnejše odpiranje spletnih strani, saj morajo podatki prepotovati dvojno pot preden dosežejo uporabnika.

3. Požarni zid – zaščita pred vdori v zasebna omrežja

Z naraščajočim obsegom interneta in storitev, ki jih ponuja, narašča tudi število potencialnih vdorov in namenov vdora v lokalna omrežja ponudnikov internetnih storitev, organizacij, inštitucij in podjetij. Z namenom zaščite zasebnih omrežij pred vdori, prisluškovanji, krajo podatkov in onemogočanjem opravljanja svojih dejavnosti je potrebno vzpostaviti ustrezen varnostni sistem.

Varnostni sistem, imenovan požarni zid (ang. firewall), se vzpostavlja z namenom prestrezanja informacij oziroma prometa med lokalnim omrežjem in prostranstvi interneta. Namen požarnega zidu ni zgolj zaščita pred nepovabljenimi gosti, temveč tudi prestrezanje pomembnih podatkov o uporabniku/ih lokalnega omrežja, ki jih lokalno omrežje posreduje v internet. To so mnogokrat lahko zaupne informacije podjetja, ki bi lahko bile usodne za uspešno poslovanje podjetja.

Požarni zid v grobem služi naslednjim namenom (Chapman, Zwicky, 1995, str. 4):

- omejuje vstop v lokalno omrežje v dobro nadzorovanih točkah (vratih),
- preprečuje potencialnim vsiljivcem dostop do ostalih zaščit sistema ter
- omejuje izstop iz lokalnega omrežja v internet v dobro nadzorovanih točkah (vratih).

Logično in analitično gledano je požarni zid ločevalec in razmejevalec med zaupnim lokalnim omrežjem in internetom. Pogostokrat pa se požarni zid uporablja kot razmejevalec različnih delov omrežja z različnimi varnostnimi zahtevami znotraj zasebnega omrežja. Pogostokrat je to takrat, ko si omrežje delijo subjekti z različnimi pristojnostmi in se s tem omejuje dostop do določenih baz nepooblaščenim osebam znotraj omrežja.

Fizična implementacija požarnega zidu se navadno razlikuje od omrežja do omrežja. Najpogosteje je požarni zid vzpostavljen s strojno in programsko opremo ali pa so to omrežja z ustrezno varnostno programsko opremo.

Podjetje se lahko odloči ali bo samo zgradilo požarni zid ali pa bo poseglo po že obstoječih komercialnih rešitvah. Slednje, ki so navadno v obliki programskih paketov so cenejše, vendar praviloma ne upoštevajo specifičnih značilnosti in lastnosti posameznega omrežja, kjer se vzpostavlja požarni zid.

Izgradnja lastnega požarnega zidu je učinkovitejša, v večini primerov boljša rešitev, ki pa je tudi dražja, saj zahteva najetje strokovnjakov izvajalcev za njegovo izgradnjo.

Kljub temu, pa kvalitetni požarni zidovi vzpostavitev katerih predstavlja lahko precejšen strošek, ni brez pomanjkljivosti. Ni ga varnostnega sistema, ki bi ponujal popolno zaščito pred vsemi mogočimi nevšečnostmi, katerim je zasebno omrežje izpostavljeno.

Požarni zid nudi odlično zaščito pred zunanjimi vsiljivci, vendar pa ne more nič zoper zlonamerne posameznike, ki so že znotraj požarnega zidu. Ravno tako ne more nuditi zaščite pred povezavami, ki zaobidejo požarni zid. Včasih strokovno podkovani posamezniki (zaposleni) ali upravljalci sistema vzpostavijo neodvisno telefonsko- modemsko povezavo skozi zadnja vrata v omrežje. Tu gre za problem upravljanja s človeškimi viri in ne za tehnični problem.

Ravno tako nas lahko požarni ščit varuje zgolj pred znanimi oblikami groženj. Pojavljajo pa se vedno nove oblike napadov pri vdorih v omrežja, tako, da je potrebno požarni zid ustrezno posodabljati.

Najtrši oreh za požarne zidove predstavljajo prav gotovo virusi,.črvi, itd. Res je, da nekateri programski paketi za vzpostavitev požarnega zidu nudijo protivirusno zaščito, vendar le-ta navadno ni najkvalitetnejša. Poleg tega, da je med podatki, ki prihajajo skozi požarni zid zelo težko identificirati računalniški program z uničevalnimi posledicami, saj so podatki v mnogih primerih stisnjeni (kompresirani), kodirani ali kako drugače obdelani za prenos, lahko sami uporabniki omrežja prinašajo podatke okužene z virusi mimo požarnega zidu na svojih disketah, diskih, cd-jih, itd.

Pri tem najbrž ni potrebno omenjati, da požarni zid, ki predstavlja ozko grlo za komuniciranje med uporabniki na internetu (ang. end to end user communication), upočasnjuje vse oblike komuniciranja in izmenjavanja podatkov med uporabniki obeh strani požarnega zidu. Komuniciranje je upočasnjeno, podatki, ki bi jih želeli posredovati, ne morejo skozi zid, itd.

To pa so stranski učinki in cena, ki jo je potrebno plačati za vzpostavitev varnostnega sistema z namenom zaščite pred nezaželenim odtekanjem podatkov in vdori različnih vsiljivcev.

3.1 Zaščita pred vdori v domače računalnike

Število uporabnikov, ki so ves čas priključeni na internet, se ves čas povečuje. Pri nas še zlasti zaradi prihoda ADSL in kabelskega interneta. S tem pa se pojavijo tudi nove nevarnosti. Računalnik, ki je ves čas povezan na internet, ima namreč stalni internetni naslov, zaradi česar je varnostno precej bolj občutljiv od računalnika, ki mu začasni naslov vsakič, ko se priključi na internet, dodeli strežnik internetnega ponudnika. Domači računalniki, ki običajno niso ves čas priključeni na internet, za razliko od podjetij, organizacij in institucij, ki imajo najete vode, navadno niso tarča vdorov, vendar pa se vedno utegne najti kak posameznik, ki se bo svoje obrti začel učiti prav na našem.

Kako dobro smo zaščiteni pred vdori lahko preverimo na spletni strani družbe Gibson Research Corporation (Gibson Research Corporation: ShieldsUP!. [URL: http://www.grc.com], 15.3.2002), ki ima na svoji strani poseben preizkus varnosti, ˝ShieldsUP!˝. Ta program nam na zelo slikovit način razkrije, kako ranljiv je naš računalnik. Ime našega računalnika in številka omrežne kartice sta že podatka, ki ju računalnik brezskrbno posreduje vsakomur, ki zanju vpraša. Najbolj občutljiva točka omrežnega računalnika so vrata (ang. port). Za različne načine komuniciranja s svetom so prirejena različna vrata. Ena za elektronsko pošto, druga za splet, tretja za izmenjavo datotek, itd. Promet skozi ta vrata je navadno dvosmeren, težava pa je, da navadno ne vemo, katera so morda na stežaj odprta. Shields UP! nam omogoča, da preverimo, katera vrata so odprta, zaprta ali zakrita. Na nezavarovanem računalniku so vrata navadno zaprta, nekaj pa je celo odprtih in skozi slednja odtekajo podatki o našem računalniku.

Najbolje je, če so vrata zakrita. Najenostavneje računalnik zavarujemo s primernim programom, ki omogoča vzpostavitev požarnega zidu. Tak program poskrbi, da so naša vrata ne samo zaprta, ampak tudi zakrita, uporabnik računalnika pa ima nadzor nad internetnimi povezavami.

3.2 Izpostavljenost vdorom in zaščita pred vdori v lokalna omrežja podjetij

Do sedaj smo imeli opravka predvsem z varnostjo domačih računalnikov povezanih v internet, katerih največja nevarnost so resnici na ljubo še vedno virusi, črvi, trojanski konji in programske bombe.

Stvari pa so nekoliko drugačne, ko postanejo tarče napada upravljalci strežnikov, ponudniki internetnih storitev, podjetja in organizacije, ki imajo postavljeno lokalno omrežno infrastrukturo. Ker gre v tem primeru za sisteme, ki so ves čas povezani na internet, je tveganje za vdore veliko večje, potencialna nastala škoda pa je lahko astronomska.

V tem primeru so potrebne kompleksnejše varnostne rešitve, ki kombinirajo požarni zid, omejevanje dostopa na internet, uporaba protivirusnih programov, zapletenih gesel, popravki programske opreme in spremljanje šibkih točk.

Podjetja kot so npr. pri nas Hermes plus (Hermes Plus: Rešitve in produkti. [URL: http://www.hermes-plus.si/ResitveProdukti/ResitveProdukti.shtml], 12.3.2002) ponujajo ustrezne pakete zaščite za izgradnjo sistema varnosti informacijskega sistema in programsko podporo za varno e-poslovanje in e-trgovanje.

Po projekcijah spletne strani Computer Economics verjetnost, da bo posamezno podjetje z zasebnim omrežjem postalo žrtev vdora v njihovo omrežje, narašča. Po njihovih najskromnejših ocenah naj bi število vdorov zgolj v letošnjem letu naraslo vsaj za 230% (Computer economics security review 2002. [URL: http://www.computereconomics.com/article.cfm?id=356], 10.5.2002). Pri tem je treba upoštevati, da vsega 20% oškodovanih podjetij dejansko prijavi vdor v njihovo omrežje. Podjetja se namreč bojijo, da bi razkritje takšnih podatkov povzročilo padec zaupanja v varnost njihovega poslovanja in s tem negativno vplivalo na njihovo poslovanje.

Tabela 4: Izpostavljenost podjetij v posameznih sektorjih vdorom v zasebna omrežja.

INDEKS RANLJIVOSTI[3]	SEKTOR
100	Bančništvo in finance
97	Transport
85	Prodaja na debelo
83	Prodaja na drobno
76	Manjša proizvodna podjetja
71	Poklicne storitve
66	Trgovina
64	Proizvodnja
61	Državna in lokalna uprava
59	Zdravstvo
51	Zavarovalništvo
46	Zvezna vlada

Vir: Computer security institute: CSI/FBI Computer Crime and Security Survey.
[URL: http://www.gocsi.com/press/20020407.html], 10.5.2002.

[3] Višji indeks pomeni večje tveganje. Najvišji indeks je 100.

Ameriški inšitut za računalniško varnost (The Computer Security Institute) je v aprilu letošnjega leta v sodelovanju z FBI-jem objavil rezultate letne raziskavo s področja računalniškega kriminala in računalniške varnosti (Computer Crime and Security Survey). V raziskavi so sodelovala 503 podjetja, od korporacij, vladnih agencij, finančnih inštitucij in univerz.

Namen raziskave je povečati ozaveščenost na področju internetne varnosti in oceniti obseg računalniškega kriminala v ZDA.

