UNIVERZA V MARIBORU
EKONOMSKO-POSLOVNA FAKULTETA, MARIBOR

DIPLOMSKO DELO

VARNOSTNA POLITIKA INTERNETNEGA POSLOVANJA

SECURITY POLICY OF E-BUSINESS

Kandidatka: Polona LIPOVŠEK
Študentka rednega študija
Številka indeksa: 81640753
Program: visokošolski strokovni
Študijska smer: Finance in bančništvo
Mentor: dr. Samo BOBEK

Maribor, oktober, 2009

PREDGOVOR

V diplomskem delu sem prikazala zgodovino internetnega poslovanja in potek prehoda s klasičnega poslovanja na elektronsko. Predstavljeni so tudi modeli in vrste elektronskega poslovanja. Najpogostejši vrsti e-poslovanja sta B2C, torej poslovanje med podjetjem in kupcem, in B2B, poslovanje med dvema podjetjema.

Elektronsko poslovanje je v veliki meri že zamenjalo klasično poslovanje, saj ga najdemo v večini podjetij. S tem so tudi mala podjetja postala konkurenčna na trgu, saj jim elektronsko poslovanje omogoča nižje stroške. Na drugi strani pa tudi za kupce pomeni večjo možnost izbire, lažje komuniciranje s ponudniki, kakovostnejše izdelke.

Poleg naštetih prednosti pa ima elektronsko poslovanje tudi slabosti, s katerimi mora biti vsak posameznik pravočasno seznanjen. To so nevarnosti, ki nam grozijo ob uporabi elektronskega poslovanja, npr. virusi, črvi ipd. Ker se temu skoraj ni mogoče izogniti, se je potrebno pred njimi zavarovati. V diplomskem delu sem zato predstavila različne oblike zlorab in navedla na kakšen način se pred njimi zavarovati.

V diplomskem delu sem preučila tudi, kakšno je e-poslovanje med slovenskimi podjetji in jih nekaj naštela. Tovrstno poslovanje še ni uvedeno v vseh slovenskih podjetjih, vendar pa se to število vedno bolj povečuje. Podjetja se zavedajo, da poleg slabostim, bodo z elektronskim poslovanjem le pridobili konkurenčno prednost.

KAZALO VSEBINE

1 UVOD

1.1 Opredelitev področja in opis problema

Internet je poleg povezovanja poslovnih sistemov med seboj omogočil tudi povezovanje s strankami oziroma kupci, z državno in javno upravo itd. Zato internet teoretično odpravlja časovne in geografske ovire.
Preprosto rečeno elektronsko poslovanje pomeni »poslovati elektronsko«. Tovrstno poslovanje pa je predvsem pomembno na štirih področjih, in sicer pri:

- povezovanju med potrošniki in organizacijami,
- notranjem poslovanju organizacije,
- poslovanju med organizacijami in
- poslovanju državne administracije med seboj in z občani.

Elektronsko poslovanje ima številne prednosti glede časa in prostora, vendar pa ima tudi slabosti. Ena izmed teh je nevarnost, da nam hekerji zbrišejo ali spreminjajo osebne podatke preko interneta.

Zato je za zagotovitev varnosti in zanesljivosti uporabe internetnega poslovanja nujno potrebno poznavanje delovanja računalniških sistemov in možnosti računalniških zaščit, ki so na razpolago. Zaradi tega se bom v diplomskem delu osredotočila na same nevarnosti e-poslovanja in kako se pred njimi zaščiti. Poleg tega pa se bom dotaknila tudi standardov, ki so povezani z elektronskim poslovanjem.

1.2 Namen, cilji in osnovne trditve

Namen

Ker se poraja vprašanje ali je e-poslovanje preko interneta varno, bom v diplomski nalogi poskušala preveriti, katere metode in mehanizme lahko uporabimo, da bi bilo e-poslovanje na internetu varnejše za vse udeležence. Proučila bom naslednja vprašanja:
- Kaj je računalniški kriminal in kriminal na internetu?
- Katere so ostale najpogostejše nevarnosti interneta?
- Kako v osnovi varujemo informacijsko premoženje v podjetju ali organizaciji?
- S katerimi varnostnimi mehanizmi lahko zaščitimo podatke?
- Kako razvito je internetno poslovanje v slovenskih podjetjih?

Cilji

Cilji diplomske naloge so:
- predstaviti internetno poslovanje,
- prikazati razvoj e-poslovanja ter prehod s klasičnega na e-poslovanje,
- prikazati prednosti in slabosti e-poslovanja,
- predstaviti nevarnosti pri e-poslovanju in kako se pred njimi zaščititi,
- prikazati, kako je e-poslovanje razvito med slovenskimi podjetji.

Osnovne trditve - hipoteze

Trdim, da je elektronsko poslovanje za podjetja postala nuja, če želijo ostati konkurenčni in prodirati na nove trge.

Trdim, da bo uporaba elektronskega poslovanja še naraščala.

Trdim, da je prisotnih vedno več nevarnosti, ki bi lahko ogrozile e-poslovanje.

Trdim, da slovenska podjetja uporabljajo manj elektronskega poslovanja, v primerjavi z ostalimi evropskimi državami.

1.3 Predpostavke in omejitve raziskave

Predpostavke

Predpostavljam, da so podjetja seznanjena s slabostmi e-poslovanja in da se zato zaščitijo pred različnimi nevarnostmi, ki bi lahko škodile njihovemu poslovanju.

Predpostavljam, da naraščanje informatizacije prinaša mnogo prednosti za podjetja.

Predpostavljam, da bo internetno poslovanje v Sloveniji še naraščalo.

Omejitve

Pri analiziranju elektronskega poslovanja se bom najbolj poglobila v zaščito pred nevarnostmi, ki prežijo na poslovanje preko interneta.

Pri proučevanju elektronskega poslovanja bom omejena na dostopne podatke in na podatke, ki niso zaupni.

Pri predstavitvi zaščite e-poslovanja se bom osredotočila le na najpomembnejše informacije.

Pri analiziranju elektronskega poslovanja v slovenskih podjetjih se bom omejila na raziskave, katerih rezultati so dostopni na internetu.

1.4 Predvidene metode raziskave

Raziskava, ki jo bom opravila z diplomsko nalogo, bo statična, saj bo proučevala stanje v določenem trenutku.

Uporabila bom tudi metodo kompilacije, saj bom prevzela opazovanja, stališča, spoznanja, sklepe in rezultate drugih avtorjev in različnih strokovnjakov, ki delujejo na področju elektronskega poslovanja.

Uporabila bom metodo deskripcije, saj bom opisovala dejstva, procese in pojave ter njihova empirična potrjevanja. S to metodo bom opisala elektronsko poslovanje in podrobno predstavila nevarnosti e-poslovanja in kako se pred njimi zaščititi.

Literaturo in vire bom pridobila s knjižnično informacijskim sistemom in s pomočjo interneta. Uporabila bom samostojni induktivni pristop.

2 ELEKTRONSKO POSLOVANJE

2.1 Definicija

E-poslovanje avtorji različno definirajo. Nekateri celo trdijo, da splošne definicije e-poslovanja pravzaprav ni. Kljub temu pa so tukaj dane nekatere od definicij (Valh 2008):

- E-poslovanje pomeni »poslovati elektronsko«, torej pomeni vsa opravila v okviru svoje poslovne dejavnosti s pomočjo računalniških aplikacij in omrežij;
- E-poslovanje je katera koli oblika poslovanja, pri kateri stranke delujejo elektronsko, namesto da bi delovale fizično oziroma bi bile v neposrednem fizičnem stiku;
- E-poslovanje je alternativa »papirnim« metodam komunikacije in hranjenja informacij. Je poslovanje, pri katerem se uporablja čim manj papirja;
- E-poslovanje je po eni strani komercialna aktivnost, ki se izvaja po elektronskih omrežjih, po drugi strani pa prenos oz. izmenjava poslovnih dokumentov po elektronskih omrežjih;
- E-poslovanje je uporaba računalniškega omrežja za izboljšanje poslovanja podjetja oz. optimizacija poslovnih aktivnosti s pomočjo digitalne tehnologije in je prisotno v vsaki poslovni panogi;
- E-poslovanje je kakršna koli oblika poslovne ali administrativne transakcije oz. izmenjave informacij z uporabo kakršne koli informacijsko-komunikacijske tehnologije;
- V najširšem smislu e-poslovanje vključuje uporabo vseh oblik informacijske in komunikacijske tehnologije v poslovnih odnosih; sem sodijo trgovinske, proizvodne in storitvene organizacije ter tudi ponudniki informacij, potrošniki, državna uprava itd.

Izraz e-poslovanje izhaja iz angleškega izraza »e-business« oz. prvotno iz izraza »e-commerce«. E-poslovanje poleg komercialnih aktivnosti e-trgovanja vsebuje še poglobljeno sodelovanje s poslovnimi partnerji, elektronske transakcije ter tudi notranje poslovanje: razvoj in produkcija, finance, človeški viri, upravljanje s človeško silo, upravljanje informacij in znanja, upravljanje odnosov s strankami in upravljanje rizikov. (Valh 2008)

E-poslovanje se v bistvo deli na dva osnovna modela (Valh 2008):

- **Tradicionalno e-poslovanje:** elektronska izmenjava podatkov, sodelovanje omejenega števila partnerjev v specifičnih panogah, zaprta zasebna omrežja, poznani in preverjeni partnerji, strukturno okolje, možna regulacija.
- **E-poslovanje na internetu:** neomejeno število partnerjev na neomejenem tržišču, globalen obseg; odprta in nezavarovana omrežja, internet ter poznani in nepoznani partnerji, nestrukturirano okolje, regulacija ni možna.

2.2 Zgodovina e-poslovanja

Prve sledi e-poslovanja najdemo že na koncu šestdesetih let prejšnjega stoletja. Razvijejo se računalniške mreže in internet, združujejo se telekomunikacijske in informacijske tehnologije, pojavijo se prvi standardi. V sedemdesetih letih pride do finančnih prenosov v bankah, v začetku osemdesetih pa do prenosa datotek in računalniške izmenjave podatkov med podjetji. Pojavi se elektronska pošta in avtomatizacija pisarniškega dela.

Sredi osemdesetih let je dostopnost in izmenjava informacij preko interneta že večja, možni so pogovori preko interneta, saj se razvijejo klepetalnice in razne elektronske konference. Sredi devetdesetih let pa zaradi enostavne uporabe in objave informacij s spletnimi tehnologijami elektronsko poslovanje doživi velik vzpon, ki traja še danes. Od srede devetdesetih do danes pa so se podjetja že modernizirala z računalniško-informacijsko infrastrukturo in storitvami znotraj svojih okvirjev (intranet), tesnejša je povezava podjetij s svojimi partnerji, pojavljajo se nove vrste poslovanja in novi poslovni modeli, ki imajo znaten vpliv na ekonomske, socialne in politične spremembe v družbi in na posameznika. (Valh 2008)

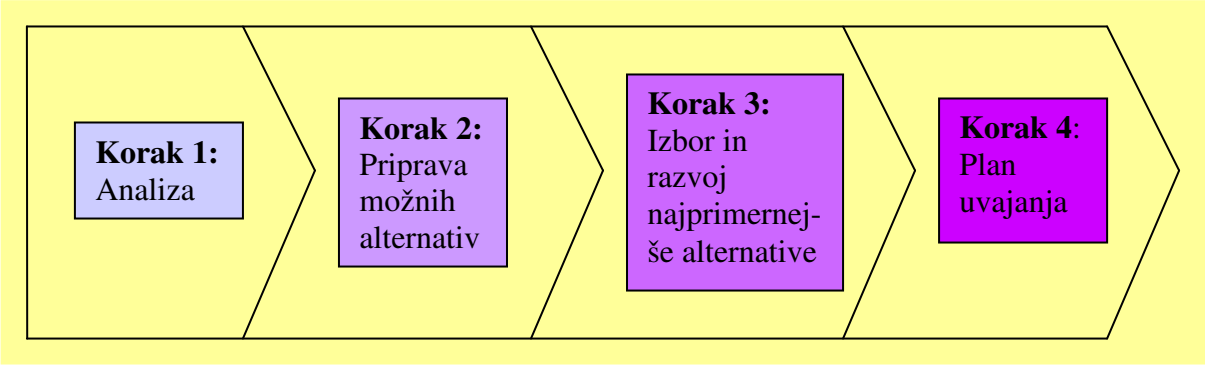
Mnogi avtorji označujejo leto 1996 kot prelomnico v zgodovini e-poslovanja. V tem letu se namreč začne množična uporaba interneta. V zadnjih desetih letih se vse bolj širi uporaba tehnologij interneta, ki omogoča globalno poslovanje brez geografskih mej. Omogoča hitrejše in bolj prilagodljivo poslovanje, ki se je sposobno odzivati na trgu, obenem pa širi meje podjetij tudi na globalni trg. (Valh 2008)

2.3 Prehod s klasičnega poslovanja na e-poslovanje

Prehod s klasičnega poslovanja na e-poslovanje poteka v več fazah. In sicer v prvi fazi se objavijo ponudbe ali povpraševanja na spletu, uporaba e-pošte je v prehodni fazi. Tukaj še ne gre za neposredno povezovanje med podjetji, e-pošta pa nadomešča faks in telefon. V drugi fazi že poteka prava elektronska izmenjava posameznih dokumentov (nabava, prodaja), v tretji fazi pa se pojavljajo različne oblike sodelovanja med podjetji, ustanavljanje virtualnih organizacij in internetnih podjetij. V zadnji četrti fazi pa poteka integracija in dinamično povezovanje vseh poslovnih partnerjev v verigi. (Valh 2008)

Na naslednji sliki lahko vidimo osnovne korake metodologije razvoja strategije e-poslovanja.

Slika 1: Metodologija razvoja strategije e-poslovanja



Vir: Valh, 2008

Cilji po posameznih korakih (Valh 2008):

- Pri analizi je glavni cilj poiskati priložnosti in grožnje e-poslovanja za podjetje. Potrebno je izvesti analizo zunanjega in notranjega okolja ter predvideti priložnosti e-poslovanja. Rezultati analize so glavne strateške usmeritve v povezavi z e-poslovanjem.

- V drugem koraku je cilj oblikovanje več možnih alternativ strategije e-poslovanja. Potrebno je izbrati model e-poslovanja, pripraviti ponudbo za kupce, poiskati vire in razjasniti vire prihodkov.

- V tretjem koraku je potrebno oceniti ustreznost, sprejemljivost in izvedljivost alternativ ter izbrati najustreznejšo alternativo. Rezultat je samo ena najbolj ustrezna, sprejemljiva in izvedljiva alternativa strategije e-poslovanja.

- Cilja v četrtem koraku sta izdelan plan akcij uvajanja izbrane strategije in določeni časovni termini za uvajanje. Potrebno je določiti akcije za dosego cilja, merski sistem in možnih tveganj. Končna rezultata sta akcijski načrt, ki zajema ljudi, sisteme, procese in ostalo ter zbirka merskih indikatorjev.

V tabeli so povzete razlike med klasičnim poslovanjem in e-poslovanjem.

