UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

POMEN IN ZAGOTAVLJANJE VARNOSTI INFORMACIJSKIH SISTEMOV V FINANČNEM SEKTORJU

Ljubljana, december 2007 **Jernej Pečnik**

IZJAVA

Študent Jernej Pečnik izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom doc. dr. Aleša Groznika. Skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne

Podpis:_____

Kazalo

Kazalo slik

Kazalo grafov

1. Uvod

Finančne institucije so organizacije, katerih poslovanje v celoti temelji na informacijski tehnologiji, saj so danes praktično vsi podatki predstavljeni v digitalni obliki, hkrati pa so ti podatki tipično zelo zaupne narave. Tehnične, sociološke, pravne, politične ter ekonomske razsežnosti problema varnosti informacij predstavljajo težko obvladljivo celoto oziroma že skoraj najpomembnejši del informacijske tehnologije. Razvoj računalnikov in informacijske tehnologije je potekal in poteka z izjemno hitrostjo. Še nikoli prej v zgodovini človeštva se povsem nova tehnologija ni razširila po svetu s takšno hitrostjo in tako velikim dojemanjem virtualnosti vseh človeških aktivnosti. Informacijska tehnologija je omogočila veliko prednosti in koristi na mnogovrstnih področjih od vesoljskih raziskovanj in umetne inteligence do povsem navadnih, vsakodnevnih opravil. Z razvojem elektronskih komunikacij je postala varnost informacijskih sistemov ključnega pomena za zagotavljanje varnosti podatkov. To še posebej velja za organizacije, ki so izpostavljene največjemu tveganju, to pa je gotovo finančni sektor. Zaradi kompleksnosti sistemov postaja možnost napake vse večja, napako je tudi težje odkriti. Še tako dovršena tehnologija ne more zagotoviti popolne varnosti informacijskih sistemov.

O varnosti infrastrukture se pogosto razmišlja šele, ko so omrežna povezljivost in strežniške vloge že vpeljane, zato morajo marsikatere organizacije svoje informacijske sisteme, ki niso bili zasnovani z dovolj pozornosti za varnost, spremeniti. Dejstvo je, da tega ni mogoče zagotoviti samo s tehničnimi sredstvi, pač pa tudi z ustreznim vodenjem in vpeljavo ustreznih postopkov s čim tesnejšim sodelovanjem zaposlenih in poslovodstva. Zahteve po obvarovanju varnosti pri tem ne smejo pomeniti prekomernega posega v človekove pravice (Donaldson, 1992, str. 2). Pojavlja se potreba po ozaveščanju javnosti o vlogi in pomenu varovanja informacij ter po obsežnejšem izobraževanju in vzgoji o varnosti (Žurman, 2005, str. 6-7). Sprejetje in izvajanja standarda BS 7799 (Zupan, 2005, str. 39-40) in s tem poenotenje pravil in obnašanja na področju informacijske varnosti bi naj imelo pozitivne posledice na vseh področjih naše družbe, kjer se uporablja informacijska tehnologija.

Uporabniki informacijskih tehnologij se srečujemo z varnostjo na vsakem koraku. V zadnjem letu se je število člankov na temo varnosti prav opazno povečalo praktično v vseh revijah in dnevnikih, tudi poljudnih, seveda pa še posebej v specializiranih za vse vrste informacijske tehnologije. Nobena konferenca (povezana z računalništvom in informatiko) ne mine brez vsaj enega predavanja o informacijski varnosti, čedalje več je konferenc, predavanj in izobraževanj, ki so namenjene izključno informacijski varnosti. Na uporabnike računalnikov doma ali na delovnem mestu pretijo nevarnosti, ki si jih tudi strokovnjaki za informacijsko varnost težko predstavljajo. Takšen primer je bila varnostna luknja pri zadnjem izdanem operacijskim sistemu Microsoft Windows Vista: uporabnik je bil v nevarnosti, če je imel prižgane zvočnike (na slišno glasnost) in je pustil vključen mikrofon. Težava se je skrivala v novem glasovnem prepoznavanju, ki ne potrebuje vključitve s pritiskom na tipko: vsako besedo, ki je izrečena v pravem tonu in je v besednjaku tega operacijskega sistema, lahko le-ta

interpretira kot ukaz. Zlonamernež lahko na določeno spletno stran posname zvočno datoteko (z upanjem, da so zvočniki in mikrofon prižgani ter je naloženo glasovno prepoznavanje), ki bi vklopila prepoznavanje glasu, odprla Raziskovalca Oken (angl. Windows Explorer), zbrisala na primer mapo Moji dokumenti ali kaj drugega. Tak scenarij je težko mogoč, ni pa nemogoč (Računalniške novice, 2007, str. 17).

Namen magistrskega dela:

- preučiti
  - osnovne pojme s področja varnosti informacijskih sistemov,
  - osnovne pojme s področja standardizacije in certificiranja,
  - osnovne pojme s področja etike,
  - osnovne pojme s področja socialnega inženiringa,
  - kakšno vlogo imajo in igrajo vodje informatike v organizacijah v smislu varovanja in zagotavljanja varnosti informacij in informacijskih sistemov ter opredeliti, v kolikšni meri so odgovorni za svoje delo ter predvsem, ali se zavedajo svojih etičnih norm;
- opredeliti grožnje in nevarnosti, ki pretijo informacijskim sistemom, ter predstaviti dejavnike, ki vplivajo na varno in učinkovito elektronsko poslovanje, katerega cilj je uspešno poslovanje podjetja in zagotavljanje obstoja na konkurenčnem trgu;
- izvesti
  - anketo med vodji informatike v finančnem sektorju na temo informacijske varnosti,
  - anketo med zaposlenimi v zavarovalnici in obenem izvesti socialni inženiring med zaposlenimi,
  - socialni inženiring med slovensko populacijo.

Cilji magistrskega dela:

- definirati težave, ki bi se pri varovanju informacijskih sistemov lahko pojavile ali pa se že pojavljajo v smislu socialnega inženiringa,
- podati splošne usmeritve in ukrepe, ki preprečujejo nastanek neljubih dogodkov in povečujejo zavest uporabnikov o pomenu informacijske varnosti,
- ovreči splošno miselnost, da tehnologija sama po sebi zadošča in zagotavlja popolno varnost v elektronskem poslovanju,
- ugotoviti
  - kako lahko sodobni varnostni koncepti in pristopi prispevajo k doseganju ciljev informacijskega sistema,
  - poznavanje in opredelitve vodij informatike v finančnem sektorju do uvajanja standardov, etike in etičnih kodeksov ter socialnega inženiringa,

- kakšna pravila veljajo za skrbnike informacijskih sistemov, ki imajo dostop do večine podatkov,
- stopnjo znanja in osveščenosti na področju informacijske varnosti med zaposlenimi v zavarovalnici.