Rezultati raziskave na področju internetnega kriminala vključujejo sledeče (Computer security institute: CSI/FBI Computer Crime and Security Survey. [URL: http://www.gocsi.com/press/20020407.html], 10.5.2002):

- 90% podjetij udeleženih v raziskavi je v zadnjem letu zabeležilo vsaj en vdor v lastno omrežje. V večini primerov gre za velike korporacije ali vladne agencije.
- 80% podjetij udeleženih v raziskavi je zaradi vdorov utrpelo finančno škodo.
- 40% udeleženih podjetij je uspelo oceniti nastalo ekonomsko škodo. 223 podjetij je utrpelo za kar 455,8 milijona dolarjev škode.
- Kakor tudi v prejšnjih letih, je tudi letošnja raziskava ugotovila, da je največ škode nastalo zaradi kraje zaupnih podatkov (170,8 milijona dolarjev) in finančnih prevar (115,8 milijona dolarjev).
- 34% vseh vdorov je bilo prijavljenih oblastem. Leta 1996 je bilo takih prijav zgolj 16%.

Podjetja, udeležena v raziskavi, poročajo o številnih različnih oblikah zlorab njihovega zasebnega omrežja:

- 40% vdorov je iz odprtega omrežja,
- 40% jih je utrpelo napad tipa ˝denial of service˝,
- 78% anketiranih podjetij je bilo oškodovanih s strani insiderjev (zaposlenih v podjetjih),
- 85% anketirancev je zabeležilo okužbo z virusom,
- 38% jih je utrpelo nepooblaščen dostop do njihovih spletnih strani ali zlorabo le-teh,
- 70% vdorom v sistem je sledil vandalizem ter
- 12% udeležencev raziskave poroča o kraji transakcijskih podatkov.

4. Varnost e-poslovanja in e-trgovanja

Tehnologije in orodja pod imenom požarni zid so v preteklosti omogočila varno vzpostavitev povezave z internetom. Ta tehnologija je danes že splošno uveljavljena in praktično ni podjetja,

ki je ne uporablja za zaščito internetne povezave. Vendar pa ima le-ta svoje omejitve. Nastala je za zaščito pred nedovoljenimi vzpostavitvami povezav z internim omrežjem in to nalogo odlično opravlja. Problem pa nastane, ko želimo internet uporabljati za poslovne transakcije. Tehnologija požarnega zidu nam v ta namen ne nudi ustrezne zaščite. Če želimo uporabljati internet ali kateri drugi komunikacijski medij, nad katerim nimamo nadzora, moramo za varno poslovanje zagotoviti sledeče (Jerman-Blažič, 2001, str. 101):

- zanesljivo identifikacijo obeh udeležencev v transakciji (v elektronski obliki),
- zaupnost transakcije,
- integriteto/celovitost prenesenih podatkov med prenosom prek nevarovanega/neznanega omrežja,
- nezatajljivost (ang. non-repudation).

Osnovna orodja, ki omogočajo uporabo šifriranja za zaščito prenosa podatkov, so SSL (https protokol na spletnih strežnikih) in VPN (navidezna zasebna omrežja). V zadnjem času se jima s pospešenim tempom pridružuje WTLS (WAP strežniki). Ta orodja z uporabo šifriranja zagotavljajo zaupnost transakcij in integriteto prenešenih podatkov.

Identifikacija obeh udeležencev v transakciji in nezatajljivost, pa omogoča uporaba tehnologije digitalnih podpisov in z njo povezanih tehnologij javnih-skrivnih ključev ter digitalnih potrdil. Programska orodja in vsi postopki, ki omogočajo izdajo digitalnih potrdil in njihovo upravljanje, so znana pod imenom PKI (ang. Public Key Infrastrucure).

Podjetje, ki razmišlja o postavitvi sistema elektronskega poslovanja oziroma trgovine na internetu z varnim on-line sistemom plačevanja, ima na voljo tri možnosti:

1. Postavitev sistema elektronskega poslovanja iz nič

Dobra možnost za velika podjetja, ki razpolagajo s primernim strokovnim osebjem, ki imajo na voljo velika finančna sredstva in možnost razvoja programske opreme. Tako so nekatera znana podjetja kot npr. Cisco, Amazon.com, Dell, sama vzpostavila sistem elektronskega poslovanja in pri tem porabila nekaj milijonov dolarjev.

2. Uporaba že izdelanih paketov programskih orodij

Ponavadi predstavljajo ti paketi le delno rešitev, saj jih je večina omejena na elektronsko izložbo, predstavitev izdelkov in delno podporo sprejemanja naročil. Podjetja, ki jih že izdelani osnovni programski paketi orodij ne zadovoljijo, morajo kupiti dodatne pakete orodij, npr. za obdelavo naročil in pomoč kupcem, kar bistveno podraži zadevo, poleg tega pa morajo različna orodja med seboj uskladiti in nato vzdrževati.

3. Najetje zunanjega izvajalca za uvajanje sistema elektronskega poslovanja

Podjetja, ki nimajo lastnega znanja s področja informacijske tehnologije, nimajo svojih strokovnjakov ter se ukvarjajo z dejavnostjo, ki zahteva izgradnjo edinstvenega sistema elektronskega poslovanja, standardna programska oprema pa ne nudi zadovoljive rešitve, je prisiljeno najeti zunanjega izvajalca za vzpostavitev sistema elektronskega poslovanja.

4.1 Ponudniki storitev e-poslovanja v Sloveniji

V večini podjetij, ki uvajajo sistem elektronskega poslovanja, se najpogosteje odločijo,da bodo izvedbo v celoti prepustili zunanjemu izvajalcu, ki razpolaga z vso potrebno infrastrukturo.

Primera ponudnikov storitev elektronskega poslovanja na slovenskem trgu sta Siol in Eon (CSP - Commerce Service Provider). S pomočjo vodilnega podjetja na področju varnega elektronskega poslovanja Open Market so pri obeh podjetjih vzpostavili celotno *infrastrukturo* za sodobno elektronsko poslovanje, imenovano Transact 4 (Eon: commerce service provider: Transact 4 – infrastruktura za spletno poslovanje. [URL: http://portal.eon.si/eongroup/eon.jsp], 18.5.2002).

Le-ta predstavlja vodilno svetovno strežniško aplikacijo, saj je v uporabi v več kot 1000 velikih korporacijah v 25 državah po celem svetu in ima 30% tržni delež na področju programske opreme za elektronsko poslovanje. Ker predstavlja Transact 4 izredno uspešno rešitev za varno poslovanje preko interneta, ga pri svojem poslovanju na internetu uporabljajo številna znana podjetja kot so AT&T, Barclay's Bank, Time Warner Pathfinder in Disney.

Ločeno je upravljanje prodajalčeve ponudbe, kot so katalogi izdelkov na spletnih straneh, od procesiranja naročil in povezovanja z bankami, ki preverjajo plačilno sposobnost kupca ter opravljajo prenose sredstev. S tem se zagotavlja optimalna varnost, upravljanje in nadgradljivost celotnega sistema za elektronsko poslovanje.

Prav tako omogoča varno on-line plačevanje s kreditnimi karticami. Bistvo takšnega načina plačevanja je, da se v varnem in zakodiranem finančnem okolju lahko takoj preveri kupčeva plačilna sposobnost in veljavnost njegovega računa pri izdajatelju plačilne oziroma kreditne kartice. Tako sta zavarovana trgovec in izdajatelj kartice, kupcu pa je onemogočeno, da bi kupoval prek svojih zmožnosti ali celo goljufal. Za varnost skrbi 128-bitni ključ, ki je praktično nezlomljiv.

Vse občutljive informacije, na primer podatki o plačilih in kupcih, se shranjujejo za dvema požarnima zidovoma, vsi potrošnikovi podatki o plačilu so individualno kodirani, poleg tega pa

je zagotovljena tudi podpora za vse najvarnejše svetovne plačilne protokole vključno s standardom SET.

4.2 SiShop-slovenska programska oprema za elektronsko poslovanje in trgovanje

Paket za elektronsko poslovanje in trgovanje, ki naj bi po kakovosti bil enakovreden podobnim tujim izdelkom, vendar je prilagojen posebej za slovenski trg, so razvili tudi v računalniški hiši ICOS in podjetju za računalniški inženiring in consulting Abraxas, ki sta leta 1997 na slovenski trg poslala celovito rešitev elektronskega poslovanja SiShop (Abraxas: Sishop 2.0. [URL: http://www.abraxas.si/ sishop.htm], 15.5.2002).

Zaradi zagotavljanja varnosti so v sistem vključeni najsodobnejši mehanizmi varovanja in varnostnih protokolov. Da so vse informacije, ki se prenašajo po omrežju šifrirane in s tem nedostopne drugim udeležencem v omrežju internet skrbi varnostni protokol SSL (Secure Socket Layer). SET (Secure Electronic Transactions) protokol pa zagotavlja kupcem diskretnost, trgovcem pa samodejno avtorizacijo transakcij s kreditnimi karticami prek povezave z bančnimi sistemi. SiShop temelji na tehnologiji sodobnih relacijskih podatkovnih baz, ki z različnimi mehanizmi zagotavljajo, da bodo vsi shranjeni podatki med seboj konsistentni, pravilni in nedostopni nepooblaščenim uporabnikom.

ICOS marketing s tem programom zagotavlja varnost vseh udeležencev v transakciji, kjer ni zavarovan le plačilni promet, temveč celotno komuniciranje med partnerjema. V primeru implementacije različnih protokolov, vključno s SET-om, naj bi SiShop imel pripravljene rešitve za vmesnike in je odprt za različne plačilne standarde.

Programski paket SiShop podpira gotovinske in negotovinske plačilne sisteme, vključno z plačilnimi karticami. Plačevanje poteka s pomočjo modula SiPay, ki omogoča 128 bitno zakodirano povezavo s plačilnim centrom za kreditne kartice Aktiva in Eurocard.

4.3 Šifriranje oz. kriptiranje kupčevih naročil na spletu

Podatki o transakcijah, ki si jih izmenjavajo kupec, trgovina in banka, so zelo zaupne narave, zato so ti podatki šifrirani. Stopnja zaščite je med drugim odvisna tudi od velikosti šifrirnega ključa (Jerman-Blažič, 2001, str. 105).

Šifriranje je postopek, s katerim zaščitimo vsebino sporočila pred vpogledi s strani neavtoriziranih oseb. Kako varna so zaščitena sporočila, je odvisno od vrste uporabljenega šifrirnega postopka, predvsem pa od velikosti šifrirnega ključa (merjeno v bitih). Daljši je ključ, težje je zaščito zlomiti in prebrati vsebino sporočila. Bistvena razlika med 40-bitno in 128-bitno zaščito, ki sta največkrat uporabljeni, je v številu možnih ključev, s katerimi je zaklenjeno sporočilo. Tako npr. 128-bitna zaščita pomeni, da je med prenosom sporočilo šifrirano z enim od 2^{128} različnih možnih ključev. Po navedbah Netscape-a bi z današnjo tehnologijo 128-bitno šifrirano sporočilo razbili kar 309.485.009.821.345.068.724.781.056-krat težje od tistega, ki je kodiran s 40-bitnim ključem (Skbnet: Varnost na internetu. [URL: http://www.skb.si/html/skbnet/varnost_internet.html], 12.3.2002).