Tabela 1: Primerjava klasičnega poslovanja in e-poslovanja

KLASIČNO POSLOVANJE	E-POSLOVANJE
Prodaja poteka fizično v trgovinah	Prodaja poteka »online«
Prodajajo se materialne dobrine	Prodajajo se tudi digitalni proizvodi
Planiranje proizvodnje poteka interno znotraj proizvodne organizacije	Uporabljajo se e-katalogi, e-tržnice, e-dražbe
Uporabljata se intranet in tradicionalna računalniška izmenjava podatkov	Uporablja se intranet, ekstranet in internet
Papirni dokumenti (računi, ponudbe…)	Elektronski dokumenti (računi, ponudbe…)
Izdelek je v središču	Kupec je v središču
»Push« proizvodnja (izdelki se najprej proizvedejo, šele nato prodajajo)	»Pull« proizvodnja (izdelki se prodajo, preden se proizvedejo)
Velike zaloge izdelkov/storitev	Majhne zaloge, informacije nadomeščajo zaloge
Standardni izdelki	Masovna kustomizacija izdelkov
Linearne oskrbne verige	Središčno organizirane oskrbne verige, majhni fiksni stroški poslovanja

Vir: Valh, 2008

2.4 Vrste elektronskega poslovanja

E-poslovanje (povzeto po Kovačiču, 2004) je pomembno predvsem na štirih področjih, in sicer pri poslovanju:

- med podjetji (B2B)
- med podjetji in potrošniki (B2C)
- med potrošniki (C2C)
- med podjetji in javno oziroma državno upravo (B2G)
- med državljani in javno oziroma državno upravo (C2G)
- znotraj javne oziroma državne uprave (G2G)

Za opise področij e-poslovanja uporabljamo angleške kratice, ki so sestavljene iz krajšav izrazov za udeležence e-poslovanja (Valh 2008):

- B = »Business« (posel) – poslovni svet, podjetja.
- C = »Consumer« (potrošnik) – porabnik, stranka, kupec.
- G = »Governement (vlada), tudi A = »Administration« (administracija) – javna uprava oz. vladna, državna administracija.
- E = »Employees« (zaposleni) – zaposleni v organizaciji oziroma podjetju.
- 2 = »To« (proti, k, med) – gre za kratico, ki označuje razmerje med udeleženci e-poslovanja.

Vrste e-poslovanja lahko prikažemo tudi s tabelo.

Tabela 2: Vrste e-poslovanj

	B Podjetje, organizacija	**C Potrošniki, državljani**	**G Javna uprava**
B Podjetje, organizacija	**B2B Podjetje – podjetje** npr. informiranje, e-trgovina	**B2C Podjetje-potrošnik** npr. informacije, e-trgovina	**B2G Podjetje-javna uprava** npr. oskrba javnih služb
C Potrošniki, državljani	**C2B Potrošnik-podjetje** npr. primerjava cen	**C2C Potrošnik-potrošnik** npr. e-dražbe, e-pošta, blogi	**C2G Potrošnik-javna uprava** npr.e-davki
G Javna uprava	**G2B Javna uprava-podjetje** npr. informiranje	**G2C Javna uprava-potrošnik** npr. informiranje, e-uprava	**G2G Javna uprava-javna uprava** npr.koordinacija

vir: Valh, 2008

Po ocenah analitikov pomeni elektronsko poslovanje med podjetji, merjeno v vrednosti transakcij, najpomembnejši delež elektronskega poslovanja. Zajema različne oblike

poslovanja od elektronskega bančništva za pravne osebe, povezav med podjetjem in njegovimi kupci, do sodelovanja v virtualnih organizacijah. Elektronsko poslovanje med podjetji in potrošniki je pogosto zmotno opredeljeno kot najpomembnejša oblika poslovanja. Razlog lahko iščemo v tem, da nam je kot potrošnikom najbližja, saj jo v vsakdanjem življenju najpogosteje srečujemo. Primeri elektronskega poslovanja med podjetji in potrošniki so elektronsko bančništvo za fizične osebe, elektronsko trgovanje, izobraževanje na daljavo itd. elektronsko poslovanje med potrošniki je namenjeno interakciji potrošnikov, ki na elektronski način bodisi komunicirajo ali poslujejo. Posebno področje elektronskega poslovanja predstavljajo vrste, kjer kot subjekt nastopa javna oziroma državna uprava. (Kovačič 2004)

Čeprav je pobuda za razvoj in razmah elektronskega poslovanja nastala v poslovnem okolju, je zaradi različnih razlogov pomemben tudi razvoj elektronskega poslovanja javne in državne uprave. (Kovačič 2004)

2.5 Modeli elektronskega poslovanja

Vpeljava elektronskega poslovanja v podjetje ne pomeni le nakupa informacijske in komunikacijske tehnologije, ampak tudi vrsto sprememb v poslovanju. Elektronsko poslovanje vpliva na razvoj novih poslovnih modelov, prenovo poslovnih procesov, sprememb v poslovni kulturi, organizacijski strukturi, vodenju itd. Spremembe v načinu poslovanja, kot odraz vpeljave elektronskega poslovanja so povzročile tudi nove poslovne modele. Model elektronskega poslovanja je način poslovanja, s katerim organizacija dosega dodano vrednost na podlagi interneta kot distribucijske poti. Modele elektronskega poslovanja lahko razdelimo na več načinov. V strokovni literaturi zasledimo delitve glede na način, cilje in namen elektronskega poslovanja. Za naše razumevanje tematike lahko modele elektronskega poslovanja delimo na (Kovačič 2004):

- spletno oglaševanje,
- virtualne skupnosti,
- spletno trgovino,
- posredniški model,
- informacijske portale,
- predplačniški model.

V praksi se našteti modeli lahko medsebojno prepletajo, kar otežuje enolično razvrščanje. Potrebno pa se je tudi zavedati, da se elektronsko poslovanje zelo hitro razvija in s tem tudi modeli. (Kovačič 2004)

2.5.1 Spletno oglaševanje

Spletno oglaševanje je podaljšek tradicionalnega oglaševanja, ki izrablja splet kot dodatno komunikacijsko pot. Namen spletnega oglaševanja je prek spletnega mesta ponuditi informacije in storitve kupcu. Spletno mesto je zaključena celota spletnih strani. Spletna mesta pogosto vsebujejo tudi reklamna sporočila drugih organizacij, s katerimi podjetja ustvarjajo prihodek na osnovi »oddajanja prostora«. Spletno oglaševanje se čedalje bolj posveča dodatnim storitvam, s katerimi želijo prodajalci vzbuditi in ohraniti odnos s kupcem. (Kovačič 2004)

2.5.2 Virtualne skupnosti

Virtualne skupnosti so pravzaprav oblika spletnega oglaševanja. Za razliko od spletnega oglaševanja so neprofitabilne. Temeljijo na lojalnosti uporabnika in najpogosteje zbirajo brezplačne informacije ter ponujajo brezplačno strokovno pomoč in izmenjavo izkušenj. (Kovačič, 2004)

Vir dohodka virtualne skupnosti so članarine in oglaševanje. Virtualne skupnosti se kot sestavni člen lahko pojavljajo v poslovnih modelih e-nakupovalnega centra, trga zunanjih izvajalcev ipd. Cilj je povečati potrošnikovo zvestobo in bolj ekonomično združevanje manjših podjetij za skupen nastop v postopku naročanja in nabave. (Valh 2008)

2.5.3 Spletna trgovina

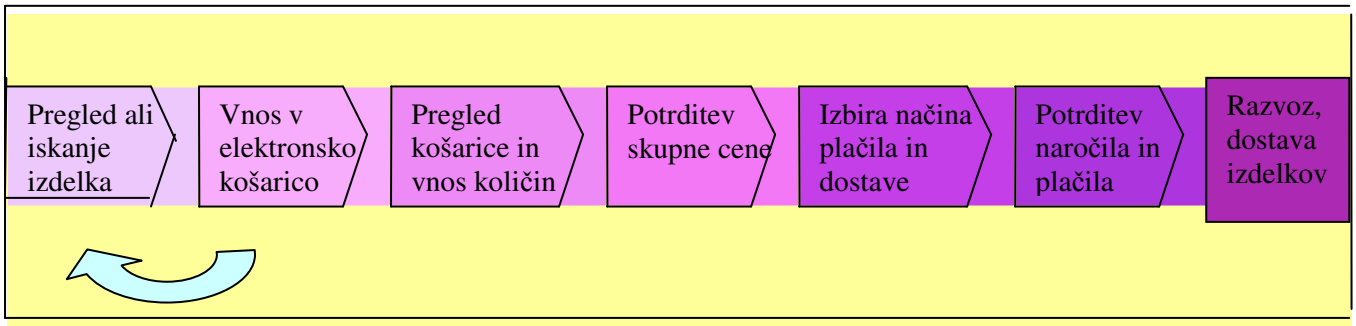
Je pravzaprav analogija klasični trgovini, vendar svoje proizvode ali storitve prodaja preko spleta. Včasih gre samo za dodatno obliko prodaje, ki dopolnjuje siceršnje (klasična, kataloška…), nekatera podjetja pa so bila ustanovljena na novo prav z namenom tovrstne prodaje. Pogosto spletno trgovino uporabljajo proizvajalci, ki želijo svoje izdelke prodajati brez posrednikov. (Kovačič 2004)

Pri spletni trgovini (po Valhu, 2008) gre za e-poslovanje B2C, ki jo ločimo na:

- **Izložbo za izdelke**: ni transakcij, torej e-trženje, marketing. Navadno je to spletna stran, kjer podjetje predstavlja svoje izdelke in storitve s slikami, video vsebino, katalogi, ceniki. Običajno je na spletni strani še zgodovina in opis podjetja ter blagovnih znamk, reference, priznanja, certifikati, podatki o kontaktih itd.
- **Pravo e-trgovino**: tu lahko izdelke tudi naročimo in plačamo.

Na naslednji sliki vidimo primer naročila in plačila izdelkov preko spletne trgovine.

Slika 2: Primer poslovanja s pomočjo e-trgovine



Vir: Valh 2008

Značilnost takega modela je zbiranje izdelkov za nakup, priprava ponudbe in plačilni sistem. Logistika, transport oziroma dostava blaga so sicer del poslovnega modela, vendar se ne morejo izvesti elektronsko, razen če gre za izdelke v elektronski obliki. Ponavadi se v e-trgovinah plačuje s plačilno kartico. (Valh 2008)

2.5.4 Posredniški model

Povezuje kupce in prodajalce ter omogoča izmenjavo in prodajanje različnih dobrin neposredno med fizičnimi in pravnimi osebami. Spletno mesto, ki predstavlja posredniški model elektronskega poslovanja, praviloma živi od oglasov. Najvidnejša predstavnika posredniškega modela sta blagovna borza in avkcija.
Blagovne borze so spletna mesta, kjer se trguje z materialnimi dobrinami. Zelo pogosto so povezane z določeno industrijsko panogo, npr. farmacevtsko, kemično, avtomobilsko ipd. Značilnost blagovnih borz je, da se poleg nakupa in prodaje izvajajo tudi ostale storitve, kot so analiza trga, pogajanja in ostale posredniške storitve. Posredniki svoje storitve plačujejo iz članarine ali provizije. Avkcije pa so najbolj množičen posredniški model elektronskega poslovanja. Zanjo je najbolj značilen angleški tip avkcije, pri kateri sodeluje en ponudnik, ki prodaja en proizvod, in več potencialnih kupcev. Kupci prek spletnega mesta oddajajo svoje ponudbe, prodajalec izbere najugodnejšo, ki ne sme biti manjša od vnaprej določene najnižje možne ponudbe. Avkcije trajajo nekaj dni in so pogosto specializirane za prodajo določenih artiklov. (Kovačič 2004)

2.5.5 Informacijski portali

So ena izmed novosti, ki jih je prinesel splet, saj pred tem ni bilo na voljo toliko brezplačnih informacij. Informacijski portali se običajno financirajo z oglasi, ki jih je tam možno objavljati. Nekateri portali, predvsem tisti z ozko specializirano vsebino, so svojim uporabnikom že začeli zaračunavati dostop do svojih strani. (Kovačič 2004)

2.5.6 Predplačniški model

Predplačniški model je izvedenka informacijskega portala. Spletno mesto je najpogosteje visoko specializirano in ponuja kvalitetne informacije. V praksi je del portala brezplačen, preostanek pa je plačljiv – dostopen samo predplačnikom. (Kovačič 2004)

2.6 Razlogi za uvedbo elektronskega poslovanja

Elektronsko poslovanje (Kovačič 2004) ne glede na obliko povezovanja s poslovnimi partnerji ali vrsto prinaša podjetjem, udeležencem takšne oblike poslovanja, neposredne koristi v obliki stalnega:
- zniževanja stroškov nakupa,
- zniževanja obsega zalog,
- skrajševanja poslovnega cikla,
- razvijanja učinkovitejše in uspešnejše pomoči in povezovanja z njihovimi odjemalci ter
- zniževanja stroškov prodaje in trženja ter ustvarjanja novih tržnih priložnosti.

2.6.1 Nižji stroški nakupa

Proces nakupa oziroma poslovni postopki, ki potekajo med kupcem in dobaviteljem, vezani na nakup, so dokaj kompleksni, intenzivni in spremljani z množico dokumentov v obeh

smereh. Podjetja iščejo možnosti znižanja nabavnih stroškov skozi združevanje naročil in tesnejše nakupno in razvojno sodelovanje s svojimi ključnimi dobavitelji. Na ta način lahko pričakujejo količinske popuste in tesnejše in neposredno povezovanje njihovih proizvodnih procesov. (Kovačič 2004)

Po izkušnjah podjetij kaže, da neposredno povezovanje organizacijam v procesu nakupa znižuje zlasti stroške na področju samega izvajanja procesa ter izdelave in pošiljanja dokumentov. Avtomatizacija postopkov in prenova poslovnih procesov omogoča zaposlenim več časa za pogajanja o boljših nakupnih pogojih in ustvarjanje boljših odnosov z dobavitelji.
(Kovačič 2004)

2.6.2 Zmanjšanje obsega zalog

Slabše kot je organizacija povezana s svojimi dobavitelj, večje so njene potrebne lastne zaloge surovin, materialov in polproizvodov, s katerimi lahko pravočasno oskrbuje svoj proizvodni proces. Večji obseg zalog po drugi strani obvezno pomeni za organizacijo višje stroške, običajno pa ne tudi pričakovanega hitrejšega in ustreznejšega odzivanja na potrebe odjemalcev. (Kovačič 2004)

Elektronsko poslovanje na tem področju odpira tudi nove možnosti in izzive. Organizacije, ki so neposredno poslovno in tehnološko povezane v proizvodni verigi, se lahko izognejo dvojnemu skladiščenju tako, da kot izhodno iz proizvodnje oziroma vhodno v naslednjo fazo proizvodnje uporabljajo skupno skladišče. Običajno tako podjetje, ki v verigi sledi, uporablja kot skladišče vhodnih elementov v svojo proizvodnjo neposredno kar izhodno skladišče svojega dobavitelja. Dobro povezane organizacije lahko ob načrtovanju lastnega proizvodnega procesa neposredno vplivajo tudi na proizvodni proces svojih ključnih dobaviteljev. Na ta način si ob pravem času in na pravem mestu zagotavljajo optimalne količine vhodnih elementov ter močno znižujejo ali celo odpravljajo lastne in dobaviteljeve zaloge in stroške skladiščenja. (Kovačič 2004)

2.6.3 Skrajšanje poslovnega cikla

Poslovni cikel predstavlja celoten čas, ki je potreben za razvoj, izdelavo in posredovanje proizvoda odjemalcu. Krajši poslovni cikel pomeni med drugim nižje stroške in hitrejši odziv na dinamične zahteve trga ter s tem seveda bistveno primerjalno prednost pred ostalimi proizvajalci. (Kovačič 2004)
Elektronsko poslovanje nam v primeru povezovanja organizacije z njenimi dobavitelji in kupci omogoča bistveno hitrejše pošiljanje in sprejemanje naročil, računov, prometnih in ostalih dokumentov. Internet je na tem področju ponudil in že tudi uveljavil neposredno povezovanje in delo skupin, ki se sicer nahajajo na različnih lokacijah kjer koli po svetu.
(Kovačič 2004)