Metode dela

Poleg slovenske in svetovne strokovne literature in člankov ter informacij, pridobljenih s svetovnega spleta, sem uporabil znanja, pridobljena na podiplomskem študiju poslovne informatike na Ekonomski fakulteti v Ljubljani, vse to pa združil z večletnimi praktičnimi izkušnjami iz lastnega delovnega okolja. V empiričnem delu magistrskega dela sem izvedel in analiziral dve anketi, prvo med vodji informatike v finančnem sektorju, drugo med sodelavci v zavarovalnici. Anketo sem v vseh primerih poslal po elektronski pošti na elektronske naslove anketirancev; le-ti so imeli možnost, da izpolnjeno anketo vrnejo po elektronski ali po klasični pošti. Le v slednjem primeru so anketiranci ostali popolnoma anonimni. Izvedbo tretje ankete sem prekinil že med pripravo nanjo oziroma po pogovoru s predstavniki kriminalistične policije, ki sem jo prosil za pomoč in sodelovanje.

Kot predmet obravnave sem si izbral finančni sektor, ki je še posebej občutljiv na vsakršne nepravilnosti in zlorabe, po eni strani zaradi ogromnih vsot denarja in vseh drugih vrednostnih papirjev, po drugi strani pa zaradi dostopnosti in vsakodnevne uporabe storitev, ki jih ponujata na primer spletno bančništvo in spletno zavarovalništvo večini prebivalstva v Sloveniji. Preko svetovnega spleta je možen dostop od koderkoli drugod po svetu, zaradi tega je ta način zanimiv in predstavlja možnost nelegalnega zaslužka, tatvine ali druge zlonamerne, kriminalne oblike dejanja. Finančni sektor sem si poleg že naštetega izbral tudi zato, ker sem že dlje časa zaposlen v eni od slovenskih zavarovalnic in poznam to področje dejavnosti.

Osredotočil sem se le na tri specifična področja informacijske varnosti, za katere sem menil, da so aktualna in zanimiva, da pa v dostopni literaturi in predvsem v praksi vseeno dosegajo premalo ustrezne pozornosti. To so standardi, etika in socialni inženiring v povezavi z varnostjo informacijskih sistemov.

Vsebina magistrskega dela obsega le del celotnega področja informacijske varnosti, ki v zadnjem obdobju intenzivno pridobiva na svojem pomenu in narekuje ter usmerja nadaljnji razvoj informacijske in komunikacijske tehnologije.

2. Varnost informacijskih sistemov

Definicij informacijskih sistemov je več, v nadaljevanju navajam dve:

- »Informacijski sistem je sistem, v katerem se ustvarjajo, shranjujejo in pretakajo informacije« (Gradišar in Resinovič, 2001, str. 338).

- »Informacijski sistem je definiran kot množica ljudi, strojev, idej, aktivnosti, podatkov in postopkov, ki skupaj omogočajo pridobivanje koristnih informacij« (Damij, 2004, str. 30).

Informacijski sistemi temeljijo na informacijski tehnologiji, ki omogoča shranjevanje podatkov in njihovo predelavo v koristne informacije, torej informacijska tehnologija predstavlja tehnološko osnovo sodobnih informacijskih sistemov (Baloh et al, 2002, str. 7).

Cilj informacijskega sistema je poleg zagotavljanja natančnih informacij v primarni uporabni obliki (Damij, 2004, str. 30) tudi zagotavljanje varnosti informacij. Varnost informacijskih sistemov je skupek sistematičnih ukrepov za varnost in nadzor nad informacijskimi sistemi, osnovni pogoji za varnost informacijskega sistema organizacije so (Gradišar, 2003, str. 276):

- razumevanje zaposlenih, zakaj varnostni ukrepi obstajajo,
- preprečevanje dostopa do informacijskih virov vsem nepooblaščenim,
- uporaba nepiratskih kopij programov in programov, ki so zaščiteni proti virusom,
- razpolaganje s svežo kopijo podatkov,
- poročanje o prekrških, ki ogrožajo varnost sistema,
- posvečanje fizični zaščiti strojne opreme in podatkov,
- elektronsko podpisovanje pomembnih datotek,
- previdnost pri odpiranju elektronske pošte.

Varnost se ne nanaša le na strojno, programsko in drugo pomožno opremo, temveč tudi na procese, delovne razmere in okolje. Informacijska tehnologija je pomembna, vendar varnost vedno temelji na dobri organizaciji in usposobljenosti zaposlenih. Varnosti informacijskih sistemov se je potrebno posvetiti na dnevni ravni, potrebno se je zavedati, da je varnost nepretrgana dejavnost, za katero morajo biti odgovorni vsi zaposleni. Za varnost nikakor ne more biti odgovorna le določena tehnična funkcija ali oddelek, saj gre za sistematičen proces, ki zadeva celotno organizacijo. Varnost informacijskih sistemov upošteva varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij, upošteva zakonska in druga določila, neprekinjeno poslovanje in okrevanje po katastrofi ter vprašanja glede zasebnosti.

Definicija varovanja informacij je po ISO/IEC 17799:2005 ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij, poleg tega tudi ohranjanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost. Varovanje informacij je zaščita informacij pred raznimi vrstami groženj, da se zagotovi neprekinjeno poslovanje, zmanjša poslovno tveganje ter da se doseže kar največji dohodek iz naložb in poslovnih možnosti (ISO/IEC 17799:2005).

Informacijsko varnost (angl. information security) opredelimo kot lastnost informacije, ki zagotavlja, da je informacija resnična, pravočasna, nespremenjena in ima tudi vse tiste lastnosti pri hranjenju ali prenašanju, ki ji ohranjajo informacijsko vrednost, na primer tajnost, verodostojnost, istovetnost avtorja, preverjenost, podpisanost, časovno opredeljenost, imetje certifikata in podobno. Celovitost informacije pomeni, da je bila vsakršna napaka ali goljufanje preprečeno ali vsaj odkrito (Pahor in Drobnič, 2002, str. 51).