Nešteto možnih kombinacij bitov v ključu je potrebno preveriti in uporabiti zapletene matematične izračune, ki vzamejo kar nekaj časa, preden je mogoče odkriti pravi ključ. Seveda so na tržišču zelo dobri računalniki, ki lahko pregledajo veliko možnosti na sekundo, toda tudi najhitrejši osebni računalniki bi rabili mesece, morda celo leta, da bi našli pravi 128-bitni ključ Celo za zlom 40-bitnega ključa bi potrebovali več tednov. Zaščita z varnostno kodo (enkripcija) je torej dovolj velika in pomeni veliko zapravljanje časa in truda za tiste, ki bi se lotili razbijanja zakodiranih podatkov

4.4 Elektronsko podpisovanje elektronskih dokumentov

Nezaupanja glede zagotavljanja verodostojnosti elektronskih dokumentov se je tehnološki razvoj lotil tudi z uporabo kriptografskih metod. Iznajdba asimetričnega postopka šifriranja je namreč omogočila uvedbo digitalnega podpisa, s katerim lahko zagotavljamo verodostojnost elektronskih dokumentov.

Asimetrična kriptografija uporablja za šifriranje in dešifriranje par ključev, ki sta neenaka, a neločljivo povezana, poleg tega pa se iz poznavanja samo enega ključa ne da generirati drugega. En ključ se imenuje zasebni in je namenjen dešifriranju podatkov, drugi ključ je javni in je namenjen šifriranju podatkov. Da lahko nekdo elektronski dokument prebere, ga mora najprej dešifrirati, obenem s tem pa dobi tudi potrdilo o njegovi verodostojnosti oziroma preveri naš digitalni podpis (Toplišek, 1998, str. 38).

Zasebnost pri asimetričnem šifrirnem postopku in verodostojnost digitalno podpisanega dokumenta v celoti slonita na tajnosti zasebnega ključa. Če ta ključ nekdo odkrije, lahko po eni strani dešifrira vse zaupne dokumente, ki so šifrirani z našim javnim ključem, po drugi strani pa lahko v našem imenu digitalno podpisuje dokumente, ki jih mi sami sicer ne bi podpisali. Za tajnost svojega zasebnega ključa moramo zato sami v celoti prevzeti odgovornost.

Elektronsko podpisovanje, ki temelji na javnem kriptografskem ključu, omogoča prejemniku podatkov, ki so poslani v elektronski obliki, preverjanje izvora podatkov, celostnost in nespremenjenost le-teh ter na ta način varuje njihovo nespremenljivost. Zaradi večje zanesljivosti lahko prejemnik zahteva tudi zanesljivejše informacije o identiteti podpisnika. Takšne informacije lahko posreduje podpisnik sam, tako, da prejemniku izda zadovoljive dokaze. Lahko pa identiteto podpisnika potrdi tudi tretja stranka To je navadno institucija za upravljanje z javnimi ključi, ki ji zaupata tako ena kot druga stranka.

4.5 Overitelj - upravljalec z javnimi ključi

Inštitucija, ki skrbi za izdajanje, preklicevanje, podaljševanje, skratka za upravlajnje z javnimi ključi, je overitelj (ang. Certification Authority - CA). Le-ta je nekakšen posrednik med poslovnimi partnerji pri izmenjavi javnih ključev (Jerman-Blažič, 2001, str. 109).

V kolikor želimo s partnerjem komunicirati z uporabo javnega ključa, lahko pri overitelju registriramo svoj javni ključ. Ob registraciji ključa overitelj digitalno podpiše naš javni ključ in s tem potrdi njegovo verodostojnost. Tako podpisan ključ objavi na svojem strežniku javnih ključev, na katerem ga lahko najde vsak, ki ima dostop do interneta. Podobno lahko na tem strežniku tudi sami najdemo ključe svojih poslovnih partnerjev. Ker nam digitalni podpis overitelja zagotavlja verodostojnost tega ključa, smo varni pred morebitnimi nesporazumi glede avtentičnosti in izvornosti elektronskih dokumentov.

4.6 Varno nakupovanje na spletnih straneh

4.6.1 Previdnost pri internetnem nakupovanju

Na spletnih prodajalnah nas prepričujejo, da so podatki, ki jih pošiljamo, varni pred zlorabo, plačevanje računa s kreditno kartico preko POS terminala v lokalu ali kje drugje pa mnogo bolj rizično. Vendar vedno ni tako, zato je potrebna previdnost. Pri trgovanju preko spletnih trgovin številko svoje kartice pošljemo vnaprej slepo verujoč podatkom, ki jih objavi prodajalec na svoji spletni strani.

Primeri izmišljenih podjetij na Internetu, ki so objavljala ponudbe izdelkov, redno odmevajo v medijih. Kupci so pridno pošiljali številke svojih kartic in kupovali izdelke, ki jih ni bilo. Zlorabo so opazili, ko tudi čez nekaj tednov niso prejeli plačanih izdelkov, denar na njihovih računih v bankah pa je skopnel.

Najvarnejše so ponavadi tiste trgovine, ki so v svetovnem spletu že dodobra uveljavljene. Preden se lotite nakupovanja je koristno prebrati besedilo o varnosti, ki je običajno objavljeno na spletni strani spletne trgovine. V njem je razloženo, kako skrbijo za varnost podatkov (ang. privacy policy). Posebno pozorni bodite na droben tisk. Tako vam, npr. pri Amazon.com, na svoji strani o varnem nakupovanju zagotavljajo 100% varnost pri prenosu podatkov. Pravijo, da pri morebitni zlorabi kartice, ki bi bila posledica nakupa pri njih, kupec ne nosi nikakršnih stroškov. Vendar se v drobnem besedilu na dnu strani skriva presenečenje, saj piše, da Amazon.com krije stroške do višine 50 dolarjev in še to samo v primeru, da do zlorabe ni prišlo zaradi vaše napake.

Zato podatke o svojih karticah pošiljajmo samo preverjenim podjetjem, nikakor pa ne z namenom dostopa do drugih internetnih strani ali, da bi dokazali svojo polnoletnost.

Pred nakupovanjem se je smiselno pozanimati pri izdajatelju plačilne kartice, kako je s kritjem stroškov, ki bi nastali ob morebitni zlorabi. Izdajatelji plačilnih kartic imajo ponavadi tudi tako imenovano črno listo podjetij, pri katerih zaradi kupčeve varnosti nikakor ni priporočljivo nakupovati. Če ugotovimo zlorabo naše kreditne kartice, je potrebno takoj poklicati servisni center izdajatelja kreditne kartice, saj stroške zlorabe do prijave ter nadaljnjih 24 ur krije uporabnik kartice, kasneje pa izdajatelj. Izjema je American express, ki krije le določen znesek zlorabe.

Dobro si je omisliti posebno plačilno kartico zgolj za spletno nakupovanje, po možnosti pa tudi račun, ki se ga napolni po potrebi. Takšno kartico, ki ne omogoča negativnega stanja, račun pa se polni po potrebi imenujemo debetna kartica.

Čeprav banke avtomatično podaljšujejo veljavnost plačilnih kartic, je smiselno sem in tja zamenjati kartico ali vsaj številko kartice, ki jo uporabljamo za spletno nakupovanje.

4.6.2 Razpoznavnost zaščitenih protokolov na spletnih straneh

Poglavitna nevarnost pri spletnem trgovanju je možnost prestrezanja podatkov, ki niso javni, predvsem številke kreditne kartice, ki se lahko na škodo uporabnikov zlorabijo. Zato se v spletnem trgovanju za zaščito podatkov uporabljajo določeni standardi kodiranja prenosa podatkov od uporabnika do strežnika spletne trgovine ter kodiranje elektronskih plačilnih transakcij med strežnikom spletne trgovine in omrežjem banke, s katero se transakcija izvaja.

Celotno spletno naročanje, ki vključuje podatke o kupcih, naslove, načine plačevanja in podatke plačilne kartice, je pogosto zaščiteno z uporabo tehnologije SSL (ang. Secure Socket Layer), tehnologija SET (ang. Secure electronic transaction) pa se zadnje čase uvaja kot standardni

protokol za varno elektronsko plačevanje s kreditno kartico, pri čemer kot tretja stranka v udeležbi nastopa banka, ki plačilno transakcijo izpelje.

Kadar je spletna stran zaščitena z uporabo tehnologije SSL, uporablja zaščiteni protokol Https://, za razliko od nezaščitenega Http:// protokola. To pomeni, da so kupčevi podatki zaščiteni z varnostno kodo in varnostnimi ukrepi še preden so poslani z računalnika. Sistem spletnega naročanja sprejema podatke samo od brskalnika z vgrajeno zaščito podatkov.

4.6.3 Varnost kupčevih podatkov na strežnikih spletnih trgovin

Vendar pa protokol SSL ne zagotavlja, da so preneseni podatki varni tudi pred zlorabo trgovca, saj jih ščiti le med prenosom med odjemalcem in strežnikom.

Poleg tega se zopet pojavi vprašanje, kako dobro je poskrbljeno za varnost shranjenih podatkov na trgovčevem strežniku. So primeri, ko so nepridipravi vdrli v strežnike spletnih trgovin in se dokopali številk kreditnih kartic. Seveda je teh zlorab zelo malo, saj je v dobro zavarovan strežnik sposobno vdreti zelo malo hacker-jev.

Nevarnejši in popularnejši način pridobivanja številk kreditnih kartic je naključno generiranje števil s posebnimi programi. Proti tem programom se izdajatelji plačilnih kartic borijo z drugimi varnostnimi ukrepi. Kljub vsemu, da se delež teh zlorab zmanjšuje, pa pri podjetjih, ki so najbolj na udaru, še vedno dosega okoli 5% celotnega prometa s karticami.

4.6.4 Ne/Varno e-nakupovanje

Kljub vsem potencialnim nevarnostim zlorabe vaše številke kreditne kartice omenjenih v točki 4.6.1, ki vas lahko doleti pri spletnem nakupovanju, od prestrezanja številke, vdora v spletni strežnik, naključnega generiranja števil, pa je treba ugotoviti, da obstaja večja nevarnost, da vas okradejo v običajni trgovini kot na spletu. Varneje je celo od telefonskega in kataloškega nakupovanja in to prav zaradi vseh modernih postopkov kodiranja in enkripcije podatkov.

Plačevanje v restavraciji, kjer ste pri plačevanju s kreditno kartico petnajst minut čakali na račun, faksiranje kartice za hotelsko rezervacijo, plačevanje hotelskih storitev in pa brskanje tujcev po vaših smeteh, so vse primeri potencialnih možnosti pridobitve in zlorabe vaše plačilne kartice. Precej lažje se je dokopati do številk kreditnih kartic v košu za smeti bližnjega supermarketa kot pa prestreči podatke o kupcih pri spletnem nakupovanju, zatorej smo lahko prepričani, da je spletno nakupovanje zelo varna oblika nakupovanja.