2.6.4 Razvijanje učinkovitejše in uspešnejše pomoči in povezovanje z odjemalci

S tem, ko organizacija prek interneta omogoči svojim odjemalcem, to je kupcem izdelkov ali uporabnikom storitev, podroben opis svoje ponudbe in neposreden vpogled v stanje oziroma status njihovih naročil, lahko močno razbremeni svojo prodajno službo ter dvigne raven zaupanja in zadovoljstva odjemalcev. Organizacije, ki imajo za uspešno uporabo svojih proizvodov organizirano tehnično pomoč, v ta namen vse več uporabljajo internet. Velika računalniška podjetja lahko z uporabo interneta samo z zagotavljanjem neposrednega dostopa in posredovanja dopolnitev in novih verzij programov ter pomoči pri uporabi ter odpravi napak letno prihranijo po nekaj deset milijonov ameriških dolarjev. (Kovačič 2004)

2.6.5 Znižanje stroškov prodaje in trženja ter ustvarjanje novih tržnih priložnosti

Pri individualni prodaji je obseg prodaje omejen s številom razpoložljivih prodajalcev. Uporaba interneta odpravlja v primeru potrebe po povečanju prodajnih zmogljivosti fizični problem širitve, ki izhaja iz omejitev možnega števila prodajalcev, ob tem pa ne povzroča skoraj nobenih dodatnih stroškov. Razen tega internet odpira možnosti neposrednega naročanja in odpravlja časovno zamudno ročno izpolnjevanje naročil. Namesto tega se zaposleni v prodaji lahko bolj neposredno posvečajo prodajnim, zlasti pa poprodajnim aktivnostim, ki ustvarjajo in ohranjajo zadovoljstvo kupcev. (Kovačič 2004)

2.7 Prednosti e-poslovanja

E-poslovanje ima za podjetja ali organizacije številne prednosti (Valh 2008) predvsem zaradi:

- **Neposrednih komunikacijskih povezav in sprotne interakcije**, ki omogočajo nižje stroške nabave, prodaje, trženja in komunikacij; učinkovito nabavo, nove, krajše prodajne in nabavne kanale; tesnejše povezave s poslovnimi partnerji; nižje administrativne in transakcijske stroške ter večjo hitrost transakcij; znižanje obsega zalog, lažjo vključitev v oskrbovalne verige; hitrejši doseg trga, lažjo analizo trga, hitrejše povratne informacije; učinkovito in uspešno pomoč strankam, boljšo skrb za stranke, učinkovitejše poprodajne storitve; hitrejše prilagajanje spremembam na trgu; možnost takojšnje distribucije storitev in izdelkov; neposreden dostop do potencialnega kupca ali potrošnika z možnostjo oblikovanja posebej prirejene ponudbe; globalizacijo poslovanja po celem svetu.
- **Globalizacije poslovanja,** ki prenese širši krog potencialnih partnerjev; dostop do večjega, globalnega tržišča in s tem krajevno neodvisno neodvisnost; internacionalnostjo, poslovanje preko meja posameznih držav; ustvarjanje novih tržnih priložnosti; večjo konkurenčnost, manj odvisno od velikosti podjetja; dodatno možnost oglaševanja, novi medij (splet).
- **Avtomatizacijo poslovnih procesov,** ki omogoča krajše procese obdelave naročil; krajše razvojne, proizvodne, nabavne in logistične cikle; vzporednost izvajanja posameznih poslovnih funkcij; manj napak zaradi tega, ker je izključen človeški faktor; hitro in preprosto ažuriranje informacij, lažji dostop do informacij; večji nadzor nad opravljenim delom; učinkovitejše poslovne modele z višjo stopnjo produktivnosti; poslovanje 24 ur dnevno, časovno neodvisnost.

Prednosti, ki so jih deležni potrošniki, pa so:
- Hitrejše odkrivanje najugodnejšega ponudnika zaželenega izdelka ali storitve na poljubni lokaciji v svetu ob poljubnem času,
- nižje cene za boljšo kakovost, več različnih, cenejših storitev,
- oblikovanje izdelkov po želji kupca,
- hitrejša odzivnost na potrebe in želje kupca, hitrejša dobava,
- velika možnost dostopa do informacij,
- ni potrebnega čakanja na blagajni ali v gneči na cesti.

2.8 Pomanjkljivosti e-poslovanja

E-poslovanje ima tudi nekaj pomanjkljivosti (Valh 2008), in sicer naslednje:

- **Težave s kadri** pomanjkanje dovolj usposobljenega in izobraženega kadra za uvajanje in integracijo e-poslovanja; visoki stroški izobraževanja; nenehno izpopolnjevanje in prilagajanje na novosti; organizacijske težave znotraj podjetij (tudi odpuščanje starejših delavcev;
- **Težave potrošnikov:** možnost nepravilne obveščenosti potrošnika o izdelku ali storitvi; potrošniki se težje posvetujejo, ker ni posrednikov ali prodajnih agentov; omejene možnosti pogajanja; nezaupanje v tehnologijo in internet; prepričanje potrošnikov, da je e-poslovanje drago in tvegano;
- **Neetična dejanja:** vprašanje varnosti informacij: kršitve zasebnosti potrošnikov; poslovno vohunstvo; zloraba omrežij, vdori v plačilne sisteme; kršenje pravic intelektualne lastnine;
- **Tehnične pomanjkljivosti:** pomanjkljivi sistemi varnosti in zaupnosti; vprašanje poenotenih rešitev in standardov, neustreznost standardov; nezadostna telekomunikacijska in informacijska infrastruktura; dodatni stroški, povezani z nabavo opreme za e-poslovanje; veliki stroški za zagotavljanje kar največje možne stopnje varnosti; izpad omrežnih povezav do interneta in znotraj organizacije;
- **Netehnične pomanjkljivosti**: pravne pomanjkljivosti, kot so pravna podlaga pogodb, reševanje sporov, davki, carina…; zakonodaja in standardi še ne predvidevajo vseh možnih okoliščin; koristi e-poslovanja so v nekaterih primerih težje merljive.

Pomembno je vedeti, da ima e-poslovanje tudi nekatere slabosti in je zato dobro, da se jih zavedamo. Nekatere težave e-poslovanja so specifične za določeno vrsto e-poslovanja. E-poslovanje je del procesa globalizacije in spreminjanje družbe iz industrijske v postindustrijsko oz. informacijsko družbo (Valh 2008).

2.9 Kaj bo prinesla porast e-poslovanja v prihodnje

Kljub napakam in neuspehom posameznih podjetij narašča količina e-poslovanja za 15 do 25% letno. Rast e-poslovanja bo povečala celoten obseg trgovine. Približno 80% e-poslovanja se bo odvijalo izključno med podjetji in bo povzročilo hitrejši prenos in razvoj informacijskih tehnologij. S tem se bo izboljšal dostop do informacij na trgu. Številne informacije bodo na voljo uporabnikom internetnih storitev (Valh 2008).

Posebnih prednosti bodo deležna manjša in srednja podjetja, ki lahko precej ceneje postavijo virtualno kot pa resnično trgovino. S širitvijo na internet namreč odpirajo nove posle, saj niso več tako odvisna od posrednikov, preprodajalcev in agentov. S široko ponudbo na internetu pridobijo tudi potrošniki, ki lahko izbirajo različna razmerja med kakovostjo in ceno. Potrošniki bodo postavljeni v novo, osrednjo aktivno vlogo, saj bodo imeli več vpliva na končni izdelek ali storitev, ki ga želijo. (Valh 2008)

Poveča pa se tudi možnost oglaševanja za posameznike in ne samo za podjetja. Dejstvo je, da bodo v prihodnosti uspevali le tisti posamezniki in organizacije, ki bodo od svojih strank dobili potrdilo o zadovoljstvu z delom. To jim bo uspelo le s kakovostnimi storitvami in dobro komunikacijo z uporabniki svojih storitev. Na drugi strani pa prednosti e-poslovanja koristijo tudi proizvajalci, saj lahko globalno nabavljajo sestavne dele, komponente in polproizvode po nižjih cenah. (Valh 2008)

Z razmahom e-poslovanja se pojavljajo tudi nevarnosti. Morda bodo razpadle obstoječe preskrbovalne verige in se bo povečala odvisnost od velikih mednarodnih družb. Če bo rast e-poslovanja povečala celoten obseg trgovine, je nevarnost tudi v tem, da bo največ pridobil razviti in povezani del sveta. V državah, kjer ne bodo imeli dostopa do interneta, ne bodo mogli koristiti prednosti e-poslovanja. Poleg dostopa, za katerega je potreben kapital, pa je nujno tudi strokovno znanje, zato bodo na tem področju pridobile države, ki bodo imele kapital in možnost, da ponudijo ustrezno izobraževalno delovno silo. S širitvijo e-poslovanja se pojavlja nevarnost, da bodo precej izgubili tudi domači proizvajalci in dobavitelji. Prvi bodo lahko izgubili obstoječe stranke, saj jim bo na voljo več različnih proizvajalcev, ki bodo proizvajali izdelke različnih kakovosti, barv, lastnosti po različnih cenah. Tako bodo potrošniki imeli možnost izbire in lahko se zgodi, da bodo domače proizvajalce zamenjali s tujimi. Prav tako pa se lahko zgodi, da bodo na obrobje potisnjeni tudi domači dobavitelji, saj bodo proizvajalci lahko nabavljali določeno blago neposredno in po nižjih cenah. (Valh 2008)

3 NEVARNOSTI PRI E-POSLOVANJU

Večina uporabnikov interneta je zaskrbljena glede varnosti na internetu. Zaradi tega veliko ljudi ne zaupa osebnih podatkov preko interneta ali pa se prej prepriča o tem, kako so podatki zavarovani pri določeni osebi oziroma podjetju. (Seely 2002)

Zagotavljanje varnosti na internetu pomeni doseganje naslednjih ciljev (Hurley 2002) :
- Zasebnost: zagotovljeno naj bi bilo, da nihče ne bo bral naše elektronske pošte in imel dostop do podatkov, ki smo jih poslali preko interneta
- Avtentičnost: ta nam pove, da naj bi bili podatki na spletu legitimni oziroma zakoniti. Torej, če prejmemo dokument preko interneta, mora biti zagotovljeno, da prihaja od pooblaščene osebe, ne pa od osebe, ki se pretvarja, da je zakonita oseba.
- Poštenost: zagotavlja, da tako pošiljatelj kot prejemnik nista prilagodila oziroma ponaredila podatkov.
- Nadzor: pri nadzoru se želi preprečiti razne zlorabe, ki so vsakodnevno prisotne na internetu.

V nadaljevanju so predstavljene nevarnosti, ki so prisotne pri elektronskem poslovanju.

3.1 Računalniški kriminal in kriminal na internetu

Računalniški kriminal pomeni uporabo informacij in komunikacijskih tehnologij pri storitvi kaznivega dejanja zoper osebo, lastnino, organizacijo ali informacijski sistem. Tu gre za kakršno koli kriminalno dejavnost, ki zajema kopiranje, odstranitev, vmešavanje, vdor, uničenje ali drugo manipulacijo računalniškega sistema, računalnika, podatk0ov ali računalniških programov Informacijski sistemi, omrežja in komunikacijske naprave postajajo vse bolj povezani, kar povečuje možnost vnosov, manipulacij, oviranj, uničenj in kraj podatkov, ki se nahajajo ali prenašajo med temi sistemi. Današnja družba je postala zelo odvisna od omrežij in pretoka podatkov po njih in od elektronske avtomatizacije mnogih dejavnosti, zato je očitno, da je ranljivost velika. Vse to je razvidno iz incidentov kraje podatkov, spletnih goljufij, razširjanja zlonamernih virusov, onesposobljenih sistemov in milijonskih škod. Kriminal na internetu pojmujemo kot kaznivo uporabo računalniškega omrežja ali drugega sistema na internetu, napade ali zlorabe sistemov in omrežij za kriminalne namene, kazniva dejanja in zlorabe z uporabo novih tehnologij ali novo razvita kazniva dejanja. Računalniški kriminal, kibernetski kriminal in kriminal visokih tehnologij so zaradi vse večje povezanosti sistemov skoraj sinonimi. (Valh 2008)

Internet kriminalcem (po Valhu 2008) ob razvoju računalnikov in interneta omogoča:
- globalno razsežnost, večje število žrtev in ogromno nelegalnih priložnosti,
- anonimnost in neposredne varne komunikacije ter
- dostop do znanja in pomoč pri obstoječih nelegalnih poslih.

Računalniški kriminal (Valh 2008) je pogosto del kriminalne dejavnosti, ki si pojavlja v fizični obliki. S porastom in sprejetjem interneta s strani družbe so se močno povečali tipi žrtev in njihovo število, ki so sedaj razširjene po vsem svetu, in sicer od vojaških, vladnih, izobraževalnih ustanov, podjetij in drugih poslovnih uporabnikov, družb, ki skrbijo za infrastrukturo in servise na internetu do posameznih uporabnikov interneta in kritičnih infrastruktur družbe (preskrba z elektriko, vodo, gorivi, nujno medicinsko pomočjo,

telekomunikacije ipd.). Različni motivi storilce računalniškega kriminala vodijo h kaznivim dejanjem. To so:

- finančni motiv oziroma pridobitev premoženjske ali druge koristi (pridobitev informacij, tatvina storitev, izogibanje plačilu za blago ali storitve),
- politični motivi, posledično tudi teroristični motivi,
- zlonamernost, škodoželjnost ter
- radovednost in osebne spodbude (npr. občutek moči, sposobnosti, dokazovanje).

Najpogostejše nevarnosti interneta so goljufije oz. internetne prevare, hekerstvo, virusi, črvi, trojanski konji, vohunski in vsiljivi oglaševalski programi; zloraba e-pošte in spletnih strani za namene vsiljivega oglaševanje; zlorabe plačilnih kartic, kraja identitete. Ostala najbolj pogosta kazniva dejanja, ki vključujejo informacijske tehnologije so tatvine, kraje intelektualne lastnine, piratstvo programske opreme, pedofilija, terorizem, prekupčevanje z drogami in orožjem, izsiljevanje in oderuštvo, pranje denarja ter napadi na kritične infrastrukturne stebre družbe. (Valh 2008)

Spletna goljufija ali internetna prevara se nanaša na kakršen koli tip prevare, ki uporablja eno ali več komponent interneta, da bi potencialne žrtve prepričala v izvedbo denarne transakcije v svojo škodo. Najpogostejše internetne prevare (PO Valhu 2008) so:

- lažne e-dražbe, v katerih se kupljeni predmeti nikoli ne dostavijo kupcu,
- plačevanje dostave kupljenih predmetov, kjer naj bi to že bilo vključeno v ceno,
- nigerijske poslovne ponudbe, kjer se preko sporočil e-pošte od žrtve zahteva številka bančnega računa za nakazilo večje količine denarja v izogib plačilu davka v Nigeriji za visoko provizijo, rezultat pa je izpraznjen bančni račun žrtve,
- prevare pri nakupu računalniške in programske opreme,
- lažni internetni ponudniki, ki zaračunavajo uporabnikom neuporabljene usluge,
- plačevanje preko kreditnih kartic za usluge, ki naj bi bile zastonj,
- ponudbe za delo na domu, za kar se obljublja velik zaslužek v kratkem času,
- lažni krediti, pri katerih se zahteva plačilo neke vrste članarine za kredite, ki se po tem plačilu nikoli ne uresničijo,
- ribarjenje – e-sporočilo ali spletna stran, ki je na pogled enaka e-sporočilu ali spletni strani legitimnega podjetja, npr. znane banke, od uporabnika zahteva, da vnese svoje finančne podatke in gesla za dostop do e-bančništva,
- lažni loterijski dobitki, za katere morajo »dobitniki« najprej plačati neko vsoto za plačilo izmišljenih bančnih transakcij, provizij posrednikom ipd., kar naj bi bilo potrebno za prenos dobitka k »dobitniku«.