Informacijska varnost ni več postranski vidik poslovnega okolja, postaja pomembna postavka strateških načrtov, čeprav nekatera podjetja še ne razumejo, da je naložba v varnost informacijskega sistema podobna naložbi v zavarovanje. Podjetja se pri investiranju v informacijsko varnost srečujejo z enakimi pomisleki kot pri upravičenosti naložbe v nakup zavarovalne police. Področje informacijske varnosti je področje, kjer se najtežje izkazuje donosnost investicij ali celo povečanje dobička. Vpeljava sistema za upravljanje varnosti informacij je postala nuja, organizacijam ne samo povečuje zaupanje in ugled, izkazuje tudi urejenost organizacije in njeno zavezanost k odličnosti.

Po mednarodnih standardih revidiranja je ocena zanesljivosti informacijskih sistemov ena od pomembnih sestavin pri revidiranju računovodskih izkazov. Tako je tudi v Sloveniji, saj je v izvedbenih predpisih nadzornikov na področju bančništva, zavarovalništva in drugih finančnih storitev ocena informacijskega sistema pomembna obvezna sestavina letnega poročila, ki ga je potrebno predložiti regulatorjem.

»Varno poslovanje je tako poslovanje, pri katerem ne more priti do zlorab v nobeni fazi opravljanja poslovne transakcije« (Schlamberger, 1997, str. 39). »Ali je elektronsko poslovanje sploh lahko varno? Varnega poslovanja ni! Ni bistveno to, ali je poslovanje varno ali ni, temveč to, kako je zaščiteno. Kakor klasično poslovanje je tudi elektronsko poslovanje lahko in mora biti zavarovano« (Schlamberger, 1997, str. 39).

Večina večjih podjetij v tujini, pa tudi v Sloveniji, se še kako zaveda pomena varovanja informacijskih sistemov, kar se nenazadnje odraža tudi v kadrovski politiki podjetij, kjer zaposlujejo varnostne inženirje (angl. Information Security Officer) posebej za področje informacijskih tehnologij (Kwok in Longley, 1999, str. 30).

Ključni elementi programa varovanja informacijskih sistemov v organizacijah so implementacija varnostnih politik, standardov, procedur in navodil (Peltier, 2002, str. 150). Nadaljnji ključni element je individualna odgovornost implementacije programa varovanja, kar se predvsem nanaša na vodje informatike v organizacijah (angl. CIO – Chief Information Officer). Nenazadnje je eden najpomembnejših dejavnikov tudi načrtno ozaveščanje uporabnikov informacijskih sistemov. Vsak od teh elementov posebej zagotavlja, da bo organizacija dosegla svoj namen in cilj.

2.1. Kratka zgodovina in namen varovanja informacijskih sistemov

- Prvi elektronsko-mehanični sistem luknjastih kartic za obdelavo podatkov je razvil Herman Hollerith na koncu devetnajstega stoletja, uporabljal pa se je za tabelaričen prikaz in poročila pri popisu prebivalstva, ki ga je leta 1890 izvajal Ameriški urad za popis prebivalstva (Bosworth in Jacobson, 2002, str. 1.1).
- Prvi digitalni računalniki so bili razviti 1940 za vojaške namene, prvenstveno za kriptirno analizo ter izračun in izpis topniških strelskih tabel. Istočasno se je sistem luknjastih kartic že uporabljal za računsko uporabo in je bil razumljiva izbira za vhodne podatke prihajajočim novim elektronskim računskim napravam.
- 1949. John von Neuman, oče kibernetike, objavi dokument, ki da slutiti, da se lahko računalniški programi sami reproducirajo.
- 1959. Douglas McIlroy, Victor Vysottsky in Robert Morris iz organizacije Bell Labs razvijejo računalniško igrico, imenovano Jedro vojn (angl. Core Wars), v kateri so programi, imenovani organizmi , tekmovali za računalniški procesorski čas.
- Programerji začnejo pisati t.i. nameščence za velike računalniške sisteme. Če nobeno opravilo ni čakalo na izvršitev, so ti programi dodali kopijo samega sebe na konec vrste. Dobili so vzdevek zajčki (angl. rabbits), ker so se razmnoževali z uporabo sistemskih resursov.
- 1971. Prvi črv. Bob Thomas, razvijalec arpaneta, predhodnikom svetovnega spleta, je napisal program imenovan Creeper, ki je prehajal z računalnika na računalnik, pri vsakem pa zapisal na ekran sporočilo.
- 1975. Reprodukcija kode. A. K. Dewdey je napisal podprogram, imenovan Pervade, za računalniško igrico na računalniških sistemih Univac 1100. Kadarkoli je katerikoli uporabnik igral igrico, je podprogram tiho skopiral svojo zadnjo verzijo v vsako dostopno mapo, vključno z mapami v skupni rabi. Posledično se je s tem širil po omrežju.
- 1978. Črv Vampir. John Shoch in Jon Hupp iz organizacije Xerox PARC začneta eksperimentirati s črvi, namenjenimi za izvajanje opravil za pomoč. Črv Vampir je bil čez dan nezaposlen, ponoči pa je dodeljeval opravila drugim računalnikom.
- 1981. Apple virus. Joe Dellinger, študent na Teksaški univerzi, je modificiral operacijski sistem Apple II tako, da se je obnašal kot virus. Ker je virus imel nenamerne stranske efekte, ni bil nikoli izdan, pač pa so bile napisane nadaljnje verzije, ki so omogočile njegovo razširitev.
- 1982. Apple virus s stranskim efektom. Petnajstletni Rich Skrenta je napisal program ELK Cloner, ki se je pognal, kadarkoli se je računalnik zagnal z okužene diskete. Druge diskete, ki so bile nato vstavljene v računalnik, so se nato okužile s tem programom-virusom.
- 1985. EGABTR trojanski konj se je distribuiral preko elektronskih poštnih predalov, okužil pa je programe, namenjene za izboljšanje grafičnega prikaza. Ko

je bil enkrat zagnan, je pobrisal vse datoteke na disku, na zaslonu pa pustil sporočilo.