4.6.5 Digitalni certifikati

Izdaja digtalnih certifikatov je storitev namenjena varovanju legitimnih spletnih trgovin. Ti certifikati preprečujejo nepridipravim, da postavijo povsem enako spletno stran, kot jo ima njihova tarča napada, in nanjo preusmerijo nič hudega sluteče kupce, katerim poberejo številke kartic. Digitalne certifikate prodajajo prav s tem namenom ustanovljena podjetja – overitelji, ki skrbijo za to, da se zlonamerne strani odstranijo z interneta. Eno izmed takih večjih podjetij je VeriSign (Verisign. [URL: http://www.verisign.com], 15.4.2002). Spletne trgovine, ki so zaščitene na tak način, prepoznamo po obvestilu pri vstopu na njihove strani, da je zaščitena z digitalnim certifikatom.

5. Zakonodaja na področju interneta

Vprašanja, ki zadevajo pravno ureditev elektronskega poslovanja, avtorske pravice, sklepanje pravnih poslov, zaščito in zbiranje podatkov, vsebino spletnih strani, elektronski podpis, zasebnost in pristnost sporočil, itd., so dodatno otežena zaradi dejstva, da se dejavnosti v internetu dogajajo po vsem svetu, ne glede na državne meje, da je potrebno upoštevati zakone posameznih držav ter, da je dostop v omrežje pravno in tehnološko omogočen nedoločenemu številu uporabnikov.

5.1 Zaščita avtorskih pravic na internetu

Avtorska pravica kot avtorjev monopol nad izkoriščanjem avtorskega dela zagotavlja avtorju po eni strani premoženjske koristi od izkoriščanja njegovega dela, po drugi strani pa spoštovanje njegovih moralnih interesov pri izkoriščanju njegovega dela.

Tako so računalniški programi po Bernski konvenciji za varstvo književnih in umetniških del[4] varovani kot književna dela. Ameriški zakon o avtorskih pravicah[5] pa opredeljuje računalniški program kot niz navedb oziroma navodil, ki se uporabljajo neposredno ali posredno v računalniku z namenom doseganja želenega rezultata, in je zavarovan v okviru avtorskih del v materialni obliki.

V slovenskem, tako kot tudi v večini ostalih pravnih sistemov, nastane avtorska pravica s samo stvaritvijo. V internetu je prosto dostopnih nešteto avtorskih del, kar pa seveda ne pomeni, da za

[4] Berne Convention for the Protection of Literary and Artistic Works
[5] U. S. Copyright Law

ta dela ne veljajo avtorske pravice. Veliko dokumentov, ki jih najdemo na internetu, ima pripeto sporočilo, ki nas opozarja na pravice avtorja, marsikdaj pa tudi določa pogoje, pod katerimi se tako avtorsko delo lahko kopira, razširja, citira ali uporablja.

5.1.1 Avtorska zaščita spletnih strani

Spletne strani naj bi bile v splošnem že vključene v področje avtorske zaščite del. Avtorsko pravico do izdelanih spletnih strani ima njihov izdelovalec. Kakor hitro pa je sklenjena pogodba o izdelavi, se avtorske pravice samodejno prenesejo na naročnika. Pravno sporna pa bi bila uporaba podobnih rešitev izdelave tudi pri predstavitvah drugih podjetij. Za naročnika namreč ni zaželeno, da bi se popolnoma enaka oblika uporabila še drugod, za avtorja pa je vsekakor zaželeno, da učinkovite rešitve vsaj do neke mere uporabi tudi pri drugih naročnikih. Zato na primer ni dopustno kopiranje originalne grafike s strani določenega uporabnika za uporabo na drugi spletni strani.

Shranjevanje spletnih strani na osebnih računalnikih uporabnikov, namenjenih kasnejši uporabi z vidika zaščite avtorskih del ni sporno. Shranjevanje spletnih strani za kasnejšo osebno uporabo strani namreč ne zmanjšuje komercialne vrednosti le-teh, kar še posebej velja v primerih uporabe v raziskovalne in izobraževalne namene.

Kadar so uporabniki pri kršitvah avtorskih pravic prisiljeni uporabiti pravna sredstva, je to smotrno najprej doseči v lastni državi. Zaželeno bi bilo, da lahko sodišče zahteva od lokalnih ponudnikov internetnih storitev preprečitev vidnosti spletnih strani, ki kršijo avtorske pravice. Čeprav odločitev sodišča še ni avtomatično veljavna v drugih državah, pa nekatere države tako odločitev že upoštevajo.

5.1.2 Zaščita avtorskih in sorodnih pravic na internetu v Sloveniji

Zakonsko avtorske in sorodne pravice v Sloveniji tudi za področje Interneta še vedno ureja Zakon o avtorskih in sorodnih pravicah (ZASP) iz leta 1995 (Uradni list RS, št. 21/95). Pri pripravi tega zakona so avtorji upoštevali vse do tedaj sprejete konvencije in direktive Evropske Unije in Svetovne trgovinske organizacije s področja avtorskega prava (Jerman-Blažič, 2001, str. 175).

Na področju računalniških programov je Slovenija prevzela določbe Direktive EU o pravnem varstvu računalniških programov iz leta 1991. Zaščita računalniških programov je opredeljena v členih 111 do 117 ZASP. Varujejo se algoritmi, programska dokumentacija, sestavni deli in naslov računalniškega programa.

Pogoje proste uporabe avtorskih del, ki se nanašajo predvsem na pridobivanje informacij javnega značaja, kot so obveščanje o dnevnih dogodkih, dnevne novice in vesti, ki imajo naravo tiskovnih poročil, in izobraževanje ter zasebno razmnoževanje določajo členi 48 do 57 ZASP.

Računalniški program je zavarovan z zakonom pod pogojem, da je le-ta individualno delo v smislu intelektualne storitve. Avtor ima tako izključno pravico do razmnoževanja celotnega programa ali pa le njegovih sestavnih delov, priredbe, predelave in posredovanja. Te pravice so z licenčno pogodbo lahko prenosljive na drugo osebo.

Po 166. členu zakona (ZASP) se posebej obravnavajo kršitve avtorskih pravic, ki temeljijo na proizvodnji, uvozu, posedovanju, distribuciji, dajanju v najem kakršnihkoli sredstev, katerih namen je neupravičeno odstraniti ali obiti zakonito zaščito (računalniški program, tehnično napravo, požarni zid), ki preprečuje nepooblaščeno uporabo.

5.1.3 Ureditev zaščite avtorskih pravic v ZDA

Področje zaščite avtorskih pravic v ZDA ureja U.S. Copyright Law, ki se nanaša na originalna avtorska dela v materialni obliki. Originalnost je definirana kot neodvisnost stvaritve, ki ni kopirana od drugih avtorjev. Materialnost pa je zagotovljena s trajno nespremenljivo obliko, ki omogoča predstavitev dela ali njegovo reprodukcijo v daljšem časovnem obdobju s pomočjo ustrezne opreme.

Razen v primerih, ko gre za prosto uporabo dela, delo v javni domeni ali idejo, je potrebna sklenitev licenčne pogodbe z namenom prenosa pravic iz avtorsko zaščitenih del. Z licenčno pogodbo se prenašajo vse ali nekatere avtorske pravice in uveljavlja pravica do uporabe dela, ki je praviloma precej omejena.

V javno domeno spadajo dela, ki jim je poteklo obdobje zaščite ali pa jih po zakonu ni mogoče zaščititi, in jih lahko brez omejitev uporablja kdorkoli v kakršnekoli namene. Nihče pa si za ta dela, čeprav niso zaščitena, ne more lastiti ekskluzivne pravice do njihove uporabe.

Z dokumentom *White paper on Intellectual Property and the National Information Infrastructure* je bila vključena nadaljnja klavzula v obstoječi zakon U.S. Copyright Law z namenom preprečevanja zlorabe ekskluzivnih pravic določenih z zakonom. Namen klavzule je prepovedati uvoz, proizvodnjo in distribucijo sredstev, katerih namen je odstranjevanje zakonitih zaščit z avtorsko zaščitenih del brez privoljenja nosilca pravice.

Nadaljnji akt, ki obravnava to področje je oktobra 1998 sprejeti Digital Millenium Copyright Act, ki vključuje tudi določila pogodb Svetovne organizacije za intelektualno lastnino (WIPO)[6]: Pogodba *WIPO o avtorski pravici*[7] in pogodba *WIPO o izvedbah in fonogramih* [8] iz leta 1996. Poudarek akta DMCA sloni na zaščiti tujih avtorjev, nedržavljanov ZDA, in tehnološki zaščiti avtorskih del.

5.1.4 Zaščita avtorskih del v EU

Glavne smernice nadaljnjega razvoja visoke zaščite avtorskih del tudi na področju digitalnih okolij v okviru EU in mednarodni ravni so predvsem v harmonizaciji nacionalnih zakonodaj in enotni zakonski regulativi za skupno nastopanje na svetovnih trgih.

Skoraj vse države članice EU kažejo interes za spremembe, ki jih narekuje razvoj informacijske tehnologije, zlasti na področju zaščite avtorskih pravic za dela, ki se hranijo ali prenašajo po digitalnih medijih.

Države Evropske unije uporabljajo oba sistema avtorskih pravic, anglosaški sistem ″copyright ″ in kontinentalni sistem ″droit d′auteur″, zato je pomembno vprašanje kako ju uskladiti.
Zaščita avtorskih pravic v državah Evropske unije temelji na moralnih in ekonomskih pravicah. Slednje omogočajo avtorju pravico do izkoriščanja dela in prenos teh pravic na druge osebe, moralne pravice pa mu omogočajo nadzor in zakonito uporabo dela.

Direktive, smernice oziroma predlogi Evropske Unije na tem področju, ki zahtevajo uskladitev nacionalnih zakonodaj s strani vseh držav članic:

- *Direktiva o računalniških programih*[9] iz leta 1991

  Direktiva poudarja nujnost sprejetja ustreznih zakonov in harmonizacije nacionalnih zakonodaj ob upoštevanju vse večjega pomena, ki ga imajo računalniški programi za gospodarski razvoj.

- *Direktiva o najemu in sorodnih pravicah*[10] iz leta 1992
- *Zelena knjiga o avtorskih in sorodnih pravicah v informacijski družbi*[11] iz leta 1995

[6] World Intellectual Property Organization
[7] WIPO Copyright Treaty
[8] WIPO Performances and Phonograms Treaty
[9] Directive on the legal protection of computer programs
[10] Directive on Rental rights and Lending right and on certain rights related to Copyright in the field of Intellectual property
[11] Green paper on Copyright and Related rights in the Information Society

- *Direktiva o bazah podatkov*[12] iz leta 1996
- *Nadaljevanje Zelene knjige o avtorskih in sorodnih pravicah v informacijski družbi*[13] (1996)
- *Direktiva o harmonizaciji določenih vidikov avtorskih in sorodnih pravic*[14] iz leta 1997
- *Predlog direktive o avtorski in sorodnih pravicah v informacijski družbi*[15] iz leta 1999

S področja zaščite avtorskih del na ravni EU sta delno harmonizirani le zaščita računalniških programov in baz podatkov. Pomanjkanje uskladitev ima negativen vpliv na razširjanje avtorskih del. Tudi lastniki in uporabniki avtorskih del ne morejo izrabiti vseh potencialnih prednosti enotnega tržišča.