V današnjem času ločimo tri osnovne skupine ljudi, ki so sposobni vdreti ali pa tudi že vdirajo v računalniške sisteme (Valh 2008):

1. **Hekerji** so bolj akademska skupina, po svojem delovanju tudi koristna. V njej so predvsem računalniški zanesenjaki, ki odkrivajo varnostne luknje oz. pomanjkljivosti v programih, njihov cilj pa ni pridobivanje ali poškodovanje podatkov. Večkrat tudi opozorijo izdelovalca programa na napake;
2. **Krekerji** so bolj vandalsko naravnana skupina, njena sestavina je pestrejša, pravega računalniškega znanja ima večinoma manj kot prva skupina. Ta skupina je odgovorna za večino računalniškega kriminala (uničenje, spreminjanje, kopiranje podatkov, napadi na strežnike ipd.), dostikrat pa uporabljajo zgolj programska orodja, ki jih je razvil nekdo drug;

3. **Frikerji** so računalniški programerji, ki so zasvojeni s kako doktrino ali pa so v službi raznih organizacij ali držav. V to skupino spadajo institucionalno organizirane skupine programerjev, ki so odgovorni za napade na konkurenčna podjetja ali države. Ta oblika je najnevarnejša, a je najredkejša.

Poznamo več vrst napadov, ki jih lahko ločimo (Valh, 2008) takole:

- Vdori v sistem imajo lahko za posledico le nepooblaščen dostop do podatkov in njihovo krajo, lahko pa tudi spremembo ali uničenje podatkov,
- prestrezanje sporočil, kjer napadalec za dostop do podatkov in tudi morebitno spremembo le-teh uporabi prenosne poti, kjer z ustrezno strojno in programsko opremo prisluškuje ali spreminja podatke, ki potujejo po napadeni poti,
- onemogočanje storitev, kjer napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen, to pa napadenemu povzroča nepotrebne stroške, druge stroške ponavadi nima; ti napadi so danes zelo popularni, saj napadalec pride do informacijskih virov zastonj ali mnogo ceneje kot sicer.

3.2 Trojanski konj

Trojanski konj je zgolj drugače poimenovan računalniški virus. Gre za specifični tip virusa, ki se ga lahko uporablja za oddaljeni dostop ali pregled računalnika iz oddaljene lokacije in s strani nepooblaščene osebe. Trojanski konj lahko uporabljajo tudi zato, da namestijo novi programi na računalnik brez vedenja uporabnika, pošiljajo lahko elektronsko pošto ali pregledujejo internetno povezavo in podatke, ki jih uporabnik vpisuje na spletna mesta (gesla, uporabniška imena, številke kreditnih kartic, naslov itd.). (info@unicreditgroup 2009)

Pri trojanskem konju gre za prevaro uporabnika, kot da program dela nekaj drugega, to pa uporabniku ustreza, zato ga namesti. Možno je celo, da se namesti brez očitne vednosti uporabnika, če je le-to mogoče. Te programe se predvsem uporablja v namene izkoriščanja okuženega računalnika za vdor v tretji sistem, omogočanje dostopa so internetnega omrežja ter krajo ali manipulacijo podatkov in informacij. Zanimivo je, da se tako okužene računalnike prodaja terorističnim in drugim kriminalnim organizacijam, ki jih nato uporabijo za svoja zlonamerna dejanja. (Valh 2008)

Trojanski konji se širijo, ko uporabniki odprejo program, za katerega verjamejo, da prihaja iz pristnega vira. Microsoft uporabnikom pogosto pošilja varnostna opozorila po elektronski pošti, vendar nikoli ne vsebujejo priloženih datotek. Trojanski konji se lahko skrivajo v programski opremi, ki se prenašajo brezplačno. Nikoli se ne prenašajo programske opreme iz vira, ki jim ni mogoče zaupati. (sipa@microsoft.com 2009)

3.3 Računalniški virus

Virus je posebna oblika trojanskega konja, ki se lahko razmnožuje in širi, podobno kot biološki virus. Ko izvajamo program, ki vsebuje virus, se izvede tudi virus. Sprogramiran je tako, da vrine kopijo samega sebe v program, ki z njim še ni okužen ali v datoteko. Proces se ponavlja in virus se hitro širi. Seveda pa ni cilj virusa samo razmnoževanje. Ko so izpolnjeni določeni pogoji, sproža virus tudi bolj ali manj neprijetne in škodljive

nepričakovane dogodke: od padanja znakov in zaslona, kar je lahko prav smešno, do uničenja podatkov in programov, kar je lahko velika škoda. V zadnjih letih se virusi širijo kot priloge k elektronski pošti. Računalnik, ki se okuži z virusom, avtomatično pošlje elektronsko sporočilo s pripetim virusom na vse naslove v imeniku naslovnikov. Najbolj znani virusi so Melissa, MyDoom, Sobig, Beagle, Nachi, Klez. (Gradišar, 2003)
Virus je računalniška koda, ki se pripne na program ali na datoteko, tako da se lahko razširi iz enega računalnika v druge in jih tako okuži. Virusi lahko poškodujejo programsko opremo, strojno opremo in datoteko. Širjenje virusa je odvisno od človeškega dejanja, kot je dajanje datoteke v skupno rabo ali pošiljanje elektronske pošte. Žal pa to ni vedno dovolj. Podjetje Microsoft (sipa@microsoft.com 2009) je podalo nekaj nasvetov kako preprečiti okužbe računalnika z virusi:

1. najprej je potrebno v računalniku poiskati protivirusno programsko opremo,
2. nato je pomembno, da je protivirusni program posodobljen in
3. izbrati je potrebno ustrezno protivirusno programsko opremo: upoštevati je potrebno, ali ima program samodejne posodobitve ter kakšen je sloves proizvajalca

3.4 Časovna bomba

Je vrsta trojanskega konja, pri katerem se skriti ukazi izvršijo v določenem trenutku, na primer na določen datum. Časovne bombe so največkrat izraz vandalizma in maščevanja nezadovoljnega delavca. Aktivirajo se, ko je delavec že zapustil organizacijo in se zapustil drugje. (Gradišar, 2003)

3.5 Logična bomba

Tudi logična bomba je vrsta trojanskega konja, ki se aktivira ob nekem logičnem pogoju, kot je na primer zagon določenega programa. (Gradišar, 2003)

3.6 Računalniški črv

Je prav tako računalniški program, katerega namen je hitra samodejna širitev preko interneta po e-pošti ali po spletnih, aplikacijskih strežnikih ali strežnikih s podatkovnimi bazami. S svojo širitvijo slabi zmogljivosti strojne in programske opreme ali celo povzroči neželene izpade in s tem povezane stroške. (Valh, 2008)

Podjetje Microsoft (sipa@microsoft.com 2009) trdi, da je črv nevaren prav zaradi izjemne sposobnosti hitrega širjenja: svoje kopije lahko na primer pošlje na vse naslove, ki so v adresarju, računalniki naslovnikov pa bodo naredili isto, kar povzroči učinek domin. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, zato je potrebno včasih do dvakrat dlje čakati za ogled posameznih spletnih strani.

Črv se ponavadi širi brez dejanja uporabnika in po omrežjih pošilja lastne kopije, včasih celo spremenjene. Črv lahko uporablja pomnilnik ali omrežno pasovno širino, zaradi česar se lahko računalnik preneha odzivati. (sipa@microsoft.com 2009)

3.7 Skrivna vrata

Skrivna vrata so zaporedje ukazov, ki omogoča uporabniku, da preskoči standardni varnostni sistem računalnika. Taka skrivna vrata si pogosto naredijo sistemski inženirji oziroma zaposleni, ki skrbijo za sistemske programe. Omogočajo jim lažji pristop v računalniški sistem. Storilec, ki najde skrivna vrata, pa jih uporabi za kriminalno dejanje. (Gradišar, 2003)

3.8 Razni vohunski in vsiljivi oglaševalski programi

Ti danes predstavljajo celo večjo nevarnost, ker so bolj razširjeni kot virusi. Njihov namen je prekomerno, vsiljivo oglaševanje, zavajanje uporabnikov, zbiranje informacij o uporabnikih itd. običajno gre za povsem samostojne programe, lahko pa gre tudi za zlorabe delovanja spletnih brskalnikov preko dodatkov brskalnika, zlorabe z ActiveX komponentami in skripti. Posledice delovanja teh programov so npr. samodejno odpiranje novih oken brskalnika, nastavitev domače strani in strani za iskanje v brskalniku itd. Ponavadi teh programov ne moremo enostavno odstraniti, saj se ponovno samodejno namestijo tudi potem, ko je na voljo odstranitev, torej se dokaj nekontrolirano širijo. Dejansko ne uničujejo podatkov (kot npr. virusi), kljub temu pa otežujejo ali celo povsem onemogočijo delo z računalnikom. Najhujše oblike vohunskih programov znajo uporabiti tudi jedra operacijskih sistemov, da prikrijejo svoje delovanje in celo tako prevarajo razne antivirusne in antispyware programe. Viruse, črve, trojanske konje in vohunsko ter oglaševalsko programsko opremo danes označujemo s skupnim imenom škodljiva programska oprema. Storitve interneta, preko katerega se ta programska oprema širi, so e-pošta, spletne strani in izmenjava datotek z aplikacijami P2P. (Valh, 2008)

3.9 Moteča e-poštna sporočila

Elektronska pošta je zelo priljubljen način komuniciranja v podjetjih in zasebno. Izmenjevanje sporočil preko interneta poteka hitro in načeloma nemoteče. Vendar pa ima elektronska pošta tudi pomanjkljivosti. (Abram Bill, januar 2005)

Poleg distribucijske poti škodljive programske opreme je e-pošta na udaru še zaradi množičnih, nadležnih, vsiljivih, nezaželenih, nenaročenih in predvsem motečih e-poštnih sporočil, kar imenujemo »spam«. Značilnost spama (po Valhu, 2008) je pošiljanje enakih ali podobnih sporočil na veliko število naslovov brez privolitve naslovnikov.Takšna sporočila pošiljajo spamerji, ki dobijo e-poštne naslove:

- s forumov, spletnih strani, iz podatkovnih baz ali verižnih e-sporočil;
- s pomočjo trojanskih konjev, ki pošljejo uporabnikov imenik, pa tudi z vdori v strežnike, kjer so shranjeni e-poštni naslovi;
- s preprostim ugibanjem in kombiniranjem pogostih uporabniških imen in domen.

Namen spama je največkrat oglaševanje z reklamnimi sporočili, kjer se predvsem ponujajo nelegalne plačljive storitve, izdelki dvomljive kakovosti ali pa so prevara. Pošiljanje spam sporočil na veliko število naslovov je poceni in če le majhen odstotek prejemnikov kupi izdelke ali storitve, ki so oglaševani v sporočilu, se to spamerjem splača. (Valh, 2008)

3.10 Zloraba HTTP- piškotkov

HTTP-piškotki so tekstovne datoteke, ki jih pošljejo strežniki spletnemu brskalniku, da jih shrani in ponovno pošlje nespremenjene takrat, ko z brskalnikom dostopamo do istega strežnika. Nekateri zmotno menijo, da je piškotek program, sploh pa neškodljiv program, kot je npr. virus. Opravičljivo pa se je do piškotkov obnašati nezaupljivo, saj prihaja do zlorab piškotkov in s tem do vprašanja internetne zasebnosti. Piškotki služijo poenostavljenemu dostopu do spletnih strani, ohranjanju podatkov med navigacijo po spletnih straneh (s piškotki je namreč možno realizirati nakupovalno košarico); sledenju uporabe internetnega brskalnika; ter vzdrževanju specifičnih informacij o uporabnikih itd. (Valh, 2008)

Problemi (po Valhu, 2008), ki so povezani s piškotki, so naslednji:

- Kraja piškotkov (do njih lahko pridejo drugi računalniki v omrežju),
- netočna identifikacija uporabnika (več uporabnikov hkrati uporablja isti računalnik- npr. javni računalnik),
- zastrupitev piškotkov (napadalec spremeni vsebino piškotka, preden ga brskalnik vrne strežniku; zastrupitev ni nevarna, če je v piškotku zapisana samo identifikacijska številka seje, ne pa pravi podatki),
- časovni iztek piškotkov (stalni piškotki so namreč najbolj nevarni za ostale zlorabe, čas veljavnosti naj bi zato bil kratek) in
- »cross-site cooking« (zloraba, ki je bila možna v starejših brskalnikih, ki so dopuščali, da se koristni piškotki regularne strani pomešajo s piškotki nelegalne spletne strani in s tem dejansko zastrupijo piškotke).

4 ZAŠČITA PRED NEVARNOSTMI ELEKTRONSKEGA POSLOVANJA

Internet je globalno omrežje, do katerega ima lahko dostop kdorkoli, zato je ena najpomembnejših nalog zaščita podatkov. Ena od možnosti zaščite so gesla, ki jih morajo vnesti uporabniki ob prijavi na določen računalnik v omrežju. Ta vrsta zaščite je zelo negotova, saj dopušča vdore v informacijske sisteme. Za zaščito podatkov je bil razvit poseben sistem, ki se imenuje požarni zid. Ta deluje kot filter, preko katerega potujejo podatki na določenem terminalu. Sistem ima informacije o podatkih, katere lahko prepušča in je sam po sebi zaščiten pred vdori.

Taki sistemi varujejo predvsem poslovne skrivnosti podjetij. Zavarovati pa je potrebno tudi podatke posameznih uporabnikov. Pri naročanju (in plačevanju) izdelkov preko Interneta uporabnik namreč pošlje številko kreditne kartice. Za zaščito podatkov te vrste se uporablja programska zaščita. Program zakodira številko kreditne kartice na tak način, da jo je nemogoče ugotoviti.

4.1 Varnostni mehanizmi za zaščito podatkov

Varnostni mehanizmi za zaščito podatkov so npr. požarni zid, močna gesla, šifriranje, certifikat, elektronski podpis itd.

4.1.1 Požarni zid

Za zaščito podatkov je bil razvit poseben sistem, ki se imenuje požarni zid. Deluje kot filter, preko katerega potujejo podatki na določenem terminalu. Sistem ima informacije o podatkih, katere lahko prepušča in je sam po sebi zaščiten pred vdori. (Vrečar, 1998)

Z namestitvijo požarnega zida zagotovimo pregled prometa, ki pride v naš računalnik in s tem lahko zaščitimo računalnik pred raznimi nezaželenimi zunanjimi dejavniki. Požarni zid bo opozoril na nevarnost in preprečil, ko bo skušal nekdo vdreti v sistem. (Rattle, 2002)

Požarni zid je sklop komunikacijskih naprav, računalnikov in programske opreme, katerih funkcija je ločevanje omrežij, filtriranje in beleženje prometa, kakor tudi izvajanje drugih varnostnih postopkov. Najpomembneje je, da podjetje ščiti pred zunanjimi nepooblaščenimi uporabniki, medtem ko je nemočen pred zlorabami zaposlenih znotraj omrežja. Ločimo dva tipa požarnih zidov (Valh, 2008):

- požarni zid na omrežni ravni (ugotavlja IP-naslov in vrata protokola, podatki se pretakajo z interneta direktno skozi njih v varovana omrežja in obratno) in
- požarni zid na aplikacijski ravni (preprečuje direktni pretok podatkov med dvema omrežjema tako, da prestreže IP-paket in dovoli uporabo aplikacije le uporabnikom, ki imajo dovoljenje za uporabo).