- 1986. Prvi virus za osebni računalnik, imenovan Brain, sta menda napisala dva brata v Pakistanu, ko sta ugotovila, da drugi ljudje kopirajo njuno programsko opremo. Če je bil računalnik okužen s tem virusom, se je virus skupaj z obvestilom o avtorskih pravicah skopiral na vsako disketo, ki je bila vstavljena v okužen računalnik.
- 1987. Črv Božično drevo (angl. The Christmass Tree Worm). Če je uporabnik dobil elektronsko pošto z okuženo elektronsko božično voščilnico in je le to tudi pognal, se je na ekranu izrisalo božično drevo, obenem pa se je ta elektronska voščilnica preposlala vsem v uporabnikovem imeniku. Ta promet je paraliziral IBM-jevo mrežo po vsem svetu.
- 1988. Spletni črv. 23 letni študent Robert Morris je izdal črv na US DARPA svetovnem spletu. Razširil se je na tisoče računalnikov, zaradi svoje »napake« pa je ponovno napadel že okužene računalnike, kar je pomenilo njihovo sesutje.
- 1989. Trojanski konj z imenom AIDS se je širil z disketami, ki so ponujale informacije o bolezni HIV, na okuženem računalniku je zakriptiral trdi disk, za zameno (odkriptiranje in geslo) pa zahteval plačilo.
- 1991. Prvi široko razvejan polimorfični virus je bil Tequila. Polimorfični virusi otežujejo detektiranje virusov protivirusnim programom s spreminjanjem svoje zunanjosti z vsako novo okužbo.
- 1992. Virus Michelangelo je bil načrtovan za brisanje vsebine trdih diskov na računalnikih. Imel je časovno nastavljen zagon oziroma proženje in sicer na Michelangelov rojstni dan, 6. marca. Virus je po svetu izzval veliko panike, v resnici pa je bilo malo okuženih računalnikov.
- 1994. Prva potegavščina (angl. hoax), ki je prejemnike elektronske pošte svarila pred zlonamerno kodo oziroma virusom, ki naj bi pobrisal cel trdi disk le z odprtjem elektronske pošte, je bila elektronska pošta z naslovom »Good Times«.
- 1995. Pojavil se je prvi makro virus ali dokumentni virus imenovan Concept. Širil se je z makroji v oblikovalniku besedil Microsoft Word.
- 1998. Prvi virus, ki je vplival na strojno opremo, se je imenoval CIH ali Chernobyl. Virus je napadel BIOS, ki je potreben za zagon računalnika.
- 1999. Virusi so za svoje širjenje začeli množično izkoriščati elektronsko pošto. Najbolj znan predstavnik je bil virus Melissa. Pojavil se je tudi prvi virus, imenovan Bubbleboy, ki je okužil računalnik, če je uporabnik odprl elektronsko sporočilo.
- 2000. Pojavil se je prvi virus za operacijske sisteme Palm; zanimivo, noben uporabnik se ni okužil. Tistega leta se je pojavil tudi do takrat »najuspešnejši« virus Love Bug. Tistega leta so hekerji s tako imenovanim distribuiranim napadom za zavrnitev storitve (angl. distributed denial-of-service attack) napadli spletna

podjetja Yahoo, eBay in Amazon ter še nekatera druga spletna mesta in povzročili nekajurno nedostopnost teh spletnih strani.

- 2001. Virusi so se začeli širiti prek spletnih strani ali mrežnih povezav. Zlonamerni programi so uporabljali ranljivosti in slabosti v programski opremi, tako da so se lahko širili brez pomoči uporabnikov. Virus Nimda je okužil računalnik medtem, ko je uporabnik le brskal po določeni spletni strani. Virus Sircam je uporabljal za širjenje svoj lastni program za elektronsko pošto, prav tako se je širil prek mrežnih povezav.
- 2003. Računalniki, imenovani zombiji in ribarjenje. Črv Sobig je omogočil hekerjem kontrolo nad okuženim računalnikom, ki je postal tako imenovani zombi, preko katerega se je lahko pošiljala neželena elektronska pošta (angl. Spam), ne da bi uporabniki vedeli za to.
- 2004. Razvili so se zlonamerni IRC boti (angl. Internet Relay Chat). Trojanski konji so lahko namestili bot na računalnik, kjer se je bot nato lahko povezal na IRC kanal brez vednosti uporabnika ter tako omogočil hekerjem kontrolo nad računalnikom.
- 2005. Sonnyjev protikopirni zaščitni sistem, imenovan DRM, ki je bil dodan na glasbenih CD-jih, je namestil na uporabnikov računalnik korenski komplet, ki je povzročil, da so določene datoteke postale skrite in se glasbeni posnetki niso mogli kopirati. Hekerji so napisali programe (Trojanske konje), ki so izrabljali to varnostno slabost in namestili na računalnik tako imenovana zadnja vrata (angl. back door).
- 2006. Zgodnja primera programov, virusov, ki zakodirajo oziroma zašifrirajo uporabnikove datoteke in v zameno za dešifrirno geslo zahtevajo plačilo, sta trojanska konja Zippo in Archiveous.

2.2. Varovanje informacijskih sistemov

Takoj, ko spoznamo, da je informacija vredna varovanja, ta postane predmet sistema upravljanja varovanja informacij, pa naj bo informacija v pisni, elektronski ali ustni obliki. Taka informacija je lahko tudi poslovna skrivnost, ki je definirana kot (Overly, 1999, str. 60) informacija, formula, vzorec, kompilacija, program, naprava, metoda, tehnika ali proces, ki doprinaša neodvisno ekonomsko vrednost.

Premiki v naravi in obliki groženj informacijskim sistemom zahtevajo spremembe in dopolnitve tudi na obrambni strani. Danes široko uveljavljeni način reaktivnega varovanja s požarno pregrado in protivirusno obrambo bo potrebno nadgraditi in premakniti v bolj proaktivno varovanje (Egan in Mather, 2005, str. 204). Proaktivno varovanje je tako varovanje, ki ne varuje le pred znanimi nevarnostmi (na primer s podpisi, definicijami pred že znanimi virusi in črvi), ampak uporablja metode, ki odkrijejo in preprečijo napade na podlagi neobičajnega obnašanja v omrežju in na sistemih, še preden izdelovalci varnostnih rešitev

izdelajo in distribuirajo ustrezne popravke ter nadgradnje. Proaktivno pomeni tudi zadosti zgodnje opozorilo in pravočasno ukrepanje.

Tako imenovane mešane (angl. blended) grožnje vedno bolj zahtevajo tudi mešano obrambo – varovanje na več ravneh:

- na meji varovanega omrežja,
- na strežnikih,
- na odjemalcih.

Dosedanja obramba (reaktivno varovanje) (Egan in Mather, 2005, str. 204) je zasnovana predvsem na omrežnem nivoju; v zadnjem času zaznane aktivnosti napadalcev pa so vedno bolj usmerjene v ranljivosti aplikativnega nivoja. V novejših napadih je vse očitnejša kriminalna motiviranost napadalcev: pridobiti denar, osebne podatke ali ukrasti identiteto in podobno.