Potrebno je uskladiti predpise zlasti na naslednjih področjih zaščite avtorskih del, ki so trenutno najbolj problematična (Jerman-Blažič, 2001, str. 174):

- Obdobje zaščite

  Obdobje zaščite avtorskih del se po državah članicah zelo razlikuje. Tako so na primer v bolj razvitih državah precej daljše kot v manj razvitih. V nekaterih državah uživajo avtorji pravice za svoja avtorska dela le za obdobje svojega življenja, nekatere pa so omejene na določeno število let.

- Moralne pravice

  Pri usklajevanju moralnih pravic je potrebno upoštevati vrsto in način uporabe avtorskih del, še posebej pri multimedijskih proizvodih in storitvah, kjer je neurejenost tega področja najbolj moteča.

- Pravica do distribucije

  V nacionalnih zakonodajah se pojavljajo razlike pri določitvi posameznih vrst teh pravic. Avtorju pripada ekskluzivna pravica odločanja o distribuciji njegovih del v materialni obliki. Z usklajevanjem bi pri teh avtorskih delih dosegli uveljavljanje pravice do distribucije takoj, ko se delo pojavi na tržišču.

[12] Directive on the legal protection of databases
[13] Follow-up to the Green paper on Copyright and Neighbouring rights in the Information Society
[14] Directive on harmonization of Copyright and Related rights
[15] Proposal for Directive on Copyright and Related rights in the Information society

- Tehnološka zaščita

  Naloga usklajevanja na področju tehnološke zaščite je v spremljanju razvoja tehnoloških sredstev zaščite, ki je pretežno v lasti zasebnega sektorja. Potrebno je torej določiti in standardizirati legalna tehnološka sredstva zaščite in poskušati regulirati uporabo teh sredstev, da se prepreči zlorabe.

5.2 Varstvo podatkov na internetu

Nadaljnji vidik obravnave zaščite podatkov zadeva zbiranje podatkov o uporabnikih. Po slovenski ustavi ima vsakdo pravico do varstva osebnih podatkov, torej, da sam odloča, kdaj, komu in v kakšni obliki bodo sporočeni podatki, ki se nanašajo nanj. Ta pravica pa z vstopom na internet nekako zbledi. Poslovanje po internetu namreč prinaša s seboj tveganje, da bo en udeleženec pričel brez vednosti drugega zbirati podatke o drugem (Jerman-Blažič, 2001, str. 182).

Ob obisku spletnega kraja se avtomatično prenesejo nekateri podatki o obiskovalcu na obiskani strežnik, ki si jih v večini primerov zapiše med svoje statistične podatke. Med njimi so internetni naslov priključka, operacijski sistem obiskovalčevega računalnika in naslov strani, ki je pripeljala do tega obiska. Posebej prirejeni programi si lahko zapomnijo vse, kar določena oseba počne na internetu, in tako lahko ustvarijo profil stranke.

Nekatere države zakonsko regulirajo zbiranje podatkov o posameznikih in predpisujejo, da mora zbiralec svojo dejavnost prijaviti, seznaniti ljudi z vrsto podatkov in namenom njihovega zbiranja, omejuje se možnost distribucije teh podatkov, dana je pravica posamezniku do vpogleda v podatke o sebi ter v nekaterih primerih prepove zbiranje.

Pravna praksa na tem področju med EU in ZDA se precej razlikuje. V ZDA je skrb za podatke prepuščena posameznikom, v EU pa so za podatke odgovorni zbiralci le-teh. EU prepoveduje izvoz arhiva podatkov o državljanih EU v države z nižjo stopnjo zaščite, torej tudi v ZDA.

V Združenih državah amerike so glede zbiranja podatkov zaščiteni le otroci do trinajstega leta starosti. Zbiralec podatkov je namreč dolžan najprej prositi za dovoljenje otrokove starše ali skrbnike.

5.2.1 Varnost zasebnosti potrošnikov v Sloveniji

Pravico do varstva in zaščite osebnih podatkov V Sloveniji opredeljuje 35.člen Ustave RS, poleg tega pa je varovanje zasebnosti opredeljeno še v nekaterih ratificiranih mednarodnih dokumentih kot so npr.:

- *Konvencija o varstvu človekovih pravic in temeljnih svoboščin*[16] *(8. člen),*
- *Splošna deklaracija o človekovih pravicah*[17] *(12.člen)* ter
- *Mednarodni sporazum o državljanskih in političnih pravicah*[18] *(7.člen).*

Organizirano varstvo potrošnikov v Sloveniji se je pričelo z ustanovitvijo Zveze potrošnikov Slovenije leta 1990. Ta neprofitna in nevladna organizacija sodeluje pri oblikovanju politike in pravnega varstva potrošnikov. Pravno varstvo potrošnikov ureja Zakon o varstvu potrošnikov iz leta 1998, ki ureja razmerja med ponudniki blaga in storitev ter potrošniki. Vendar pa Slovenija še nima zakona oziroma dopolnila k zakonu, ki bi opredeljevalo varstvo potrošnikov pri elektronskem nakupovanju.

5.2.2 Mednarodna ureditev na področju varstva in zaščite potrošnikov

S tem področjem se ukvarjajo vse pomembnejše mednarodne inštitucije, Evropska komisija (EC), Organizacija združenih narodov (UNO), Organizacija za gospodarsko sodelovanje in razvoj (OECD). Sprejete mednarodne regulative vsebujejo med drugim:

1. OECD

- *Smernice za varstvo potrošnikov pri elektronskem poslovanju*[19] *(1999)*

  Namen smernic je zagotoviti takšno stopnjo varnosti potrošnikov pri elektronskem poslovanju, kot je pri tradicionalnih načinih poslovanja, kar je v interesu tako potrošnikov kot ponudnikov blaga in storitev.

- *Smernice za varstvo zasebnosti in prekomejni prenos osebnih podatkov*[20] *(1980)*

[16] Convention for the Protection of Human Rights and Fundamental Freedoms.
[17] Universal declaration of Human Rights
[18] International Covenant on Civil and Political Rights
[19] Guidelines for Consumer Protection in the Context of Electronic Commerce
[20] Guidelined fot the Protection of Privacy and Transborder Flows of Personal Data

Te smernice določajo osnovna načela za ravnanje s podatki v odprtih omrežjih. Za zbiranje osebnih podatkov morajo obstajati določene omejitve, podatki se morajo zbirati na veljaven in korekten način, z vednostjo in dovoljenjem osebe, o kateri se podatki zbirajo.

- *Izjavo o varstvu zasebnosti na svetovnih omrežjih*[21] *(1998)*

2. Evropska unija

- *Direktivo EU o varstvu oseb pri obdelovanju osebnih podatkov (1995)*

  Direktiva zagotavlja visoko varnost osebnih podatkov in zasebnosti, pri čemer je poudarek na odpravljanju ovir za prost pretok osebnih podatkov znotraj EU. Ostale države morajo pri izmenjavi podatkov z Evropsko unijo zagotoviti vsaj takšno stopnjo varnosti in zaščite kot velja v EU.

- *Direktivo EU o varstvu potrošnikov pri poslovanju na daljavo*[22] *(1997)*

  Direktiva ureja posamezne aktivnosti naročanja in nakupovanja preko interneta. Vzpostavlja minimalne standarde zaščite na področju EU pri nakupovanju potrošnikov v drugih državah znotraj Unije. Pomembne aktivnosti za učinkovito in varno nakupovanje so pridobitev predkupnih informacij, potrjevanje, izvrševanje naročila, plačevanje, storniranje, pritožbene možnosti za učinkovito reševanje sporov.

5.3 Omejevanje dostopa do vsebin na internetu

Pri brskanju po internetu se dogaja, da po naključju naletimo na nezaželeno vsebino oziroma na vsebino, kjer gre za prepovedano in kriminalno dejavnost, ščuvanje in razpihovanje sovraštva ter širjenje lažnih podatkov. Še posebno so kočljivi vsebini izpostavljeni otroci.

V ZDA so pri pravni regulativi vsebine spletnih strani naredili prvi korak. Pred neprimerno vsebino so zaščitili otroke mlajše od trinajst let tako, da so od ponudnikov dvomljivih vsebin zahtevali, da svoje strani opremijo s posebnimi oznakami, ki omogočajo v brskalniku onemogočiti dostop do oporečne vsebine.

Varnost mladoletnikov pred neprimernimi vsebinami zahteva razvoj in uporabo ustrezne programske opreme, ki onemogoča dostop na strani z vprašljivo vsebino. Tu gre predvsem za

[21] Declaration on the protection of Privacy on Global Networks
[22] Directive on the Protection of Consumers in respect of Distance Contracts.

filtrirno programsko opremo kot je Cyber Patrol, Net Nanny, Parental Guidance, itd., ki omogočajo odraslim osebam nadzor nad ustreznostjo spletnih strani, ki jih mladoletni najpogosteje uporabljajo.

Aktivno vlogo pri nadziranju vsebine bi morali odigrati tudi ponudnik internetnih storitev (ISP). Toda tu lahko pride do problemov, ker je sprotno nadzorovanje vsebine v nasprotju s svoboščinami in pravico govora, poleg tega pa tehnično prezahtevno in drago. Etično pa bi bilo, da bi ponudnik posredoval vsaj takrat, ko je na zlorabo opozorjen.

5.4 Registracija domen v tujini in doma

Vsi lastniki podjetij, ki želijo svojo dejavnost širiti tudi na splet, si prizadevajo, da bi za ime domene v omrežju uporabili ime svojega podjetja, ime blagovne ali storitvene znamke, in s tem povečali prepoznavnost svojega podjetja tudi v spletu. Na področju domen večkrat naletimo na dva poglavitna problema. Katero od dveh podjetij, ki sta registrirani pod enakima ali zelo podobnima imenoma, ima pravico registrirati tako domeno, in kaj, če uporabnik v neki drugi državi registrira kot svojo domeno ime svetovno znanega podjetja?

Iznajdljivi uporabniki so si tako registrirali domene z imeni zelo slavnih in priznanih podjetij, kot je npr. McDonald's, in nato izsiljevali nosilce le-teh, ki so bili za odkup te domene pripravljeni plačati tudi več deset tisoč dolarjev, kar je postalo znano pod angleškim izrazom ˝domain name grabbing˝ (Stanford computer science education: domain name grabbing. [URL: http://www-cse.stanford.edu/classes/cs201/projects-97-98/domain-names/problems/grabbing.html], 10.4.2002). Zlorabe pa so se vršile tudi med konkurenčnimi tekmeci, ko so podjetja registrirala domeno z imenom konkurenčnega podjetja in na takem strežniku objavljala informacije, ki so kvarile ugled konkurenčnemu podjetju. V takem primeru se je treba zateči k pravnim ukrepom, ki pa so včasih zapleteni in dragi, stranka v postopku pa je morda celo na drugem koncu sveta. Zato je priporočljivo, da podjetja poleg svoje regionalne domene registrirajo z istim imenom vsaj še različico .com.

Slovenija ima pri krovni organizaciji za upravljanje globalnega domenskega prostora ICANN (Internet Corporation for Assigned Names and Numbers. [URL: http://www.ICANN.org], 20.5.2002) registrirano regionalno domeno .si.