4.1.2 Uporaba močnih gesel

Uporaba močnih gesel je za povečanje varnosti velikega pomena, saj je danes ugibanje gesel s pomočjo namenskih programov in hitrostjo računalnikov postalo enostavno.

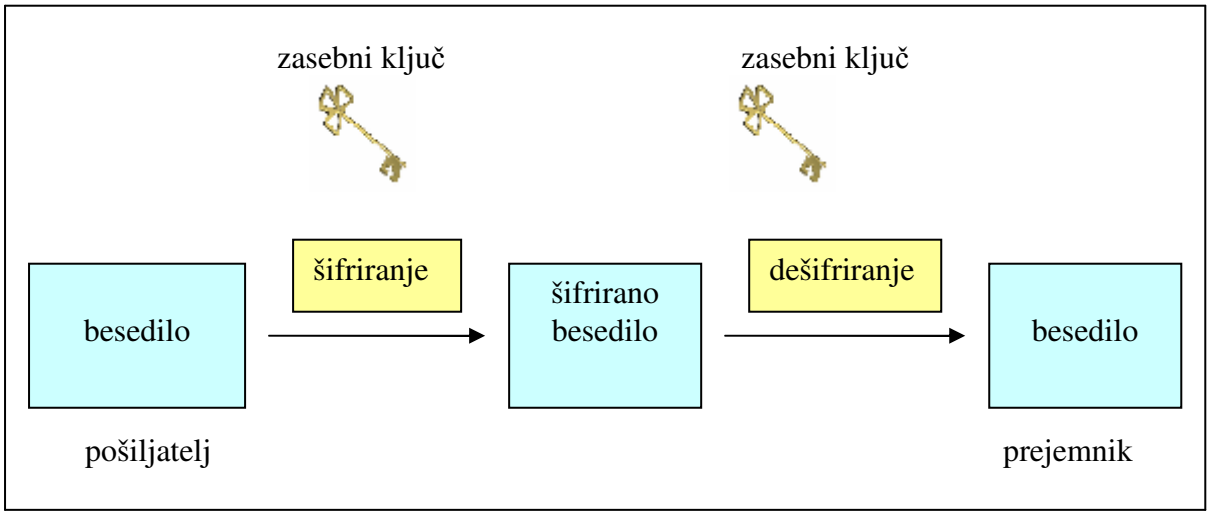
Osnovno pravilo močnih gesel je, da ne smejo vsebovati delov uporabniškega imena ali smiselnih izrazov, ker jih potem z napadom s pomočjo slovarja odkrijemo praktično takoj. Drugo pravilo je, da morajo biti daljša, vsebovati pa morajo male in velike črke, številke in posebne znake. Pri izmišljanju dobrih močnih gesel velja pravilo, da moramo dejansko besedo gesla zamenjati s stavkom ali frazo. Nujno pa je, da gesla tudi periodično spreminjamo. (Valh, 2008)

4.1.3 Šifriranje podatkov

Pri uporabi interneta za e-poslovanje je najpomembnejša zaščita podatkov pri prenosu preko interneta. Prenos podatkov je možno zaščititi tako, da jo transformiramo v obliko, ki onemogoča njihovo razumevanje in tako zagotovi tajnost. To imenujemo šifriranje, nasprotni proces pa imenujemo dešifriranje. Šifriranje zagotavlja zaupnost in nadzor nad dostopom. Pri šifriranju in dešifriranju so pomembni postopki zakrivanja in razkrivanja podatkov. Šifriranje je torej proces transformacije tekstovnih podatkov v obliko, ki onemogoča njegovo razumevanje, imenujemo šifriranje, nasproten proces pa dešifriranje. Za šifriranje in dešifriranje sporočil uporabljajo posebne algoritme, imenovane kriptoalgoritmi. Ti so znani do podrobnosti vsakomur, varnost podatkov pa zagotovijo s ključi. Ključ je parameter algoritma za šifriranje in je neodvisen od čistopisa besedila.

Poznamo simetrično in asimetrično šifriranje. Uporabnost simetričnega šifriranja je omejena, saj tako za šifriranje kot za dešifriranje uporablja isti šifrirni ključ. S takim šifriranjem dosežemo samo zaupnost sporočila, ne moremo pa dokazati izvora šifriranega sporočila, saj morata ta isti ključ za šifriranje poznati pošiljatelj in naslovnik. Prednost simetričnega šifriranja je v njegovi hitrosti (Valh 2008). Potek simetričnega šifriranja je prikazan na naslednji sliki.

Slika 3: Simetrično šifriranje

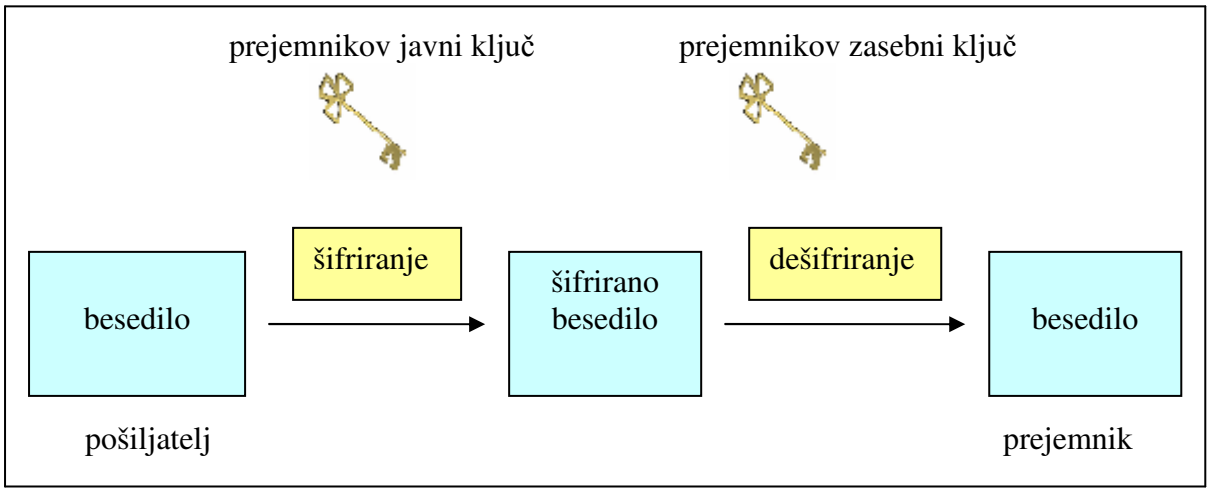


Vir: Gradišar, 2003

Pri asimetričnem šifriranju pa uporabljamo dva različna ključa, zato lahko to metodo uporabimo za dokazovanje celovitosti podatkov, izvora podatkov in tudi varovanje

zaupnosti podatkov. Najpomembnejša lastnost takih sistemov je, da iz prvega ključa (javnega) brez poznavanja dodatnih informacij ni mogoče določiti drugega ključa (zasebnega). Prvi ključ lahko zato javno objavimo. Z javnim ključem prejemnika sporočilo zašifriramo, dešifrira pa ga lahko samo prejemnik s svojim zasebnim ključem, ki ga mora skrbno varovati (Valh 2008). Naslednja slika prikazuje asimetrično šifriranje.

Slika 4: Asimetrično šifriranje



Vir: Gradišar 2003

Danes je najbolj razširjen način šifriranja kombinirano šifriranje, ki združuje prednosti obeh pristopov. Potek takega šifriranja (Valh 2008) poteka takole:

1. na strani pošiljatelja se sporočilo oz. dokument najprej šifrira z naključno izbranim simetričnim ključem za enkratno uporabo;
2. izbran simetrični ključ se na strani pošiljatelja asimetrično šifrira z javnim ključem prejemnika;
3. pošiljatelj pošlje šifrirano sporočilo in šifriran simetrični ključ prejemniku;
4. na strani prejemnika se z osebnim ključem prejemnika najprej asimetrično dešifrira izbran simetrični ključ, nato pa se z njim dešifrira prejeto sporočilo.

Čeprav je hitrost šifriranja odvisna od dolžine ključa, je za varnost pomembno, da je velikost ključev čim večja in s tem tudi število ključev, ki so na voljo za preizkušanje. (Valh 2008)

Asimetrični algoritmi (Valh 2008) omogočajo izvedbo digitalnega podpisa, ki zagotavlja:

- avtentičnost sporočila oz. dokumenta in identiteto podpisnika, saj je pošiljateljev podpis povezan z datoteko,
- celovitost oz. pristnost podatkov, kar pomeni, da se dokumenta ne da spremeniti, ne da bi to opazil prejemnik in
- nezatajljivost, saj pošiljatelj svojega podpisa ne more zanikati.

Pri asimetričnih kriptosistemih je največji problem overjanje javnih ključev, saj o vsakem ključu, ki ga najdemo v nekem strežniku v omrežju, moramo biti povsem prepričani, da res pripada njegovemu lastniku. Uveljavljena rešitev tega problema so certifikati. (Jezernik 2005)

4.1.4 Certifikat

Certifikat je elektronsko zapisano potrdilo in ga lahko primerjamo z osebno izkaznico ali potnim listom. Potrdila lahko razdelimo v štiri različne skupine (Kragelj 2004):

- osebna potrdila, s katerimi se uporabniki identificirajo v elektronskem svetu;
- strežniška potrdila, ki jih spletni strežniki predstavijo kot identifikacijsko dokazilo in uporabljajo pri vzpostavitvi varne komunikacije s spletnim pregledovalnikom;
- potrdila razvijalcev programske opreme, ki se uporabljajo za elektronsko podpisovanje različnih programskih aplikacij;
- potrdila overiteljev, ki jih navadno izdajo ali podpišejo sami overitelji.

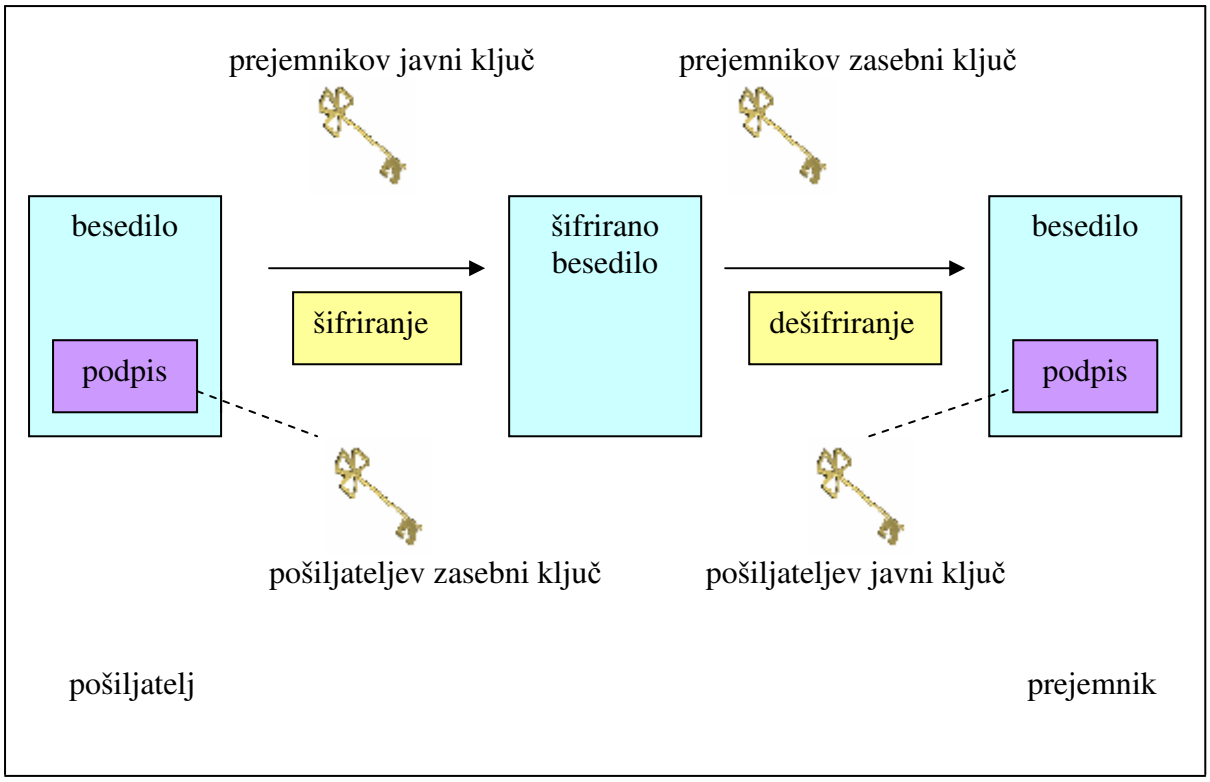
Sestavljen je iz podatkov, kot so ime, naslov, javni ključ, algoritem za katerega je namenjen, in digitalni podpis nekoga, ki s tem svojim podpisom potrjuje, da so vse informacije resnične. Agencija za izdajanje certifikatov (CA) podpiše s svojim tajnim ključem informacije za vsakega uporabnika posebej. (Jezernik 2005)

4.1.5 Elektronski podpis

Elektronski podpis je bistveni del certifikata. Ta je nadomestek lastnoročnega podpisa v elektronski izmenjavi dokumentov. Dokumente podpišemo tako, da najprej skrčimo besedilo z eno od zgostitvenih funkcij ne le nekaj vrstic, ki ima za določeno zgostitveno funkcijo stalno dolžino. To zgoščeno besedilo enolično določa dokument, iz katerega je nastal. To pomeni, da je računsko nemogoče najti drug dokument, ki se zgosti v isti blok. Zgostitvena funkcija nam omogoča to lastnost, da zagotovimo, da se pri prenosu dokument ni spremenil. Dobljeni prstni odtis (zgoščeni del besedila) nato šifriramo. Rezultat imenujemo digitalni podpis. Tudi preverjanje podpisa poteka v dveh korakih. Najprej dešifriramo podpis z javnim ključem podpisnika. Nato sami izračunamo vrednost zgostitvene funkcije na besedilu in primerjamo rezultata. Če se ujemata, je podpis pravi, če sta različna je dokument podpisal kdo drug ali pa se je vsebina besedila od časa podpisa spremenila. (Jezernik 2005).

Potek elektronskega podpisa je prikazan na sliki na naslednji strani.