Zagotavljanje varnosti informacij ni zgolj postavitev požarnega zidu ali uvedba nujne uporabe gesel in izdelave varnostnih kopij. Informacije, shranjene na elektronskih medijih, ogrožajo tudi požari, poplave, tatvine opreme, vdori v poslovne prostore. Nikakor ob tem ne gre pozabiti na človeški faktor, njegovo pozabljivost, neprevidnost, podkupljivost, škodoželjnost, malomarnost in druge negativne lastnosti. Varovanje informacij ne smemo gledati preozko; to ni zgolj tehnološki problem, s čimer se ukvarjajo informatiki in informatika. Dejansko je to problem upravljanja, ki zahteva celovit pristop, ki ga ni moč rešiti izključno s tehničnimi ukrepi, ampak jih je potrebno dopolnjevati z drugimi ukrepi in s postopki, standardi ter politikami. Naloge informacijske varnosti lahko strnemo v naslednje: (Savanović, 2007, str. 10-11):

- *Integracija*
  Integracija informacijske varnosti z organizacijo oziroma s poslovnimi procesi bo zagotovila večjo prepoznavnost in povečanje števila virov na tem področju.
- *Skladnost*
  Osnovni element integracije informacijske varnosti je skladnost s predpisi. To je sredstvo, ki organizacijam omogoča učinkovitejše varovanje pred varnostnimi tveganji.
- *Obvladovanje tveganj*
  Obvladovanje varnostnih tveganj je ključno pri poslovanju s tretjimi osebami, kar pomeni prepoznavanje izzivov, problemov in ustreznih ukrepov obvladovanja tveganj pri poslovanju z globalnimi dobavitelji in zunanjimi izvajalci.
- *Varovanje zasebnosti*
  Organizacije morajo posvetiti veliko pozornosti varstvu zasebnosti in osebnih podatkov ter izvajati aktiven in celovit pristop k preprečevanju kršitev.

- *Načrtovanje in razvoj*
  Roki, predpisani s strani nadzornih organov, in posledice kršitev informacijske varnosti, vzpodbujajo k boljšemu varstvu in obrambi pred nepooblaščeno uporabo. Posebno pozornost morajo organizacije nameniti določanju parametrov okrevanja po katastrofi, preizkusu načrtov okrevanja, izdelavi načrta kriznega komuniciranja, vključevanju novih tehnologij v načrte okrevanja ter določanju eskalacijskih postopkov kot odgovor na katastrofo.

Potrebo po večji informacijski varnosti povzročajo vse hujši pritiski tekmecev, ki organizacije silijo k vpeljavi novih tehnologij z veliko hitrostjo. To povzroči povečevanje stopnje poslovne kompleksnosti, kar pa nadalje zahteva uporabo bolj naprednih pristopov k varovanju informacij, zahteva tudi elastično informacijsko arhitekturo in konsistentne principe, politike, smernice in mehanizme, ki organizaciji omogočajo, da razvije in implementira varnostne rešitve, ki so skladne s poslovnimi zahtevami.

Pravilen pristop organizacije varovanja in zaščite podatkov je pristop od zgoraj navzdol. Najprej je potrebno postaviti strategijo varovanja in ustrezen program informacijske varnosti. Prek varnostne politike, usposabljanja in varovanja informacijskih virov se prehaja na nižje ravni varovanja. Vse ravni je potrebno varovati enakomerno, sicer obstaja tveganje, da bo ravno najšibkejši člen tarča napada in bo posledično ogrozil tudi vse druge ravni.

2.3. Varnost informacijskih sistemov v finančnih institucijah

Ribnikar (1996, str. 43) opredeljuje finančne institucije kot podjetja, ki se ukvarjajo s finančnimi posli v najširšem smislu. Prodajajo (in še prej proizvajajo) finančne oblike in/ali storitve. Posredniška vloga finančnih institucij na finančnem področju se odraža v njihovi premoženjski bilanci, kjer imajo med aktivo predvsem finančno premoženje in med pasivo zlasti dolgove (Ribnikar, 1993, str. 70). To je tudi bistvena značilnost, po kateri se finančne institucije razlikujejo od nefinančnih podjetij. Posebnost vseh finančnih institucij je, da imajo v lasti sredstva, ki so potencialno izpostavljena tveganju neizpolnitve obveznosti ter kreditnemu tveganju in poskušajo v večji ali manjši meri zagotoviti neujemanje zapadlosti sredstev in obveznosti v bilanci stanja, kar jih izpostavlja obrestnemu tveganju (Saunders in Cornett, 2005, str. 2).

Vsako podjetje, ki zagotavlja finančne proizvode in storitve posameznikom ali ostalim podjetjem, se lahko opredeli kot finančna institucija. Damodaran (2001, str. 1) deli finančne institucije v štiri skupine glede na to, kako ustvarjajo svoj dobiček:

- Banke ustvarjajo dobiček z razliko med obrestnimi merami, po katerih posojajo sredstva, in iz naslova ostalih storitev, ki jih nudijo posojilodajalcem in posojilojemalcem.

- Zavarovalnice ustvarjajo dobiček s premijami, ki jih zaračunavajo za ponujena zavarovanja, ter z dobički iz investicijskih portfeljev, katere vzdržujejo za poplačila iz naslova zavarovanj.
- Investicijske banke zagotavljajo svetovanje in podporne produkte za podjetja, ki želijo zbrati kapital na finančnih trgih, ali svetujejo pri izpeljavi poslov, kot so prevzemi, združitve ali odprodaje.
- Investicijska podjetja zagotavljajo investicijsko svetovanje ali upravljajo portfelje naložb za stranke. Njihovi prihodki izhajajo iz svetovalnih provizij iz naslova upravljanja investicijskih portfeljev.

S konsolidacijo finančne industrije se je povečalo število podjetij, ki delujejo na več področjih hkrati, istočasno pa se je ohranilo veliko število malih bank, butičnih investicijskih bank in specializiranih zavarovalnic, ki še vedno ustvarjajo večino svojih prihodkov iz enega vira (Bezlaj, 2006, str. 45).

Finančne institucije imajo veliko skupnega z nefinančnimi družbami. Tudi finančne institucije poskušajo biti čim bolj dobičkonosne; paziti morajo na konkurenco in želijo čim hitreje rasti in se razvijati (Bezlaj, 2006, str. 45).

Finančne institucije so organizacije, katerih poslovanje v celoti temelji na informacijski tehnologiji, saj so danes praktično vsi podatki predstavljeni v digitalni obliki, hkrati pa so ti podatki tipično zelo zaupne narave.