Znotraj te pa je za nadaljnje registracije v Sloveniji pooblaščena organizacija ARNES (Akademska in raziskovalna mreža Slovenije. [URL: http://www.arnes.si/domene], 18.5.2002), ki je do sedaj v svojih pravilih o registraciji domen zaradi zlorab določala, da je ime domene lahko le polno ali skrajšano registrirano ime organizacije. Za pridobitev domene pa je moral

prosilec obrazcu za registracijo priložiti tudi kopijo sklepa vpisa v sodni register, iz katerega je bilo razvidno registrirano polno in skrajšano ime organizacije.

Od meseca oktobra 2001 pa poteka v Sloveniji javna debata o spremembi pogojev registracije pod slovensko nacionalno domeno .si. Javni zavod ARNES se je zato lotil prenove pogojev registracije (Akademska in raziskovalna mreža Slovenije: Registracija domen. [URL: http://www.arnes.si/domene/registracija.html], 18.5.2002), ki so bili do sedaj precej togi. Arnes tako uvaja možnost registracije domene pod blagovno znamko, npr. www.Mars.si za revijo Mars, in prenos registracije na pooblaščene registratorje. Sprostitev registracije pa bo sprožila tudi več sporov upravičenosti imetništva posamezne domene, zato bo Arnes uvedel poseben postopek njihovega reševanja. Na začetku bo omogočeno neko prehodno obdobje za registracijo domen pod imeni blagovnih znamk, kasneje pa bodo prosto dostopne na trgu.

Globalne domene tipa .com, .org, .net, se podeljujejo bolj liberalno. Te domene je moč registrirati pri pooblaščenih registratorjih, ki jih pooblašča ICANN. V primeru, da je želeno ime še prosto, se lahko domeno takoj registrira. Liberalnost dodeljevanja domen povzroča v praksi veliko konfliktov, saj prihaja do namerne in nenamerne registracije imen, ki so sicer znana in so celo zaščitena vsaj v nekaterih državah.

Z namenom pospeševanja elektronskega poslovanja v EU so telekomunikacijski ministri sprejeli namero o uvedbi nadnacionalne domene .eu, ki bi omogočala medsebojno identifikacijo med poslovnim subjekti držav članic EU.

5.5 Internetno oglaševanje

Raznolike in ponekod stroge zakonodaje v posameznih državah onemogočajo svobodno oglaševanje po internetu, zato je potrebna dobršna mera previdnosti, da kaj hitro ne zabredemo v pravne spore. Posebnosti se nanašajo zlasti na reklamiranje alkohola in tobačnih izdelkov ter uporabo erotike in nasilja v reklamnih sporočilih.

Strani, na katerih se nahajajo določeni oglasi, so vidne potrošnikom v različnih državah, zato obstaja možnost kršitve predpisov v kateri od držav. Glede na dejstvi, da sodna praksa na tem področju še ni dorečena, bi naj v prihodnje veljalo, da, če oglas ni aktivno usmerjen in agresivno naravnan na zaščiteno področje in imajo obiskovalci s tega področja le bolj ali manj naključno možnost priti v stik s takšno reklamo, potem do kršitve ni prišlo.

Uporabniki elektronske pošte so v svojem poštnem nabiralniku najpogosteje že vajeni številnih reklamnih sporočil. Ker je v zadnjem času postalo pošiljanje nenaročenih reklamnih sporočil po

elektronski pošti izredno agresivno, se uporabniki upravičeno jezijo. Zaradi tega se je v mnogih državah pojavila težnja po prepovedi vsakega nenaročenega oglaševanja. Na splošno pa se uveljavlja stališče, da morajo biti nenaročene pošiljke opremljene z imenom in naslovom pošiljatelja ter da ima prejemnik možnost odpovedati nadaljnje pošiljke (ang. opt-out).

Prav v zadnjem času potekajo med podjetniškimi lobiji in ustvarjalci internetne zakonodaje srdite polemike o tem ali naj se v zakonodaji o internetnem oglaševanju sprejme in legalizira tako imenovana opt-in ali opt-out politika oglaševanja v internetu. Podjetniški lobiji se zavzemajo za slednjo, saj jim omogoča manjše stroške oglaševanja. Opt-out opcija oglaševanja namreč temelji na dejstvu, da lahko oglaševalci svobodno polnijo elektronske poštne predale uporabnikov z oglasno pošto, pri čemer ima naslovnik možnost pri pošiljatelju po e-pošti odpovedati nadaljnje pošiljanje reklamnih sporočil. Pri opt-in opciji oglaševanja pa mora oglaševalec za nadaljnje oglaševanje pridobiti odobritev naslovnika elektronskega predala.

Decembra 2001 je EU naredila velik korak proti prepovedi nezaželenih elektronskih sporočil, ki grozijo, da se bodo s spletnih elektronskih poštnih predalov razširila tudi na mobilno telefonijo. Evropski telekomunikacijski ministri so glasovali za prepoved nenaročenih komercialnih elektronskih sporočil. Ta prepoved je del osnutka zakona o zaščiti zasebnosti v elektronskih komunikacijah (EU States agree to pass Anti-spam law. Washington D.C. [URL: http://www.newsbytes.com/news/01/170700.html], 25.2.2002).

5.6 Sodniške pristojnosti in plačilo davka

Internet se zaradi svoje razsežnosti in nadaljnje širitve čedalje bolj uveljavlja tudi kot medij za trgovanje. Del interneta se namreč razvija v velikanski elektronski katalog, kjer si lahko izberemo poljubne izdelke iz katerekoli države. Na področju EU veljajo za prodajo po internetu enaki predpisi kot za prodajo po pošti.

Pomembno vprašanje, ki pri poslovanju na internetu vedno bolj stopa v ospredje je vprašanje plačila davka. Na splošno velja, da podjetja plačujejo davek tam, kjer so registrirana. Na internetu se zaplete ponavadi takrat, ko neko podjetje prodaja izdelke preko strežnika, ki se nahaja v drugi državi. V tem primeru ima lahko ta država določene zahteve za plačilo davka, ker je bila prodaja namreč izvršena preko strežnika na njenem ozemlju. Da ne bi prihajalo do dvojnega obdavčenja, se poskušajo takšni problemi reševati z meddržavnimi sporazumi.

Kupci pogosto negodujejo pri spletnem nakupovanju, saj so pogosto prisiljeni plačati davek za kupljeni izdelek, ki jim ga v matični državi ni treba. Države namreč pogosto zahtevajo od prodajalcev, da obračunavajo davek glede na kraj odprave pošiljke in glede na naslov dobave

pošiljke. To je zlasti problem za evropske države, zlasti države EU, ki temeljijo na davku na dodano vrednost. Ta davčna ureditev ni najbolj primerna za spletno trgovanje, saj davek pripada državi, v kateri je sedež prodajalca. To je eden od razlogov, zakaj je največ spletnih trgovin prav v ZDA, saj uporablja davčni sistem, ki je podoben slovenskemu davčnemu sistemu, veljavnem do leta 1999 (Jerman-Blažič, 2001, str. 181).

EU išče rešitve za ta problem, ZDA pa so leta 1998 sprejele zakon o zamrznitvi davkov pri spletnem trgovanju. Zlasti aktualno vprašanje ali je smiselno z neobdavčevanjem spodbujati internetno trgovanje ali pa naj države zaračunavajo svoj delež.

Pravno-formalno je pri poslovanju prek interneta pomembno, da lahko pogodbeni stranki kasneje dokažeta, da se je druga stran s pogodbo strinjala. To se lahko dokaže z elektronskim podpisom, ki omogoča prodajalcu, da dokaže avtentičnost naročila tako glede vsebine kot glede pošiljatelja. Elektronski podpis je namreč nadomestek lastnoročnega podpisa pri elektronski izmenjavi podatkov. Prednost takšnega podpisa pred običajnimi je v tem, da podpis poleg avtorstva dokumenta zagotavlja tudi njegovo neokrnjenost. Najmanjša sprememba dokumenta po podpisu povzroči, da podpis ni več veljaven. Zaradi omenjenih lastnosti predstavlja verodostojen oziroma varen e-podpis zadosten pogoj za sklepanje poslov. V nekaterih državah so že sprejeli zakonodajo, tudi pri nas v Sloveniji, po kateri je elektronski podpis enakovreden lastnoročnemu.

Sodna pristojnost je pravica in dolžnost sodišča, da posreduje v pravnem razmerju. V internetu ni pomembno, kje ima tožena stranka svoj fizični sedež, bistveno je, od kod kršitve izvirajo. Zato tuja sodišča, predvsem anglosaška, kot navezno okoliščino za določitev krajevne sodne pristojnosti uporabljajo inštitut tako imenovanega elektronskega sedeža. To je kraj, kjer je bila škoda povzročena oziroma je storilec resnično deloval.

5.7 Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)

Sporočanje pravno pomembnih in zavezujočih informacij v elektronski obliki ob pomanjkanju ustrezne zakonske ureditve lahko znatno ovira in povzroča splošno pravno negotovost. Zato je nujno potrebno zagotoviti varno pravno okolje za elektronsko poslovanje v domačem in mednarodnem poslovanju.

Prvi zakon o elektronskih podpisih je bil sprejet že leta 1995 v zvezni državi Utah v ZDA. Komisija Združenih narodov za mednarodno gospodarsko pravo (UNCITRAL) je leta 1996 sprejela Modelni zakon o elektronskem poslovanju, v pripravi pa so tudi enotna pravila o elektronskem podpisovanju. Tudi druge mednarodne organizacije, vključno s Svetovno trgovinsko organizacijo (WTO), se ukvarjajo s podobnimi vprašanji.

V okviru evropskih zakonodaj o elektronskem podpisu je prva zakon o elektronskih podpisih sprejela Nemčija leta 1997, sledile pa so ji še nekatere druge države, med njimi Avstrija in Italija. Evropska unija je z namenom poenotenja zakonodaj članic EU in z namenom pospeševanja elektronskega poslovanja in uporabe elektronskih podpisov leta 1999 sprejela direktivo: Okvir Unije za elektronske podpise[23]. Določila direktive so morale države članice udejaniti na nacionalni ravni do julija 2001. Direktiva obravnava vse vrste elektronskih podpisov in izpostavlja zlasti tiste, ki imajo enako pravno veljavo kot lastnoročni podpisi pri dokumentih v papirnati obliki (Jerman-Blažič, 2001, str. 114).

5.7.1 Zakon o elektronskem poslovanju in elektronskem podpisu v RS

Sprejem ustrezne zakonodaje v Republiki Sloveniji je bil zato nujno potreben za vključevanje v svetovno informacijsko družbo. Tako je slovenska vlada na predlog Centra za informatiko 24. februarja 2000 sprejela predlog zakona o elektronskem poslovanju in elektronskem podpisu ter ga poslala v obravnavo v državni zbor, kjer je bil sprejet 13. junija 2000.