Slika 5: Elektronski podpis



Vir: Gradišar 2003

Prednost digitalnega podpisovanja pred navadnim je v tem, da podpis poleg avtorstva besedila zagotavlja tudi njegovo celovitost. Digitalni podpis, dobljen z javnim ključem, omogoča lažjo razsodbo v primeru, ko podpisnik zanika, da bi bil podpis njegov. Ker je tako rekoč nemogoče določiti skriti ključ, ki je znan njegovemu lastniku, takega podpisa skoraj ne moremo ponarediti. Elektronski notarji podpišejo certifikate uporabnikom s svojimi skritimi ključi.
Vsak certifikat ima omejeno časovno veljavnost in serijsko številko. To so dodatne informacije, ki uporabnika varujejo pred poneverbami. (Jezernik 2005)

Veliko problemov pri zagotavljanju varnosti v poslovanju prek WWW odpravimo, če (Jezernik 2005):
- uporabljamo digitalne podpise za overjanje uporabnika in njegovih zahtev
- če strežnik, ki ima svoj digitalni podpis, zahteva overjanje drugih strežnikov, s katerimi komunicira
- če so dokumenti podpisani in so tako zavarovane avtorske pravice

Ko gre za dokumente (npr. za čeke), kjer je pomembno tudi, kdaj je bil dokument podpisan, je pomemben tudi čas nastanka podpisa. To imenujemo časovni žig, ki je posebna izpeljanka digitalnega podpisa in vsebuje poleg drugih informacij še natančen čas ustvarjanja podpisa. (Valh 2008)
Pred uporabo javnega ključa moramo najprej ugotoviti, ali ključ res pripada naslovniku šifriranega sporočila (avtentičnost). Preverjanje povezave med uporabnikom in njegovim ključem omogočajo posebne ustanove, imenovane overitelji oz. agencije za certificiranje javnih ključev. Overitelju zaupajo njegovi komitenti – imetniki digitalnih potrdil. S tem ga

tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Overitelj izda lastniku javnega ključa digitalni certifikat, s katerim zagotavlja drugim uporabnikom avtentičnost ključa. S pomočjo tega potrdila lahko lastnik dokaže lastništvo ključa in preko tega svojo identiteto. Digitalni certifikat je torej digitalni dokument, ki potrjuje povezavo med javnim ključem ali institucijo oz. strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Vsebuje javni ključ in informacijo o njegovem imetniku, ki ju podpiše oseba ali institucija, ki ji zaupamo. Potrdila morajo biti objavljena v splošno dostopnih imenikih ali na spletnih straneh. (Valh 2008)

4.1.6 Zaščita pred nevarnimi programi v e-sporočilih

Za zaščito sistemov e-pošte pred spamom in neželenimi nevarnimi programi v e-poštnih sporočilih uporabljamo kombinacije posameznih zaščit (Valh 2008):

- Zaščita z zakasnitvijo sprejema e-sporočila, kjer se prvo e-sporočilo iz neznanega strežnika ne pošlje naprej, ampak se počaka, da strežnik ponovi oddajo sporočila. Pravi strežnik bo namreč oddajo sporočil ponovil, spam strežnik pa ponavadi ne
- Odstranitev e-sporočil oz. spama, ki prihaja s strežnikov, ki so odprti za posredovanje e-pošte in so zabeleženi v črnih listah
- Odstranitev e-sporočil, ki v predmetu oz. glavi ali telesu e-sporočila vsebujejo sporne ali znane besede, ki so značilne za spam sporočila
- Odstranitev e-sporočil, ki jih filtrirajo sistemi za pregled vsebine in oblike sporočila
- Odstranitev okuženih e-sporočil s programi za zaščito pred virusi, črvi in ostalo škodljivo programsko opremo
- Prepoved e-sporočil z nevarnimi priponkami (.zip, .exe.).

4.2 Ozaveščanje o varnosti

Na srečo obstajajo podjetja in njihovi produkti, ki skrbijo za varnost in osveščanje uporabnikov na spletu. Eno izmed takih podjetij je Garlik. To je angleško podjetje za spletno varnost, ki se ukvarja z raziskavami in zaščito uporabnikov pred zlorabo osebnih podatkov na spletu. Njihove raziskave so pokazale, da spletni kriminal najbolj ogroža posameznike, saj so v kar 60 odstotkih spletnih prestopkov ciljna skupina prav posamični uporabniki. Gre za računalniško manj osveščene in naivne uporabnike, ki šele odkrivajo širše možnosti svetovnega spleta. Pri tem seveda niso izvzeta podjetja, ki jim spletni kriminal povzroča veliko poslovno škodo, z raznimi finančnimi prevarami. Garlik se predstavlja na spletu z dvema produktoma. In sicer DataPetrol, program, ki skrbi za zaščito osebnih podatkov in Qdos, spletna storitev, ki prikazuje pomembnost posameznika na internetu. (Sulčič 2008)

Poleg podjetja Garlik obstaja veliko spletnih strani, ki pomagajo pri osveščanju uporabnikov pri varnostni problematiki. V Sloveniji so nekatere najbolj pomembne Informacijski pooblaščenec, SAFE-SI, SI-CERT, Varnostne novice. Vse te strani osveščajo in obveščajo uporabnike o najnovejših nevarnostih na spletu, ponujajo različne nasvete za zaščito, predstavljajo zakonodajo RS, ki se navezuje na informacijsko varnost. (Sulčič 2008)

4.3 Samozaščita pri elektronskem poslovanju

Najpomembnejše pri varovanju podatkov v okviru e-poslovanja (po Valhu 2008) je preprečevanje nepooblaščenega zmanjševanja vrednosti informacijskega premoženja in virov podjetja. Viri so lahko zaupni podatki, kot so poslovne skrivnosti, podatki o strankah, informacije osebne narave, številke kreditnih kartic, strojna in programska oprema sistemov itd. Glavne grožnje za zmanjšanje varnosti e-poslovanja in plačevanja preko interneta, so:

- fizičen dostop nepooblaščenih oseb do računalnikov, strežnikov, omrežnih naprav,
- razkritje informacij in posredovanje podatkov nepooblaščenim osebam,
- skrivanje oz. predstavljanje pod drugim imenom – kraja identitete,
- zanikanje udeležbe v kakem delu transakcije,
- analiza prometa in prestrezanje sporočil na komunikacijskih kanalih,
- ponarejanje in pretvarjanje informacij ter
- onemogočanje dela oz. uporabe virov.

Varnost računalniških sistemov in informacijskih virov zagotavljamo s kombinacijo (Valh 2008):

- urejene varnostne politike in zavedanja ter podpore vodstva podjetja pri vzpostavljanju in vzdrževanju varnostne politike organizacije,
- vzdrževanja in upoštevanja varnostnih metod na vseh področjih delovanja,
- fizičnega varovanja računalniško-komunikacijske opreme tako, da je dostop in uporaba omogočena samo pooblaščenim osebam,
- stroge ločitve zasebnega dela omrežja od javnega dela omrežja in nadzorovane povezave s požarno pregrado,
- overjanja oz. avtentikacije uporabnikov,
- določitve in nadzora nad uporabo pravic (avtorizacija), ki jih imajo pooblaščeni uporabniki pri uporabi različnih sistemov,
- zaščite vseh transakcij s šifriranjem in digitalnimi potrdili,
- varnostnih nastavitev aplikacij, ki služijo uporabi internetnih storitev,
- razvoja varnih aplikacij že v fazi načrtovanja,
- beleženja vseh varnostnih dogodkov in nadzora ter spremljanjem dostopov do informacij,
- učinkovitega tehničnega varovanja podatkov z zaščito pred izpadom strojne opreme ključnih sistemov, vgrajenimi metodami zaščite podatkov v samih operacijskih sistemih kot tudi aplikacijah in bazah podatkov, rednim posodabljanjem ter varnostnim kopiranjem podatkov s krajšim in tudi daljšim časom hranjenja podatkov za možnost povrnitve v primeru raznih varnostnih problemov in katastrof,
- zaščite pred škodljivo programsko opremo z antivirusnimi programi in programi za odkrivanje ter odstranjevanje škodljive programske opreme,
- izobraževanja uporabnikov o varnosti in vcepljanja varnosti v njihovo zavest,
- uporabe močnih gesel ter njihovo redno menjavo,
- varnega uničevanja podatkov, ki jih ne potrebujemo več in
- rednega testiranja varnostnih sistemov skladnosti z varnostno politiko.

Varnostna politika podjetja ali organizacije določa obnašanje vseh udeležencev v procesu varovanja in zaščite podatkov. Opredeljuje delovne procese in opravila, ki se jih morajo držati zaposleni, da bi bila zagotovljena potrebna varnost. Predpisuje tudi metode in uporabo najboljših praks pri varovanju informacijskih virov, ki jih morajo upoštevati vsi

zaposleni. Pomembno je, da vodstvo nameni dovolj sredstev za vpeljavo in vzdrževanje varnostne politike.

Varnost na Internetu pomeni, da smo zavarovali vire v omrežju (vdor v računalnike), varnost podatkov pri potovanju v omrežju in neovrgljivost opravljenih transakcij. Varnost lastnih virov najbolje zagotovimo s požarnim zidom. Požarni zid pa ne reši problema varnosti potovanja podatkov po omrežju in neovrgljivost opravljenih transakcij. Varnost potovanja podatkov po omrežju zagotovimo z uporabo šifriranja, neovrgljivost opravljenih transakcij pa zagotovimo z digitalnim podpisom in drugimi mehanizmi.

4.4 Standard za varnost informacij ISO 17799/BS 7799

Standard ID 17799/BS 7799 podaja zahteve za vzpostavitev, izvajanje in vzdrževanje upravljalskih sistemov za varstvo informacij. Standard zajema politiko varovanja, organiziranost delovanja, razvrstitev in nadzor sredstev, varovanje v zvezi z osebjem, fizično in okoljsko varovanje, upravljanje komunikacij in obratovanja, obvladovanje dostopa, razvijanje in vzdrževanje informacijskega sistema, ravnanje z nepretrganim poslovanjem in usklajenost. Standard se lahko uporablja v različnih državah z različno zakonodajo, zato je pomembno tudi usklajevanje z lokalno zakonodajo. Med drugim spada sem zakonodaja na področju varovanja osebnih podatkov, intelektualna lastnina in uporaba kriptografije. Uporaba standarda prinaša poslovne koristi. Pri vpeljavi dobro spoznamo tveganja, s katerimi se srečujemo in jih zmanjšujemo na želeno raven. Pri elektronskem poslovanju se je skoraj nujno opreti na standard, da se izognemo nepreglednemu poslovanju in ravnanju z informacijami. (Jezernik 2005)

Standard varovanja informacij je objavljen v dveh delih (v Sloveniji):
- SIST BS 7799-2:2003 (sistemi za upravljanje varovanja informacij- specifikacija z napotki za uporabo),
- SIST ISO/IEC 17799:2003 (informacijska tehnologija- kodeks upravljanja varovanja informacij).

Informacije predstavljajo nujno potrebno »življenjsko tekočino« podjetij ter ustanov in lahko obstajajo v raznih oblikah. Lahko so napisane ali natiskane na papir, shranjene na različnih medijih, posredovane elektronsko ali prek običajne pošte, lahko so različne predstavitve in video gradiva podjetij ter ustanov, podatkovne zbirke, govorne informacije itd.
Če upoštevamo določila standarda BS 7799, bomo v podjetje vpeljali učinkovit sistem za upravljanje informacijske varnosti, saj nam zagotavlja, da je informacija dostopna samo tistemu, ki mu je namenjena. Zagotavlja nam tudi točnost in popolnost informacije ter metod obdelave le teh ter dostop avtomatiziranih uporabnikov do informacije in s tem povezanih sredstev, kadarkoli je potrebno. (Jezernik 2005)

4.5 Nasveti za varnejšo rabo spletnih informacij

Načine kako bolj varno uporabiti spletne informacije je podala Kragelj Ingrid (2004):

Ko želimo priti do določenih podatkov, moramo najprej oceniti vir informacij, in sicer, če je informacijo objavila pristojna institucija, vladna organizacija ali ugleden avtor. Viri, ki

jih pripravljajo raznovrstni strokovnjaki, so skoraj zagotovo zanesljivi in kakovostni. Zanesljivost pa povečujejo tudi navedene reference ali izjave o preverjenosti spletne strani, ki jih podajajo usposobljeni ocenjevalci spletnih strani. Le-ti zbirajo, ocenjujejo in uvrščajo spletne strani v sezname, izdelujejo njihove opise in priporočila.
Naslednje, kar moramo upoštevati je, da se izogibamo podatkom iz neznanih izvirov. Komunicirajmo z objavljenimi telefonskimi številkami ali prek elektronskih naslovov, ki jih spletne strani ponujajo kot pomoč uporabnikom.
Informacijo moramo potrditi še z uporabo drugih virov. Dobro je, da se o iskani informaciji prepričamo še pri kakšnem drugem spletnem ponudniku ali jih dopolnjujemo z informacijami, zbrane na druge načine, na primer iz tiskanih gradiv, pomnilniških medijev, iz javnih medijev, itd. čeprav podvajanje informacij še ne pomeni zanesljive informacije, nikoli ne uporabljamo informacije, ki je ne moremo preveriti.
Opredeliti moramo poslanstvo spletne strani. Poiščimo odgovor na vprašanja, kakšen je namen spletne strani. Ali je informativne, oglaševalske ali strokovne narave. Preveriti je potrebno datum posodobitve spletne strani. Informacijska integriteta izraža vrednost določene informacije v nekem časovnem trenutku. Pri vseh, še posebej pri informacijah, ki se hitro spreminjajo se prepričajmo o »roku uporabe informacij.
Nujno je uporabljati protivirusno programsko opremo. Na trgu jih je veliko, od manj dobrih do odličnih. Skrbimo, da bo podatkovna baza z definicijami virusov vedno novejša, saj bomo le tako sorazmerno varni pred napadi. Namestimo najnovejše popravke za operacijski sistem, ki ga uporabljamo. S tem bomo odpravili marsikatero napako pri prenosu sporočil.
Na nekaterih spletnih straneh je treba izpolniti tudi obrazec z različnimi podatki o uporabniku. Izpolnjujemo samo obvezne dele obrazca, ki so ponavadi posebej označeni z zvezdico ali drugačno barvo. Napišemo lahko tudi izmišljene podatke in ne resničnih, bodimo čimbolj anonimni, neznani. Neobvezna polja pustimo prazna. V drobnem tisku nekje čisto na dnu strani je polje, kjer določimo željo, da ne želimo prejemati reklamne elektronske pošte v svoj poštni predal.
Prepričati se moramo, da obiskana spletna stran varuje našo zasebnost. To še posebej velja za primere, ko upravljalcem spletnih strani posredujemo osebne ali celo zaupne podatke, kot je na primer številka kreditne kartice. Zaupanja vredne spletne strani imajo čedalje pogosteje posebej poudarjeno varovanje zasebnosti.
Raven varovanja zasebnosti v brskalniku določa, kako strog naj bo brskalnik pri varovanju zasebnosti. Določimo dovoljenja posameznim spletnim stranem, npr. v računalnik zapisujejo piškotke.
Gesla za dostop do posameznih informacijskih baz v računalniku ne shranjujmo. Gesla pogosto menjajmo. Ne pišimo gesel na listke in ne pozabljajmo disket s certifikati v računalniku.
Premislimo o upravičenosti cene informacije, saj najboljše informacije morda niso dostopne ali je njihova cena za uporabnika previsoka.
Vedno preberimo navodila za uporabo informacij s spleta in avtorske pravice. Avtorski dokumenti, tako spletne strani, besedilne, zvočne, video, grafične datoteke, programi in drugo, niso naša lastnina, zato je nujno dosledno upoštevati zahteve in opozorila.