Varnost informacijskih sistemov v finančnem sektorju se v osnovi ne razlikuje od varnosti v drugih sektorjih, kot na primer v javni upravi, vojski, trgovini, energetskem sektorju in podobno. Zagotavljanje celovitosti, tajnosti, pravočasnosti, popolnosti, ustreznosti in razumljivosti informacij je v vseh informacijskih sistemih temeljnega pomena. Finančni sektor je specifičen oziroma drugačen od drugih v smislu pomembnih, pogostih in občutljivih relacij med njim in ljudmi kot posamezniki, med katerimi mora obstajati globoko zaupanje (primer: ljudje zaupajo svoj denar bankam, banke zagotavljajo ljudem, da bo ta denar na varnem). V kakršnemkoli primeru, ko pride do pomot, napak, zlorab, nepravilnosti ali drugih kriminalnih dejanj, je to zaupanje omajano, in to ne samo pri posamezniku. Posledično lahko pomeni propad za finančno institucijo, zaradi različnih razlogov, kot so negativna propaganda konkurence, objava v javnih občilih, nesposobnost hitrega okrevanja, ponovitev težave in podobno. Varnost informacijskih sistemov v finančnem sektorju naj bi zagotavljala, da do informacijskih nesreč ne bi moglo prihajati, v primeru naravnih in drugih nesreč pa mora z ustreznimi pravili in postopki zagotavljati čimprejšnje okrevanje po nesreči oziroma tako imenovano neprekinjeno poslovanje. V finančnem sektorju je vloga informacijske tehnologije zelo pomembna, saj je skoraj vsak poslovni dogodek zabeležen v informacijskem sistemu finančne institucije.

Svetovalna in revizijska hiša Deloite Touche Tohmatsu je med vodilnimi svetovnimi finančnimi institucijami opravila raziskavo glede informacijske varnosti (www.deloittte.com, 2006). V njej med drugim ugotavljajo, da so vse bolj pretkani napadi in ranljivost zaradi programskih napak še vedno najvišji prednostni cilj menedžerjev za informacijsko tehnologijo. V zadnjih letih se je v informacijski varnosti pozornost preselila s področja virusov in vohunskih programov na področje vdorov ob pomoči kraje identitet. Za banke in zavarovalnice je to v 53 % primerov poglavitna skrb (www.deloittte.com, 2006). Zaskrbljujoč je tudi podatek, da se v zadnjih letih veča število kraj podatkov znotraj varovanih omrežij, kar predstavlja že okrog 18 % vseh poskusov napadov.

Raziskava (www.deloittte.com, 2006) je pokazala, da je imelo 49 % podjetij vsaj eno težavo v povezavi z varnostjo, 18 % pa prizna, da so pri tem doživeli pobeg podatkov iz varovanega okolja. Teroristični napadi in naravne nesreče so pustili velik pečat zlasti na severnoameriških finančnih institucijah, ki so postavile povrnitev po katastrofi med najvišje prednostne cilje (49 %). Kar 81 % vprašanih v raziskavi (www.deloittte.com, 2006) trdi, da imajo v podjetjih pripravljene programe za nepretrgano poslovanje, čeprav natančne analize načrtov in postopkov kažejo, da organizacije vendarle niso tako dobro pripravljene za resnične težave.

Zanimivo je, da zaradi visoke pozornosti za informacijsko varnost poročanje o stanju na tem področju in merjenje učinkovitosti zgubljata pomenu Po raziskavi (www.deloittte.com, 2006) je poročanje o varnosti zdrknilo iz kroga petih najpomembnejših področij, meritve uspehov pa so pomembne le še za 23 % vprašanih (leta 2005 še 34 %). Analitiki menijo, da zlasti zato, ker je varnostni nadzor postal vsakdanja dejavnost z visoko obremenitvijo, zato merjenja in poročanja marsikje ne vidijo kot veliko prednost.

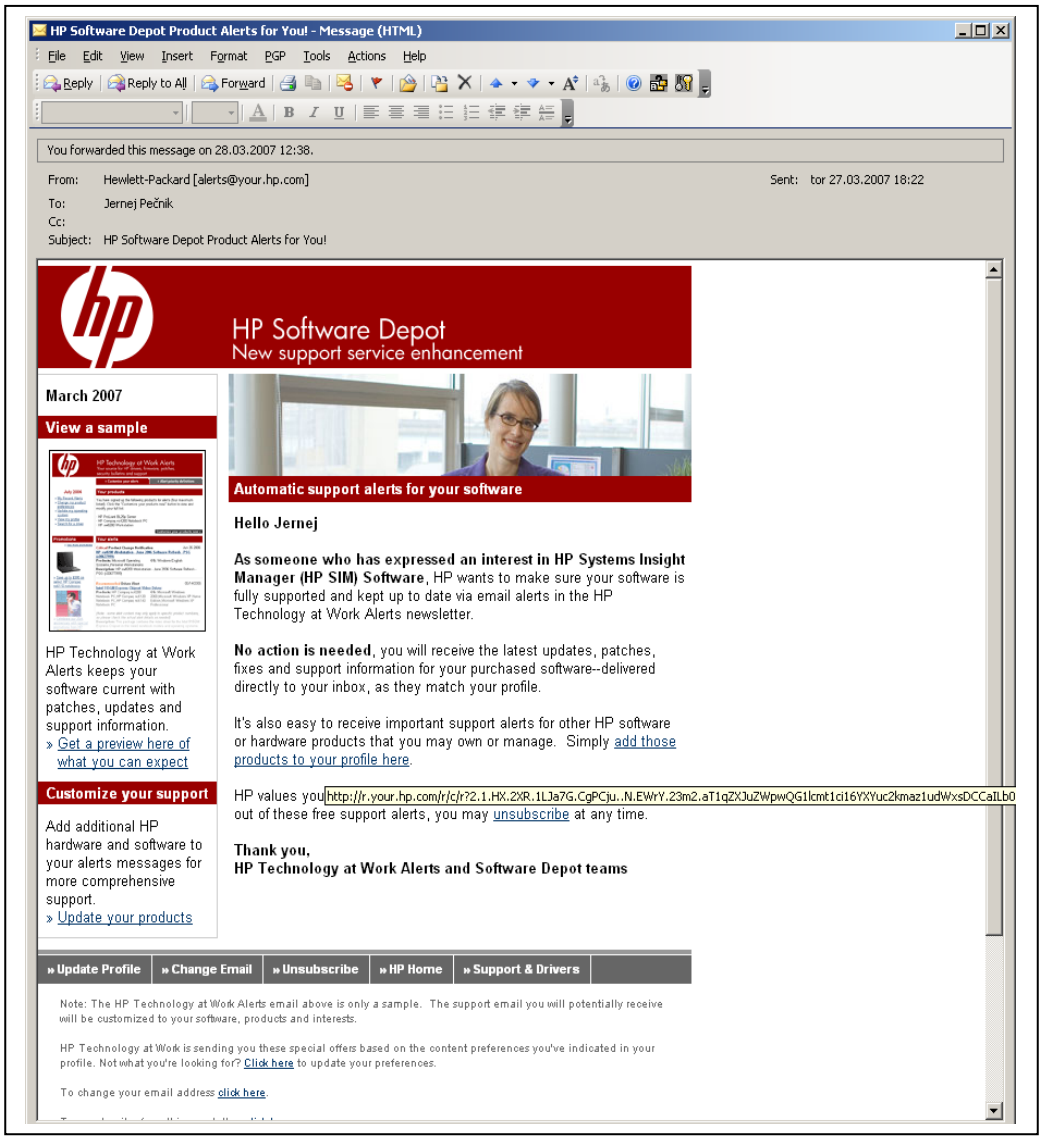
Tudi uporaba svetovnega spleta še vedno iz dneva v dan narašča, zato se ustanove in podjetja vse bolj selijo na področje poslovanja na svetovnem spletu. Finančni sektor pri tem ni nobena izjema. Zavedati se je potrebno, da kriminal sledi denarju. Kjerkoli se pojavi denar, tam se prej ali slej pojavijo tudi osebe, ki si ga tako ali drugače poskušajo prisvojiti.