Zakon je v skladu z direktivo o elektronskih podpisih EU in tudi razlikuje med elektronskimi in varnimi elektronskimi podpisi ter med certificiranimi potrdili (digitalni certifikati) in navadnimi potrdili. Čeprav je tudi slovenski zakon tehnološko nevtralen, saj se tehnologija varovanja podatkov izrazito hitro spreminja, trenutno samo digitalni podpisi na podlagi asimetrične kriptografije izpolnjujejo zahtevane pogoje kot varni elektronski podpisi.

Z novo ureditvijo se odpravljajo ovire, ki jih elektronskemu poslovanju postavljajo pravne norme, zasnovane in sprejete v času izključno papirnega poslovanja. Vzpostavlja se tudi varno okolje za preverjanje pristnosti elektronsko oblikovanih, shranjenih, poslanih, sprejetih ali kako drugače obdelanih podatkov.

Zakon o elektronskem poslovanju in elektronskem podpisu je razdeljen v pet poglavij, ki skupaj vsebujejo 55 členov.

V prvem poglavju zakon opredeljuje področje, ki ga ureja: elektronsko poslovanje ter uporabo podatkov v elektronski obliki in elektronskega podpisa v pravnem prometu ter določi pomen posameznih pojmov, uporabljenih v zakonu.

V drugem poglavju zakon ureja elektronsko poslovanje. Podrobneje je urejeno poslovanje z elektronskimi sporočili. Sledijo določbe, ki urejajo uporabo podatkov v elektronski obliki oziroma njihovo veljavnost in dokazno vrednost.

[23] A Community framework for electronic signatures

V tretjem poglavju zakon širše ureja elektronski podpis in delovanje overiteljev, ki so nujen pogoj za uporabo elektronskih podpisov. Vse overitelje in njihovo ponudbo storitev bi naj nadzoroval pristojni inšpektorat.

Ker gre za pomembno področje, kjer kršitev posameznih norm lahko resneje ogrozi zanesljivost elektronskega poslovanja in poseže v pravice drugih, so v četrtem poglavju določeni prekrški in kazni zanje.

Zadnje, peto poglavje predloga zakona vsebuje prehodne in končne določbe.

Za izvajanje zakona, ki je v celoti usklajen z določili primarne evropske zakonodaje, je v največji meri odgovorno Ministrstvo za informacijsko družbo.

Nekaj izvlečkov iz zakona o elektronskem poslovanju in elektronskem podpisu:

- Zakon zagotavlja elektronski obliki in elektronskemu podpisu enake možnosti kot dosedanji papirnati obliki.
- Za hranjenje podatkov v elektronski obliki je zelo pomemben tudi časovni žig, ki potrjuje, da so elektronski podatki resnično ostali celoviti in nespremenjeni od trenutka, ko so bili shranjeni, do trenutka uporabe.
- Zakon zato omogoča enostavno medsebojno priznavanje elektronskih podpisov znotraj Evropske unije ter širše priznavanje ob pogojih vzajemnosti oziroma s tem povezane podobnosti področne zakonodaje.
- Če ni drugače dogovorjeno, se za kraj, od koder je bilo elektronsko sporočilo poslano, šteje kraj, kjer ima pošiljatelj svoj sedež oziroma stalno prebivališče v času pošiljanja, za kraj prejema elektronskega sporočila pa kraj, kjer ima prejemnik sedež oziroma stalno prebivališče v času pošiljanja.
- Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu glede podatkov v papirni obliki ter ima zato enako veljavnost in dokazno vrednost.

5.8 Kazenski zakonik RS in vdori v računalniški sistem

Členi Kazenskega zakonika RS, ki se posredno ali neposredno nanašajo na vdore v računalniški sistem, ali na nepooblaščeno spreminjanje podatkov (Kazenski zakonik RS in vdori v računalniški sistem. [URL: http://www.arnes.si/si-cert/kz.htm], 20.3.2002):

- Zloraba osebnih podatkov, 154. člen
- Kršitev avtorske pravice, 158. člen
- Neupravičeno izkoriščanje avtorskega dela, 159. člen
- Neupravičen vstop v zaščiteno računalniško bazo podatkov, 225. člen
- Organiziranje denarnih verig in nedovoljenih iger na srečo, člen 234 b
- Vdor v računalniški sistem, 242. člen
- Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje, 309. člen

Zloraba osebnih podatkov in vdor v računalniško vodeno zbirko podatkov z namenom osebnega okoriščanja se po 154. členu zakona kaznuje z denarno kaznijo ali zaporno kaznijo de enega leta, pri zlorabah položaja uradne osebe pa z zaporom do dveh let.

Kršitev pravic iz avtorskega dela se po 158. členu kazenskega zakonika kaznuje z denarno kaznijo ali z zaporom do enega leta.

Neupravičeno izkoriščanje avtorskega dela se po 159. členu kazenskega zakonika, glede na težo kršitve, kaznuje z denarno kaznijo ali pa z zaporom od treh mesecev do treh let.

Neupravičen vstop v zaščiteno računalniško bazo podatkov se po 225. členu kazenskega kaznuje z denarno kaznijo ali zaporno kaznijo od treh mesecev do pet let, odvisno od povzročene škode in stopnje okoriščanja s podatki.

Organiziranje denarnih verig in nedovoljenih iger na srečo se po členu 234 b kazenskega zakonika kaznuje z zaporom od enega do osmih let, glede na storjeno premoženjsko škodo.

Vdori v računalniške sisteme se po 242. členu zakona kazenskega zakonika kaznujejo z zaporom do petih let.

Z zaporom do enega leta se po 309. členu kazenskega zakonika kaznuje, kdor izdela, si pridobi, proda ali da v uporabo pripomočke, ki so namenjeni za vdor v računalniški sistem.

6. Sklep

Število uporabnikov internetnih storitev po vsem svetu, kakor tudi v Sloveniji, še vedno hitro narašča, kar kažejo tudi zadnje raziskave projekta Raba interneta v Sloveniji (Raba interneta v Sloveniji: Uporabniki interneta v letu 2001. [URL: http://ris.org/publikacije/raba%20interneta-kazalo.htm], 20.3.2002), ki poteka v okviru Fakultete za družbene vede Univerze v Ljubljani. V Sloveniji naj bi tako bilo že 250 tisoč rednih uporabnikov interneta, ki uporabljajo internet

vsakodnevno, kar predstavlja 12% celotne populacije. Nekateri ponudniki dostopa na internet govorijo celo o številki 500 tisoč, vendar treba upoštevati, da mnogi štejejo svoje uporabnike dvakrat, v službi in doma. Po podatkih RIS-a pa naj bi se z internetom srečal že vsak tretji Slovenec.

S povečevanjem vloge interneta v življenju vse več uporabnikov njegovih storitev, pa se izvaja tudi vedno večji pritisk različnih interesnih skupin, ki jim internet predstavlja vedno večji kos odrezanega kruha, na regulativne in zakonodajne oblasti po usklajevanju zakonodaje na področju interneta in nadzoru njegovih vsebin.

Zakoni na področju interneta so še vedno šibka točka v vseh državah sveta, celo v ZDA, ki je zibelka interneta in ima tudi največ prakse pri sodnem obravnavanju internetnih kršitev. Usklajevanje zakonodaje na tem področju se zdi v zadnjih letih glavna naloga različnih svetovnih organizacij, inštitucij in držav z namenom poenotenja zakonodaje digitalnih medijev, ki bi omogočilo popolno sprostitev globalne uporabe internetnih storitev na mednarodni ravni brez ovir pri izvajanju komuniciranja, poslovanja in trgovanja na medmrežju med državami.
Vendar pa, ne glede na uspešnost državnih zakonodaj pri njihovi uskladitvi in njihovi kvaliteti v sami implementaciji in izvajanju, internet ni področje, kjer bi lahko regulator ali zakonodajalec, kdorkoli že to je, spal na lovorikah. Internet je živ organizem, ki se neprestano razvija na vse mogoče različne načine od storitev, ki jih ponuja do tehnologij, ki jih uvaja, zato se je resno bati, da zakonodaja in regulacija interneta nikdar ne bosta dohajala zahtevanih dopolnitev in uskladitev, ki jih bodo spremembe narekovale, tako, da bo vedno vsaj en korak zadaj.

Težave pri pisanju ustrezne internetne zakonodaje pa povzročajo tudi različni lobiji in interesne skupine, ki izvajajo pritisk na zakonodajne oblasti in regulativne inštitucije, kako naj se le-ta regulira oziroma prepušča samoregulaciji, saj glede na to, da je internet globalno medmrežje, ni last nobene oblasti oziroma države. Za samoregulacijo se zavzemajo zlasti zagovorniki svobode govora in tiska, katerim internet predstavlja zadnjo oazo v svetu reguliranih in nadzorovanih medijev. Za regulacijo interneta pa se zavzemajo zlasti poslovni oziroma podjetniški lobiji, katerih interes je zaščititi svoj vir dohodka pred različnimi zlorabami, ki jih internet kot svoboden, kaotičen in nepredvidljiv medij tehnološko omogoča, in pa z namenom ohranjanja pravice in možnosti agresivnega trženja svojih storitev.

Prav zaradi vseh mogočih zlorab, ki jih internet kot digitalen medij omogoča, od nadlegovanja, kratenja zasebnosti, kršenja avtorskih pravic, podjetniškega ali medvladnega vohunjenja, vdiranja v zasebna omrežja in kraje informacij, se je v svetu sprožil vsesplošni alarm pred grozečo nevarnostjo, ki vsakoletno napravi ogromno škode. Posledično temu sledi tudi pospešen razvoj različnih varnostnih tehnologij, katerih namen je zaščititi uporabnike med njihovo legitimno uporabo interneta.

Uporaba varnostne tehnologije od požarnih zidov, antivirusnih programov, zanesljive programske opreme, metod šifriranja pretoka informacij in učinkovitih sistemov nadzora, po možnosti podkrepljeno s strogo in učinkovito internetno zakonodajo, je vizija, tako se vsaj zdi, uporabe internetnih storitev v prihodnosti. Varnostna tehnologija bo postala najpomembnejši člen v razvoju internetnih tehnologij, ki bo morala vedno hoditi v korak s tehnološkim razvojem, in bo lahko že vnaprej predvidela možnosti zlorabe obstoječih tehnologij.

Največje pomanjkljivosti so v sedanjem trenutku na področju nezanesljivosti programske opreme, pomanjkljive standardizacije in legalizacije šifrirnih postopkov in neusklajenosti ter nedorečenosti internetne zakonodaje.

Zlasti programska oprema, na kateri slonijo računalniški sistemi po vsem svetu, zlasti osebni računalniki in strežniška programska oprema, je vedno pogosteje povzročitelj številnih varnostnih lukenj, zato se resno postavlja vprašanje o morebitni odpravi zaščite pred vsakršno odgovornostjo, ki jo uživajo proizvajalci programske opreme. Med potrošniki se je v teh letih pohoda programske opreme zasidral vtis, da je programska oprema izjema, ki ji ni treba zadostiti osnovnih varnostnih standardov. Če se nam pokvari strojna oprema, jo lahko reklamiramo, pri pomanjkljivostih programske opreme pa se nimamo kam pritožiti. Namreč pri zdajšnji ravni varnosti v najbolj razširjeni programski opremi je množično uničenje podatkov vedno bolj verjetna zgodba. Zdi se, da je pri razvoju programske opreme še vedno prvo vodilo razvoja povečevanje funkcionalnosti, ki pa bi jo bilo potrebno v prihodnosti podrediti večji pozornosti po varnosti in trdoživosti programske opreme. Tako bo potrebno zaradi varnosti v prihodnje izdelovati programsko opremo, katere varnostne pomanjkljivosti ne bodo odpravljene šele v deveti generaciji.