5 E-POSLOVANJE MED SLOVENSKIMI PODJETJI

5.1 Spletno poslovanje med podjetji

Novi poslovni model na internetu, o katerem se zadnje čase vedno več govori in ga nekateri analitiki ocenjujejo kot največjo inovacijo v poslovanju v zadnjih štiridesetih letih, se imenuje medpodjetniško spletno poslovanje. (Skrt 2001)

Začetki elektronskega poslovanja med podjetji segajo v drugo polovico 70-ih let, ko so podjetja začela s pošiljanjem in sprejemanjem naročil, faktur in ostale dokumentacije v elektronski obliki preko elektronske izmenjave podatkov.Toda ker je elektronska izmenjava podatkov potekala preko dragih privatnih omrežij, so si tako obliko poslovanja lahko privoščila le velika podjetja. S prihodom interneta in njegovo množično dostopnostjo ter uporabo internetnih tehnologij pa je elektronsko poslovanje postalo dostopno tudi najmanjšim podjetjem. (Skrt 2001)

Najpomembnejši področji elektronskega poslovanja sta poslovanje med podjetji (B2B ali medpodjetniško poslovanje) ter poslovanje med podjetji in končnimi kupci (B2C). B2C model uporabljajo podjetja za poslovanje s končnimi kupci. V tem modelu ni bistvenih razlik v primerjavi s tradicionalno trgovino. Poglavitna prednost je v tem, da lahko sedaj kupci dostopajo do spletnih trgovin po principu 24/7 in to iz domačega naslonjača. Za kupca ni nobenih časovnih in krajevnih omejitev. Danes zavzema B2C približno 10 % vse e-prodaje na internetu. (Skrt 2001)

Pri elektronskem poslovanju med podjetji gre za naročanje izdelkov ali storitev po elektronski poti na eni strani ter za opravljanje plačilnih transakcij na drugi. Lahko govorimo tudi o poslovnih odnosih med podjetji v vlogah kupcev in podjetij v vlogah prodajalcev. Kljub temu, da je medpodjetniško spletno poslovanje še v povojih, je to najhitreje rastoče področje nove internetne ekonomije. S sabo nosi skoraj neizmerljiv potencial. (Skrt 2001)

Medpodjetniško spletno poslovanje prinaša številne prednosti. Še zlasti veliko lahko pridobijo majhna in srednje velika podjetja, saj se lahko zaradi nizkih stroškov, ki jih omogoča uporaba internetnih tehnologij povezujejo z večjimi podjetji in s svojo ponudbo konkurirajo na svetovnem trgu. Hitrost transakcij, nižji transakcijski in administrativni stroški, boljše upravljanje s podatki, zmanjšanje stroškov zalog, krajši časi obračanja zalog, krajše dobavne poti, učinkovitejše poprodajne storitve, možnost globalnega poslovanja ter nove tržne priložnosti so le nekatere izmed pozitivnih posledic, ki jih je prinesla uvedba e-poslovanja v podjetjih in zaradi katerih doživlja e-poslovanje eksponentno rast. (Skrt 2001)

Z uporabo interneta postajajo fizične razdalje zanemarljive, kar še posebej velja za neotipljive proizvode (programska oprema, storitve, glasba), ki jih lahko prenašamo preko interneta in jih celo neposredno uporabljamo. Največjo korist imata zabavna industrija ter založniška dejavnost. Medpodjetniško poslovanje ponuja tudi možnost za razvoj popolnoma novih izdelkov ter storitev, hkrati pa odpira možnost prodora podjetjem na nove trge ter možnost globalnega poslovanja, saj lahko podjetje na enak način kakor poslujejo s podjetjem v sosednji ulici, poslujejo s podjetjem na drugem koncu sveta. Podjetje lahko

direktno dostopa do ciljnega tržišča in ga oskrbuje z izdelkom, ki ga tržišče želi in potrebuje. (Skrt 2001)

E-poslovanje omogoča podjetjem, da se pri prodaji izognejo vmesnim dobaviteljem, da izboljšajo dobavni čas, in da so kupcem na voljo 24 ur na dan 7 dni v tednu. Medpodjetniško spletno poslovanje zmanjšuje tudi stroške delovne sile, hkrati pa povečuje njeno učinkovitost, saj odpade mnogo administrativnega dela, ki je bilo potrebno pri klasičnem načinu poslovanja. (Skrt 2001)

5.2 Spletno poslovanje med slovenskimi podjetji

5.2.1 E-poslovanje v slovenskih malih in srednje velikih podjetjih

Slovenska podjetja se na internetu pojavljajo na različne načine- od enostavne predstavitve podjetja na spletni strani do postavitve spletnih strani, ki podpirajo poslovanje podjetja na internetu. Le 17,9% mikro podjetij in 26,9% malih podjetij ima na spletnih straneh cenike izdelkov in storitev. Srednje velika podjetja pogosteje objavljajo cenike svojih izdelkov/storitev na spletnih straneh kot mala podjetja. Pogosteje pa podjetja na spletnih straneh predstavljajo svoje izdelke/storitve. Tako ima vsako drugo malo podjetje na svoji spletni strani katalog izdelkov oziroma storitev. (Sulčič 2004)

Preko interneta podjetja opravljajo različne dejavnosti ter raziskavo trga, manj pa se prek interneta izvaja usposabljanje in izobraževanje oziroma e-izobraževanje. Glede na to, da je plačevanje računov pri slovenskih podjetjih pogosto, pa sprejemanje in oddajanje naročil ni tako pogosto. Mikro in mala podjetja pri uporabi informacijske tehnologije za podporo poslovnih procesov zaostajajo za srednje velikimi podjetji na vseh ravneh, tudi na področju podpore proizvodnje in logističnih procesov, ki so tudi na splošno manj podprti poslovni procesi v podjetjih. Sistemi za celovito podporo poslovnih procesov ERP se uporablja v manj kot 10% mikro in malih podjetij in eni petini malih podjetij. Sistem ERP uporablja skoraj vsako drugo srednje veliko podjetje. Pri mikro podjetjih so pogostejši sistemi za podporo strank CRM. Uporablja jih vsako deseto mikro podjetje. Sisteme CRM v primerjavi s sistemi ERP pa manj uporabljajo mala in srednje velika podjetja. Zanimivo je, da velika podjetja sistemov CRM ne uporabljajo kaj dosti več kot srednje velika podjetja. (Sulčič 2004)

Primerjava podatkov Eurostata je pokazala, da slovenska mala in srednje velika podjetja zaostajajo za tovrstnimi podjetji v EU pri e-nakupovanju ter pri e-prodaji, zato pa slovenska podjetja intenzivneje uporabljajo storitve e-uprave. Tudi ponudba slovenske javne uprave je obširnejša od ponudbe povprečne države EU. Uvedba e-poslovanj malim in srednje velikim podjetjem omogoča pridobitev novega znanja, pohitri dostop do informacij, poveča učinkovitost podjetja, komunikacijo s strankami, kar vse vodi v izboljšanje konkurenčne prednosti. E-poslovanje je torej za mala in srednje velika podjetja priložnost za pridobitev konkurenčne prednosti. Podjetja e-poslovanje uvajajo predvsem zaradi pritiska oziroma zahtev vodstva podjetja, manj pa zaradi pritiska konkurence, kar pomeni, da uvedba e-poslovanja pri malih in srednjih podjetjih ni posledica pritiska trga. (Sulčič 2004)

5.2.2 Slovenska podjetja, kjer uporabljajo elektronsko poslovanje

Po podatkih različnih raziskav o e-poslovanju, lahko vidimo, da ima elektronsko poslovanje v sedanjem poslovanju v organizacijah pomembno vlogo. To potrjujejo številne aktivnosti, ki se odvijajo v organizacijah v Sloveniji, saj lahko najdemo že kar lepo število primerov uspešne uporabe e-poslovanja, in sicer v Zavodu za zdravstveno zavarovanje, Agenciji za plačilni promet, Petrolu, Carinski upravi, ICOS-u in drugih. (Skrt 1999)

5.2.2.1 ICOS d.o.o. (podjetje za svetovanje in računalniški inženiring)

Poleg povečanega zanimanja za trgovanje na internetu, se hitro razvija tudi potrebna informacijska tehnologija. Na slovenskem trgu je že od leta 1997 prisotna integrirana rešitev za elektronsko trgovanje SiShop, ki so jo razvili v računalniški hiši ICOS. Le-ta se je v osmih letih delovanja razvila v eno vodilnih podjetij na posameznih področjih informacijske tehnologije (podpora poslovnih aplikacijam, bančni informacijski sistemi, podatkovna skladišča, e-poslovanje) v Sloveniji. (Čufer 2004)

ICOS pristopa k e-poslovanju določenega podjetja projektno, s pomočjo proizvoda Sishop in se prilagaja zahtevam in željam vsake stranke posebej. Sishop vsebuje enostavni in pregledni sistem privatnih in javnih prodajnih katalogov, preko katerih podpira poleg B2B tudi B2C. sistem zagotavlja integracijo e-poslovanja s poslovnim sistemom, kar pomeni, da so vse aktivnosti s strani stranke, ki se izvajajo preko interneta, vezane na transakcije v poslovni aplikaciji. Takšen pristop k e-poslovanju zagotavlja podjetju popoln pregled npr. nad zalogami določenega blaga in s tem omogoča pravočasno npr. nabavo blaga in dostavo naročil. V rešitev so vgrajene sodobne metode trženja, ki podjetju omogočajo spoznati in spremljati vsako stranko individualno. (Čufer 2004)

5.2.2.2 ZIG Ljubljana

V podjetju ZIG iz Ljubljane že več kot tri leta v sodelovanju s Turistično zvezo Slovenije, Gospodarsko in Obrtno zbornico Slovenije, ter ostalimi partnerji, razvijajo komercialni projekt PMTG (Poslovna mreža gostinstva in turizma), namenjen turistični industriji ter podjetjem in institucijam, ki so povezane s turizmom. Glavni namen bodoče mreže je povečati konkurenčnost ter učinkovitost poslovanja vseh njenih udeležencev, omogočiti profesionalno promocijo in trženje storitev izbranih turističnih in gostinskih subjektov doma in v tujini, na drugi strani pa omogočiti kvalitetnejše, enostavnejše, predvsem pa bolj ekonomično poslovanje teh subjektov s svojimi poslovnimi partnerji doma in v tujini. (Skrt 2004)

V Sloveniji bo članstvo v PMTG ponujeno hotelom, gostilnam, restavracijam, turističnim agencijam, kampom in ostalim podjetjem ki ponujajo turistične storitve ter ponudnikom blaga in storitev za turistično gospodarstvo. V mreži bo mogoče poiskati razpoložljive prenočitvene kapacitete, vozne rede, informacije o naravnih in zgodovinskih znamenitostih, podjetja bodo lahko oglaševala posebne ponudbe itd. PMTG bo sestavljena iz štirih platform: turistične, tržne, marketinške in operativna. Tržna platforma bo namenjena e-poslovanju med podjetji iz gostinstva in turizma ter vsemi ostalimi gospodarskimi subjekti. Ker podjetja iz turizma in gostinstva za svoje poslovanje dnevno potrebujejo hrano, pijačo,

čistila in drugi potrošni material, pogostokrat pa iščejo glasbene in plesne izvajalce za zabavo in animacijo gostov, ponudnike športnih in rekreativnih dejavnosti, prevoznike, itd., jim bo mreža omogočila vzpostavitev stika z željenim subjektom. (Čufer 2004)

V času elektronskega poslovanja v globalnih razmerah, ko blagovne znamke postajajo ključni in odločujoči faktor uspeha v množični ponudbi, dobiva marketing odločujočo vlogo. Tega se zavedajo tudi v podjetju ZIG, zato bodo s pomočjo poslovne mreže doma in v tujini uvajali najsodobnejše oblike poslovanja, temelječe na internetni tehnologiji in na novih marketinških pristopih. (Skrt 1999)

5.2.2.3 Petrol

Elektronsko poslovanje na Petrolu pomeni uporabo sodobnih informacijskih tehnologij v vseh delih poslovnega procesa kjer prihaja do sodelovanja s poslovnim partnerjem. Aplikacije za elektronsko poslovanje so sestavni del Petrolovega informacijskega sistema in so z njim tesno integrirane. Sama arhitektura informacijskega sistema nam omogoča relativno enostavno izgradnjo sistemov za elektronsko poslovanje. Zaradi navedenega vidimo elektronsko poslovanje ne samo kot nujen in običajen način poslovanja v prihodnosti ampak tudi kot eno od konkurenčnih prednosti našega podjetja."
V Petrolu omogočajo dobaviteljem trgovskega blaga na bencinske servise oziroma skladišča internet dostop do podatkov o zalogah (trenutna, minimalna, ..) za artikle, ki jim jih dobavljajo. Na tak način želijo, da dobavitelj postane partner, ki lahko aktivno sodeluje v nabavnem delu trgovskega procesa. Dobavitelji lahko s Petrolom tudi računalniško izmenjujejo podatke o fakturah za trgovsko blago. Postopek vnosa fakture, likvidacije in knjiženja je popolnoma avtomatiziran. V obratni smeri pa se lahko bencinski servisi povežejo s svojimi dobavitelji in distributerji za trgovsko blago ter tako elektronsko naročajo blago in potrjujejo nabave. Vsem uporabnikom Petrolove kartice je omogočen dostop do podatkov o nakupih vključno s podatki o kupljenih artiklih oziroma storitvah. Poslovni partnerji pa lahko do istih informacij pridejo tudi preko računalniške izmenjave podatkov.
Za naročanje in distribucijo goriv so v podjetju razvili kompleksen informacijski sistem, ki omogoča spremljanje stanja goriv na bencinskih servisih, avtomatsko proženje naročil ali naročil na zahtevo, dopolnjevanje naročil v logističnemu centru, itd. Sistem vključuje tudi prevoznike (Petrol namreč nima lastnih transportnih zmogljivosti) , ki naročila dopolnijo s podatki o prevozu. Tako dopolnjena naročila se po elektronski poti posredujejo v Petrolova skladišča. Podatki o realiziranih dobavah se prenašajo v obratni smeri. Ker v Petrolu ne spijo na lovorikah, želijo svojim uporabnikom vedno ponuditi kaj novega. Tako bi radi v bližnji prihodnosti ponudili uporabnikom elektronski katalog artiklov, kjer bodo imeli dostop do podatkov o blagu (tehnične specifikacije, možne alternative, cene, založenost , ipd.) in kot nadgradnjo tega - spletno trgovino. (Skrt 1999)

5.2.2.4 Agencija za plačilni promet Republike Slovenije

APP je prve elektronske storitve ponudila konec leta 1996. Preko 4500 slovenskih podjetij, bank ter vladnih ustanov uporablja storitve APP-ja. Preko interneta imajo omogočen vpogled v stanje ter podatke o opravljenem plačilnem prometu, možnost pošiljanja plačilnih nalogov po e-pošti, ter finančne podatke slovenskih podjetij (FI-PO).