Tehnike napadanja bančnih sistemov so različne (Bratuša, 2006, str. 38), od enostavnih tehnik socialnega inženiringa pa vse do namestitev administratorskih paketov na ravni jedra operacijskega sistema (angl. Kernel level rootkit). Lokalni napadi se zgodijo na žrtvinem računalniku, oddaljeni napadi prestrezajo in preusmerjajo podatke uporabnikove seje, medtem ko kombinirani napadi povezujejo lokalne in oddaljene napade in sodijo med najbolj učinkovite tehnike napadov. Najbolj znana tehnika oddaljenega napada na bančne sisteme je ribarjenje gesel, ko napadalec izdela natančno kopijo spletne strani, jo naloži v strežnik in jo nadzira. Kopija spletne strani vsebuje celotno kodo originalne spletne strani banke, ki jo je napadalec pridobil ob legitimnem obisku tarčine spletne aplikacije. V naslednjem koraku napadalec pošlje večjo količino poštnih sporočil, pri čemer sporočila priredi tako, da so podobna sporočilom banke, vsebujejo pa tudi naslov napadalčeve spletne strani. Napadalec lahko na primer obljubi žrtvam plačilo za izpolnitev ankete na ponarejeni spletni strani ali pa

zahteva menjavo gesla. Ko/če žrtev vnese pristopne podatke, jo napadalčeva spletna stran preusmeri na pravo spletno stran banke, nevedni uporabniki pa pogosto pomislijo, da so napačno vnesli identifikacijske podatke, in prijavo ponovijo.

Napadalci uporabljajo različne oblike zavajanja, trike; ena izmed oblik je pretvorba klasičnega IP naslova spletnega strežnika v njegovo decimalno obliko brez pik (na primer: http://534836582). Drugi trik je prikritje povezav v elektronskih sporočilih z znaki iz nabora *Unicode*. Tovrstno šifriranje poteka z enobajtno kodo (2 znaka HEX, pred katerima je znak %). To je priložnost za napadalca, saj lahko poševnico / interpretira kot %C0%AF. Pogosto napadalci preprosto registrirajo podobno ime domene (mojabanka-login.com, moja-banka.com, m0jabanka.com,…) , tovrstna imena pa žrtvi zbudijo lažen občutek varnosti.

Slika 1: Primer elektronske pošte spletnega ribarjenja.



Vir: Lastni vir.

Na Sliki 1 (glej stran 13) je primer elektronske pošte spletnega ribarjenja, ki je prišla v moj službeni poštni predal; moj elektronski naslov je pravilen, naslovljen sem s pravim imenom (ne s priimkom), v zavarovalnici, kjer sem zaposlen, dejansko uporabljamo izdelke podjetja Hewlett Packard, vsebina sporočila je verjetna, običajna, toda povezave kažejo na domeno, ki ima sicer podobno ime, a kontrolo nad njo ima zlonamernež in ne uradni prodajalec.

2.4. (Ne)varnosti v elektronskem poslovanju

»Elektronsko poslovanje danes pomeni poslovati elektronsko oziroma natančneje, poslovati v elektronski obliki z uporabo informacijske in komunikacijske tehnologije« (Groznik in Lindič, 2007, str. 2).

»Elektronsko poslovanje v najširšem smislu vključuje uporabo vseh oblik informacijske in komunikacijske tehnologije v poslovnih odnosih med trgovskimi, proizvodnimi in storitvenimi organizacijami, ponudniki podatkov, potrošniki in državno upravo. Elektronsko poslovanje spreminja načine ustvarjanja proizvodov in storitev ter njihovega posredovanja podjetjem, državni upravi in potrošnikom« (Gričar, 1997, str. 7).

Glede na medsebojno povezanost ločimo elektronsko poslovanje (Groznik in Lindič, 2007, str. 2):

- med podjetji (angl. Business to Business (B2B)),
- med podjetji in potrošniki (angl. Business to Consumer (B2C)),
- med potrošniki (angl. Consumer to Consumer (C2C)),
- med podjetji in javno oziroma državno upravo (angl. Business to Government (B2G)),
- med državljani in javno oziroma državno upravo (angl. Consumer to Government (C2G)),
- znotraj javne oziroma državne uprave (angl. Government to Government (G2G)).

V informacijski družbi težimo k čim večji uporabi elektronskih medijev. Poslovanje selimo s papirja na elektronske medije, z uporabo novih tehnologij pa moramo zagotoviti tudi določeno varnost in učinkovitost. V okolje informacijske družbe se najlažje vklopimo z uporabo sodobnih informacijskih tehnologij, ki omogočajo elektronsko poslovanje (Zimšek, 2000, str. 47). To je pravzaprav običajno poslovanje preko omrežja – trgovanje, bančne storitve, sporočilni sistemi in podobno.