Na področju standardizacije in legalizacije različnih šifrirnih postopkov, zlasti asimetričnega šifriranja podatkov oziroma kriptografije javnega ključa se še vedno pojavljajo dileme glede potrebe po nadzoru in regulaciji nad šifriranjem podatkov, saj mnoge države, zlasti ZDA in Velika Britanija vztrajata, med drugim tudi zaradi državne varnosti pred terorističnimi napadi, pri predaji javnih ključev s strani overiteljev in drugih nosilcev enkripcijskih metod. Tako bi lahko oblasti v primerih ogrožene državne varnosti, ali pa tudi ne, prebirale pošto svojih državljanov in dešifrirale pretok informacij po internetu. Tak primer je npr. asimetrična enkripcijska tehnologija PGP, ki se uporablja predvsem v namene šifriranja poštnih elektronskih sporočil, je bila dolgo časa s strani ZDA obravnavana kot vrsta orožja, katerega izvoz je prepovedan.

Zlasti na področju interesov ohranjanja zasebnosti na medmrežju s šifrirnimi metodami in interesu držav po ohranjanju nadzora nad pretokom informacij se kažejo navzkrižni interesi, ki zavirajo sprejetje ustreznih tehnoloških standardov in pa tudi ustrezne internetne zakonodaje.

Na področju mednarodnega usklajevanja zakonodaj o internetnem kriminalu pospešeno potekajo prizadevanja po zamašitvi te vrzeli. Na to zlasti kaže podpis Konvencije o kriminalu v kibernetskem prostoru pod okriljem Sveta Evrope (European Commission), ki je bila novembra 2001 sprejeta v Budimpešti (30 states sign the Convention on Cybercrime at the opening ceremony. [URL: http://press.coe.int/cp/2001/875a(2001).htm], 18.3.2002). Pogodbo je podpisalo že več kot 30 držav in je od datuma njenega sprejetja odprta za vključitev novih članic podpisnic te konvencije. Tudi Slovenija se pripravlja na podpis konvencije, katere slovenski prevod je že v medresorskem usklajevanju. Vzpostavlja se tudi že delovna skupina, ki bo pripravila gradivo za sejo vlade in vse potrebno za podpis konvencije.

Glavni cilj konvencije je ustvariti skupno politiko, ki bo družbo ščitila pred spletnim kriminalom s sprejetjem ustrezne zakonodaje in spodbujanjem mednarodnega sodelovanja. Konvencija obravnava predvsem kazniva dejanja povezana s kršitvami avtorskih pravic, prevare povezane s kriminalom in otroško pornografijo in kazniva dejanja povezana z varnostjo omrežij.

V prihodnosti se bo na področju interneta odvijal predvsem boj med polariziranima interesoma tistih, ki želijo ohraniti internet kot medij svobodnega komuniciranja, ki je necenzuriran in nereguliran, in tistimi, katerih interesi stremijo k strogo omejenemu, nadzorovanemu in reguliranemu mediju bodisi iz varnostnih razlogov bodisi iz poslovnih interesov. Dejstvo je, da, ne glede na to, ali se bodo države odločale za metode večje regulacije interneta in dokončno uveljavitev slovesa ˝velikega brata˝, ki si je v zgodovini podredil vsak medij, ali pa bodo čutile, da se medmrežje lahko samoregulira, je potrebno spoznanje, da krivdo za večjo ali manjšo varnost interneta kot medija ne gre pripisovati njegovi naravi, temveč, da le-ta odseva razmere družbe. Internet je le še eden medij več preko katerega odsevajo medčloveški odnosi in kot tak ni in ne more biti neposreden vir zla, ki bi ga bilo potrebno v nedogled nadzorovati.

Literatura

1. Ahuja Vijay: Secure Commerce on the Internet. London: Academic Press, Inc., 1997. 298 str.
2. Barrett Daniel J.: Bandits on Information Superhighway: what you need to know. 1st edition. Bonn: O´Reilly & Associates, Inc., 1996. 229 str.
3. Chapman D. Brent, Zwicky Elizabeth D.: Building Internet Firewalls. 1st edition. Cambridge: O´Reilly & Associates, Inc., 1995. 517 str.
4. Jerman-Blažič Borka, et al.: Elektronsko poslovanje na internetu. 1. Natis. Ljubljana: Gospodarski vestnik, 2001. 206 str.
5. Schneir Bruce: E-mail security: how to keep your electronic messages private. New York: J.Wiley & Sons, Ltd., 1995. 365 str.
6. Shimmin Bradley: Effecitive e-mail: File transfer, Security and Interoperability. London: Academic press Limited, 1997. 292 str.
7. Toplišek Janez: Elektronsko poslovanje. 1.izdaja. Ljubljana: Založba Atlantis, 1998. 336.str.
8. Zakon o elektronskem poslovanju in elektronskih podpisih (ZEPEP). Ljubljana: Vlada Republike Slovenije, Center za informatiko, 2001. 60 str.

Viri

1. 30 states sign the Convention on Cybercrime at the opening ceremony. [URL: http://press.coe.int/cp/2001/875a(2001).htm], 18.3.2002.
2. A Community framework for electronic signatures. [URL: http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html], 6.3.2002.
3. Abraxas: Sishop 2.0. [URL: http://www.abraxas.si/sishop.htm], 15.5.2002.
4. Akademska in raziskovalna mreža Slovenije: Registracija domen. [URL: http://www.arnes.si/domene/registracija.html], 18.5.2002.
5. Anonymizer. [URL: http://www.anonymizer.com], 20.2.2002.
6. Berne Convention for the Protection of Literary and Artistic Works. [URL: http://www.law.cornell.edu/treaties/berne/overview.html], 6.3.2002.
7. Computer economics security review 2002. [URL: http://www.computereconomics.com/article.cfm?id=356], 10.5.2002.
8. Computer mail services: Spam cost calculator. [URL: http://www.cmsconnect.com/Marketing/spamcalc.htm], 10.5.2002.
9. Computer security institute: CSI/FBI Computer Crime and Security Survey. [URL: http://www.gocsi.com/press/20020407.html], 10.5.2002.
10. Council of Europe: Convention on Cybercrime. [URL: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185], 25.2.2002.
11. Council of Europe: Convention for the Protection of Human Rights and Fundamental Freedoms. [URL: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm], 27.2.2002.
12. Directive on the legal protection of computer programs. [URL: http://europa.eu.int/eur-lex/en/lif/dat/1a.eu.int/eur-lex/en/lif/dat/1996/en_396L0009.html], 25.2.2002.
13. Directive on Rental rights and Lending right and on certain rights related to Copyright in the field of Intellectual property. [URL: http://europa.eu.int/eur-lex/en/lif/dat/1992/en_392L0100.html], 25.2.2002.
14. Directive on the legal protection of databases. [URL: http://europa.eu.int/eur-lex/en/lif/dat/1996/en_396L0009.html], 25.2.2002.
15. Directive on the Protection of Consumers in respect of Distance Contracts. [URL: http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf], 27.2.2002.
16. Eon: commerce service provider: Transact 4 – infrastruktura za spletno poslovanje. [URL: http://portal.eon.si/eongroup/eon.jsp], 18.5.2002.
17. EU States agree to pass Anti-spam law. Washington D.C. [URL: http://www.newsbytes.com/news/01/170700.html], 25.2.2002.
18. European Union Directives Related to Electronic Commerce. [URL: http://www.bmck.com/ecommerce/eu.htm], 26.2.2002.
19. Gibson Research Corporation: ShieldsUP!. [URL: http://www.grc.com], 15.3.2002
20. Green paper on Copyright and Related rights in the Information Society. [URL: http://europa.eu.int/scadplus/leg/en/lvb/l24152.htm], 25.2.2002.
21. Guidelines for Consumer Protection in the Context of Electronic Commerce. [URL: http://www1.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm], 26.2.2002.
22. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [URL: http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM], 25.2.2002.

23. Guidescope. [URL: http://www.guidescope.com], 20.2.2002.
24. Hermes Plus: Rešitve in produkti. [URL: http://www.hermes-plus.si/ResitveProdukti/ResitveProdukti.shtml], 12.3.2002.
25. Hushmail. [URL: http://www.hushmail.com], 15.2.2002.
26. Internet Corporation for Assigned Names and Numbers. [URL: http://www.ICANN.org], 20.5.2002.
27. Kazenski zakonik RS in vdori v računalniški sistem. [URL: http://www.arnes.si/si-cert/kz.htm], 20.3.2002.
28. Modelni zakon o elektronskem poslovanju, UNCITRAL, 1996. [URL: http://www.uncitral.org/english/texts/electcom/ml-ec.htm], 26.2.2002.
29. OECD Ministerial declaration on the protection of Privacy on Global Networks. [URL: http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/61c1c8c0a31f9457c12566de00506c13/$FILE/12E81013.ENG], 27.2.2002.
30. Office of High Commissioner for Human rights; International Covenant on Civil and Political Rights. [URL: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm], 27.2.2002.
31. Proposal for Directive on Copyright and Related rights in the Information society. [URL: http://europa.eu.int/comm/internal_market/en/intprop/news/copy2.htm], 25.2.2002.
32. Raba interneta v Sloveniji: Uporabniki interneta v letu 2001. [URL: http://ris.org/publikacije/raba%20interneta-kazalo.htm, 20.3.2002.
33. Skbnet: Varnost na internetu. [URL: http://www.skb.si/html/skbnet/varnost_internet.html], 12.3.2002.
34. Stanford computer science education: Domain name grabbing. [URL: http://www-cse.stanford.edu/classes/cs201/projects-97-98/domain-names/problems/grabbing.html], 10.4.2002.
35. The Digital Millenium Copyright Act. [URL: http://www.loc.gov/copyright/legislation/dmca.pdf], 3.3.2002.
36. Universal declaration of Human Rights. [URL: http://www.un.org/Overview/rights.html], 27.2.2002.
37. U. S. Copyright Law. [URL: http://www.loc.gov/copyright/title17/], 6.3.2002.
38. VeriSign (Verisign. [URL: http://www.verisign.com], 15.4.2002.
39. WIPO Copyright Treaty. [URL: http://www.wipo.org/eng/diplconf/distrib/94dc.htm], 6.3.2002.
40. WIPO Performances and Phonograms Treaty. [URL: http://www.wipo.org/eng/diplconf/distrib/95dc.htm], 6.3.2002.
41. Zakon o avtorskih in sorodnih pravicah (Uradni list RS, št. 21/95).
42. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). [URL: http://www.dz-rs.si/si/aktualno/spremljanje_zakonodaje/sprejeti_zakoni/sprejeti_zakoni.html], 25.2.2002.