Danes se v elektronski obliki izpolni že skoraj tretjina vseh nalogov. Ker želijo v APP to številko še povečati, podjetja redno obveščajo o prednostih takšnega poslovanja. Število podjetij, ki za informiranje o stanju in prometu denarnih sredstev med dnevom uporabljajo internet, že krepko presega številko 5.000.
V letu 1998 je bilo v elektronski obliki opravljenih za 51 milijard nemških mark prenosov denarnih sredstev od skupaj 282 milijard mark. Temu je potrebno dodati še za 155 milijard mark večjih nakazil, ki jih opravi Banka Slovenije v realnem času. Trenutno so v testni fazi razvijanja EDIFACT standarda za plačilne naloge ter informacije o stanju na računu. Uporaba EDIFACT standarda je zelo koristna, saj pokriva različna področja poslovanja, poleg tega pa se lahko uporablja tudi v mednarodnih poslovnih transakcijah. (Čufer 2004)

5.2.2.5 Slovenska izvozna družba

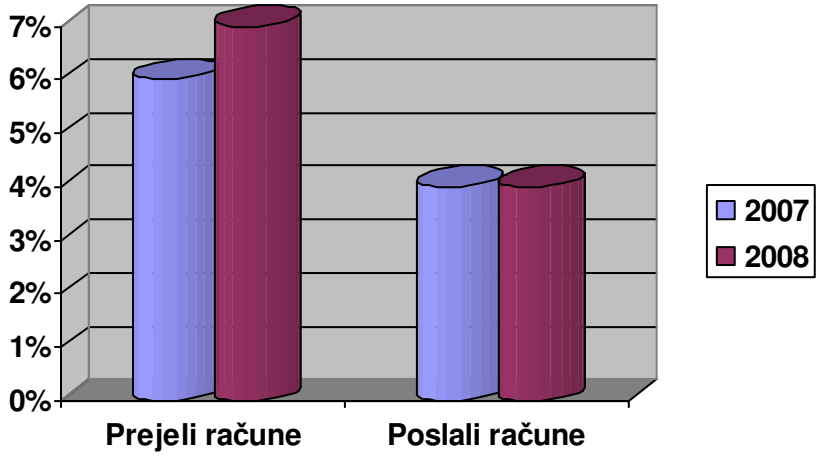
V SID so za podjetja, ki nenehno sklepajo izvozne posle večje vrednosti pripravili posebno storitev. Uporabnik ima nameščen Lotus Notes, ki omogoča neposredno izmenjavo baz podatkov med njim in družbo. Vsak uporabnik dobi svoje geslo, v bazah pa se določi, katere segmente (vrste storitev) lahko uporablja. Poglavitna prednost za izvoznika pri takem načinu dela je, da pridobi več informacij, saj lahko vidi vse svoje podatke, ki jih ima o njem SID, in jih tudi sam nadzoruje. V SID pričakujejo, da se bo zaradi novega načina komuniciranja z izvozniki, občutno zmanjšala količina operativnega dela. Ker bo odpadlo tudi pretipkavanje obrazcev, bi se naj možnost napačnega vnosa podatkov bistveno zmanjšala. (Čufer 2004)

Po poskusni dobi in opravljenem testiranju zdajšnjega delovanja želijo v SID svoj sistem še nadgraditi. Manjše in manj tvegane posle bi obdelovali avtomatično, kar pomeni, da bi računalnik sam preveril prijavo, pregledal boniteto izvoznika in kupca, izbral limite, vrnil pogodbo izvozniku in izstavi) račun za opravljeno storitev, brez posredovanja zaposlenih pri SID. Strokovni sodelavci bi vsak dan le spremljali obseg sklenjenih poslov in strukturo izvoznikov. (Čufer 2004)

5.3 Statistični podatki o e-poslovanju v Sloveniji

V letu 2008 je račune s pomočjo elektronske izmenjave podatkov pošiljalo 4% podjetij (enak delež kot leta 2007), 7% jih je račune prejemalo. Leta 2007 pa je 6% podjetij uporabilo internet za prejemanje računov. (RIS 2009)

Graf 1: Uporaba elektronske izmenjave z 10 in več zaposlenimi



Vir: SURS, 2008

V letu 2007 je naročila prek računalniških omrežij prejelo 11% podjetij. Svoje izdelke oziroma storitve je prek spleta v istem letu prodalo 6% podjetij. 27% podjetij je prek spletnih strani naročalo blago oziroma storitve.

Leta 2008 je 29% podjetij s pomočjo samodejne elektronske izmenjave podatkov izmenjevalo informacije s strani javne uprave, 18% pa jih je pošiljalo navodila finančnim ustanovam. Uporaba elektronske izmenjave informacij je pomembna tudi v upravljanju nabavne verige, za ta namen jo uporablja 27% podjetij, še kažejo podatki raziskave o uporabi interneta v podjetjih, ki jo je opravil SURS.

Poročilo RIS o uporabi IKT v podjetjih kaže, da je leta 2005 e-poslovanje uporabljajo približno tri četrtine podjetij. Delež uporabe je bil najnižji med velikimi podjetji (62%).
V letu 2002 si je, po podatkih RIS raziskave o e-poslovanju, le 3% podjetij z dobavitelji elektronsko izmenjevalo račun v standardizirani obliki, tovrstno izmenjevanje računov ni bilo prisotno v srednje velikih podjetjih, medtem ko je bilo največ tovrstnega izmenjevanja računov v mikro podjetjih (5%).

Večje organizacije si izmenjujejo elektronske listine, medtem ko se majhna podjetja težje vključujejo v tovrstno sodelovanje. Kot ovire za e-poslovanje majhna podjetja največkrat navajajo pomanjkanje kadrov (15%), premajhno število uporabnikov (16%), naravo dela ter visoke stroške strojne programske opreme (15%). (RIS 2009)

6 SKLEP

Internet uporabljamo vsak dan, saj lahko z njih kupujemo in prodajamo ter si s tem prihranimo čas in denar. Poleg tega pa si vsak dan znova s pomočjo interneta širimo obzorja in prihajamo do raznih informacij, ki nas zanimajo.

Elektronsko poslovanje prinaša uporabnikom mnogo prednosti. S tovrstnim poslovanjem lahko prihranijo na pri denarju, saj je nakup preko interneta velikokrat cenejši, kot nakup v trgovini. Prihranimo tudi na času, saj lahko nakup opravimo doma in si tako skrajšamo čas nakupa. Pri nakupovanju preko interneta imamo tudi večjo preglednost nad izdelki in storitvami, saj si lahko pogledamo ponudbo veliko podjetij, tudi tujih. Tudi komunikacija med podjetjem in kupcem je veliko hitrejša.
Vendar pa se pri razvoju interneta pojavljajo tudi določene slabosti. Z vidika uporabnikov je slabost varnost in zanesljivost. Za podjetje pa je slabost v hitrem razvoju tehnologije, zato se morajo podjetja hitro prilagajati novim razmeram, kar povzroča večje stroške. Majhna podjetja imajo tudi pomanjkanje usposobljenih kadrov, uvajanje elektronskega poslovanja pa včasih otežuje tudi visoka cena strojne in programske opreme.

Elektronsko poslovanje je za podjetja zelo pomembno, saj jim omogoča širitev ponudbe na tuje trge. Tako lahko tudi mala podjetja postanejo konkurenčna velikim. Rast e-poslovanja povečuje celoten obseg trgovine. V prihodnosti se bo približno 80% e-poslovanja odvijalo izključno med podjetji in bo povzročilo hitrejši prenos in razvoj informacijskih tehnologij. S tem se bo izboljšal dostop do informacij na trgu.

Vedno bolj pa so prisotne nevarnosti, ki lahko ogrozijo elektronsko poslovanje. Te nevarnosti so npr. kriminal na internetu, trojanski konj, računalniški virus, časovna bomba, logična bomba, računalniški črv, skrivna vrata, razni vohunski in vsiljivi oglaševalski programi, moteča e-poštna sporočila in zloraba http-piškotkov.
Nekateri računalniški virusi so neškodljivi, prejemniku pustijo samo kakšno sporočilo, drugi povzročijo neverjetne spremembe v prejemnikovem računalniku in nato še več v drugih. Na primer črvi uporabljajo za svoje razmnoževanje ravno računalniška omrežja. Pregledujejo mrežo in iščejo računalnike z varnostnimi luknjami. Če je mogoče, se tja prekopirajo in se tam začnejo znova razmnoževati.

Pred temi nevarnostmi pa se je mogoče tudi zaščititi. Zaščita podatkov pomeni varovanje podatkov pred uničenjem, krajo, izgubo, ponarejanjem, nepooblaščenim dostopom do podatkov ipd. Je skupek tehničnih, organizacijskih, pravnih ukrepov, s katerimi želimo zaščititi tako podatke, kot tudi programsko, strojno in seveda komunikacijsko opremo. Varnostni mehanizmi, s katerimi lahko zaščitimo računalnik so požarni zid, močna gesla, šifriranje, certifikat, elektronski podpis ipd.

Slovenska podjetja imajo na internetu enostavne predstavitve podjetja ali pa imajo spletne strani, ki podpirajo poslovanje podjetja na internetu. Le približno 20% mikro in malih podjetij ima na spletnih straneh cenike izdelkov in storitev. Srednje velika podjetja pa pogosteje objavljajo cenike svojih izdelkov oz. storitev na spletnih straneh. Pogosteje pa podjetja na spletnih straneh predstavljajo svoje izdelke/storitve. Tako ima vsako drugo malo podjetje na svoji spletni strani katalog izdelkov oziroma storitev.
Uporaba interneta v Sloveniji torej na področju e-nakupovanja in e-prodaje še zaostaja za podjetji v EU, vendar pa slovenska podjetja intenzivneje uporabljajo storitve e-uprave.

7 POVZETEK

Elektronsko poslovanje prinaša podjetjem in ostalim udeležencem takšnega poslovanja veliko koristi, kot so zniževanje, stroškov nabave, prodaje, trženja, in zniževanje obsega zalog, hitrejše pošiljanje in sprejemanje naročil ter hitrejše odzive trga. E-poslovanje omogoča tudi dostop do globalnega tržišča, večjo konkurenčnost, dodatno možnost oglaševanja. Prednosti, ki so jih deležni potrošniki so več različnih, cenejših storitev, hitrejša odzivnost na potrebe in želje kupca ipd.

Vendar pa ima elektronsko poslovanje tudi pomanjkljivosti, te so pomanjkanje dovolj usposobljenega in izobraženega kadra za uvajanje in integracijo e-poslovanja, visoki stroški izobraževanja. Pri potrošnikih so težave, saj so prepričani, da je e-poslovanje drago in tvegano. Problem so tudi pravne pomanjkljivosti, kot so pravna podlaga pogodb itd.

Predstavljene so nevarnosti, ki se pojavljajo, če poslujemo elektronsko. Te so kriminal na internetu, pri katerem ljudje vdirajo v računalniške sisteme. Vdore povzročajo skupine ljudi, kot so hekerji, krekerji in frikerji. Ostale nevarnosti internetnega poslovanja so trojanski konj, računalniški virus, časovna bomba, logična bomba, računalniški črv, skrivna vrata, razni vohunski in vsiljivi oglaševalski programi, moteča e-poštna sporočila, zloraba HTTP- piškotkov. Vendar pa se pred nevarnostmi lahko tudi zaščitimo, in sicer z varnostnimi mehanizmi, kot so npr. požarni zid, močna gesla, šifriranje, certifikat, elektronski podpis.

Slovenska podjetja vedno več uporabljajo elektronsko poslovanje. Internet uporabljajo na različne načine – od enostavne predstavitve podjetja na spletni strani do postavitve strani, ki podpirajo poslovanje podjetja na internetu. Vendar pa mala in srednje velika podjetja zaostajajo za tovrstnimi podjetji v EU pri e-nakupovanju ter pri e-prodaji, zato pa slovenska podjetja intenzivneje uporabljajo storitve e-uprave.

Ključne besede: kriminal na internetu, trojanski konj, računalniški virus, časovna bomba, logična bomba, računalniški črv, skrivna vrata, zloraba http-piškotkov, požarni zid, gesla, certifikat, elektronski podpis.

ABSTRACT

E-business has many advantages for companies and other participants of that kind of business. It decreases costs of buying, saling, trading and decreases range of stock. E-business makes faster sending and receiving orders and faster responeses from market. E-business makes entrance to global market, bigger competitive position, additional possibility of advertising. Advantages for consumers are lower price and variety of services and faster responding on needs of consumer.

But e-business has also weakness, like shortage of qualified and educated workers and high costs of education. Consumer are not sure about security of e-business and there is no legal base.

Danger of e-business is criminal on internet, because some people, like hackers, crackers and freakers want to breaking in computer system. Other dangers of e-business are trojan

horse, virus, time bomb, logical bomb, computer’s worm, secret door, spy and intruding advertising programs, disturbing e-messages, abuse of http-cookies. But we can protect with firewall, passwords, certificate, e-signature.

Slovenian companies more and more use e-business. Internet is used like simple presentation of company or some of them are having business over the internet. Small and medium companies are lagging behind companies in EU on area of e-buying and e-selling, but they are more intensive on e-government.

Key words: criminal on internet, trojan horse, virus, time bomb, logical bomb, computer's worm, secret door, abuse of http-cookies, firewall, paswords, certificate, e-signature.

SEZNAM LITERATURE IN VIROV

Literatura

1. Gradišar, Miro. 2003. *Uvod v informatiko*. Ljubljana: Ekonomska fakulteta.

2. Jezernik, Anton. 2005. *Informatika v poslovanju*. Celje: Visoka komercialna šola.

3. Kovačič, A., Jaklič, J., Indihar Štamberger, M., Groznik, A. 2004. *Prenova in informatizacija poslovanja.* Ljubljana: Ekonomska fakulteta.

4. Kragelj, Ingrid. 2004. *Poslovna informatika* 1. Ljubljana: DZS

5. Sulčič, Viktorija. 2008. *Management e-poslovanja*. Koper: Fakulteta za management.

6. Vrečar, Peter. 1998. *Poslovna informatika*. Ljubljana: Ekonomska fakulteta.

7. Valh, Dejan. 2008. *Elektronsko poslovanje*. Maribor: Doba, Višja strokovna šola.

Viri

1. Čufer, Marjan. »*Elektronsko poslovanje med podjetji«*. [on-line]. Available: http://www.telesat.si/~user239/elektronskoposlovanje.pdf [5.8.2009]

2. Skrt, Radoš. »*Medpodjetniško spletno poslovanje*.« [on-line]. Available: http://www.nasvet.com/b2b/ [3.8.2009]

3. Skrt, Radoš. *Elektronsko poslovanje med podjetji.* [on-line]. *Available*: http://www.nasvet.com/elektronsko-poslovanje-med-podjetji/ [3.8.2009].

4. Sulčič, Viktorija. »*E-poslovanje v slovenskih malih in srednje velikih podjetjih«*. [on-line]. Available: http://www.scribd.com/doc/11520291/Eposlovanje-v-slovenskih-malih-in-srednje-velikih-podjetjih [3.8.2009].

5. RIS- raba interneta v Sloveniji. »*E-poslovanje*.« [on-line]. Available: http://www.ris.org/index.php?fl=2&lact=1&bid=9692&parent=26&p1=276&p2=285&p3=1354&p4=1351&p4=1358&id=1358. [4.8.2009].

6. Abram, Bill. (17.1.2005). What small-business owners should know about e-mail. *Westchester county business journal.* [on-line]. Available: http://han.ukm.si/han/EIFLDirect/web.ebscohost.com/ehost/pdf?vid=87&hid=6&sid=98b08a47-7340-4f4c-9234-09ec88aa28cc%40replicon103.[14.9.2009]

7. Rattle, Barbara. (2.4.2002). Computer security for beginners: protect those passwords, invest in firewall and anti-virus technology. [on-line]. Availbale: http://han.ukm.si/han/EIFLDirect/web.ebscohost.com/ehost/pdf?vid=68&hid=6&sid=98b08a47-7340-4f4c-9234-09ec88aa28cc%40replicon103.[14.9.2009]

8. Seely, Jamey. (11.1.2002). The importance of privacy in the e-business economy. *Fort Worth Business press*. [on-line]. Available: http://han.ukm.si/han/EIFLDirect/web.ebscohost.com/ehost/pdf?vid=27&hid=9&sid=98b08a47-7340-4f4c-9234-09ec88aa28cc%40replicon103**.** [13.9.2009]

9. Hurley, Nicole; Ragothaman, Srinivasan. (junij, 2002). An Empirical Analysis of the Security Aspects of E-business Payment Systems. *Business Review*. [on-line]. Available:http://han.ukm.si/han/EIFLDirect/web.ebscohost.com/ehost/pdf?vid=18&hid=107&sid=98b08a47-7340-4f4c-9234-09ec88aa28cc%40replicon103 [14.9.2009]

10. Microsoft. (2009). Predstavitev virusov, črvov in trojanskih konjev. [on-line]. Available:http://www.microsoft.com/slovenija/doma/varnost/virusi/predstavitev_virusov.mspx [19.9.2009]

11. Microsoft. (2009). Zmanjšajte tveganje okužbe z virusi s posodobljeno protivirusno programo. [on-line]. Available: http://www.microsoft.com/slovenija/doma/varnost/virusi/antivirus.mspx [19.9.2009]

12. Unicredit Bank. (2009). Trojanski konj. [on-line]. Available: http://www.unicreditbank.si/Prebivalstvo/Online_b@nka/Varnost/Nevarnosti/Trojanski_konji [20.9.2009]

13. Astec. Varnost in upravljanje. (2009). [on-line]. Available: http://www.astec.si/index.php/sl/varnost-in-upravljanje/varnostna-politika [20.9.2009]

SEZNAM SLIK

SEZNAM TABEL

SEZNAM GRAFOV