Svetovni splet je omogočil pomembno poslovno pot, tako imenovano elektronsko poslovanje ali e-poslovanje. To omogoča podjetjem veliko novih načinov ponujanja izdelkov in storitev svojim strankam. Včasih so imela neprekinjen stik s strankami le največja podjetja, zdaj pa lahko tudi manjše družbe z omejenimi sredstvi tekmujejo z večjimi konkurenti. Svoje izdelke in storitve lahko ponujajo tudi na svetovnem spletu, kar pomeni manjšo investicijo. Storitve e-poslovanja so zelo všeč potrošnikom, ker jim svojega časa ni potrebno preživljati v

tradicionalnih trgovinah, ki so odprte samo v običajnem delovnem času, osebje je tam lahko tudi neprijazno, obstajajo lahko dolge vrste pred blagajnami in podobno. Podjetja morajo sedaj znati izkoristiti novo poslovno pot elektronskega poslovanja in hkrati obvladovati prisotno tveganje.

»Elektronsko poslovanje je za partnerje ugodno, ker posel lahko opravijo praktično v trenutku, brez zamudnega izmenjevanja papirjev. Zahtevati podpise na papirnatih listinah pomeni ovirati hitro poslovanje« (Gričar, 1997, str. 9).

Med prvimi sta bili na področju elektronskega poslovanja podjetji eBay in Amazon, ki sta nakup izdelkov na svetovnem spletu popolnoma poenostavili. Stranke lahko kupijo želene izdelke brez težav, podjetja pa so izumila nove koncepte pri poslovanju s strankami. S strankami razvijejo poseben odnos, na primer poosebljanje ponudbe, podjetja ponudbo priredijo glede na prejšnje nakupovalne navade, naslovi strank se hranijo, s tem se pospeši nakupovalni postopek.

Svetovni splet je spremenil tudi prodajo in nakup vrednostih papirjev. Tovrstno poslovanje je strankam borznoposredniških hiš močno znižalo stroške, pohitrilo in poenostavilo celoten postopek nakupa ali prodaje, omogočilo večjo preglednost, enostavnejši je pogled na zgodovino ter statistiko.

Velika ponudba povezav v svetovni splet in njihova enostavna uporaba sta omogočili široko dostopnost informacij in najrazličnejše nove storitve, tudi spletno bančništvo. Poslovanje prek spleta je vse bolj priljubljeno zaradi svojega 24-urnega delovanja oziroma priročnosti in enostavne uporabe. »Spletno bančništvo je oblika elektronskega bančništva«, »Elektronsko bančništvo pomeni sklepati bančne posle na elektronski način« (Groznik in Lindič, 2007, str. 7).

Zaradi povečanega obsega poslovanja pa se podjetja srečujejo tudi z novimi težavami, ki jih morajo odpraviti, če želijo ostati uspešna:

- Podjetja so pod velikim pritiskom, ker morajo nove sisteme izdelati čim prej, saj lahko nova zmožnost na trgu pomeni veliko konkurenčno prednost.
- Pravočasnega in natančnega dostopa do podatkov si zaposleni, stranke in partnerji ne samo želijo, ampak ga tudi pričakujejo.
- Podjetja morajo svoje izdelke in storitve ponujati na preprost in hkrati popolnoma varen način, ker hranijo zaupne podatke, kot so osebni podatki, domači naslovi, številke kreditnih kartic.
- Sistemi morajo delovati ves čas (24 ur na dan, 7 dni na teden), ker želijo stranke imeti dostop do izdelkov in storitev ali drugih informacij v podjetju kadarkoli in ne samo med delovnimi (uradnimi) urami podjetja.

Posebna uporabna vrednost elektronskega poslovanja pride do izraza še posebej v finančnem sektorju, pri bankah in zavarovalnicah. Večina plačil, nakupov, skratka vseh transakcij, poteka po elektronski poti tako med bankami in zavarovalnicami med sabo (B2B) kot med bankami in zavarovalnicami z njihovimi partnerji in komitenti (B2C). V Sloveniji je pomembno vlogo pri razmahu spletnega bančništva imela Banka Slovenije z reformo bančnega sistema (Groznik in Lindič, 2007, str. 6).

Tudi ob uporabi najsodobnejše tehnologije je potrebno še vedno ozaveščati ljudi in jih v skladu z uporabljeno informacijsko tehnologijo tudi ustrezno izobraževati (Zimšek, 2000, str. 50). Niti najnovejša tehnologija ne more preprečiti vseh zlonamernih dejanj zaposlenih. S tehnologijo se podjetje lahko do določene mere zaščiti in zgradi sistem beleženja dogodkov, ne more in tudi ne sme pa ovirati dela zaposlenih na račun večje varnosti. Za učinkovito zaščito omrežja je potrebno upoštevati celotno zgradbo omrežja in načine uporabe virov v omrežju. Zelo pomembno je sledenje novih tehnologij in sprotno posodabljanje in dograjevanje celotnega varnostnega sistema. Prav zaradi možnosti nadgradnje sistemov je potrebno ob nakupu ali naročilu opreme za zagotavljanje varnosti pregledati vse zmožnosti produktov, posebej še nadgradnje produktov ter povezovanje z drugimi produkti.

Poglavitna varnostna problema pri opravljanju spletnega bančništva sta (Groznik in Lindič, 2007, str. 17):

- prisluškovanje prenosu podatkov med komitentom in banko (elektronsko vohunstvo),
- spreminjanje podatkov (elektronski vandalizem).

Za zagotavljanje kvalitete storitev je poleg varnostnega vidika potrebno upoštevati tudi razpoložljivost informacij v določenem trenutku. Določene aplikacije zahtevajo večjo pasovno širino in so za poslovanje pomembnejše kot druge. Primer: Zagotavljanje dostopa do elektronskega plačevanja storitev je za določeno podjetje najpomembnejša storitev. Dostop uslužbencev preko te linije do svetovnega spleta je drugotnega pomena, vsaj v času, ko se izvaja prenos plačilnih nalogov. V tem primeru ima večjo težo promet strank, ki izvajajo elektronsko plačevanje storitev tega podjetja.

Zaščita omrežja je povezana z učinkovitim preverjanjem identitete. Uporabnik z določenimi pravicami se mora najprej predstaviti sistemu, ki mu glede na njegove pravice dodeli dostop do podatkov in storitev. Za preverjanje identitete je najenostavneje uporabiti par statičnih besed, ki predstavljajo uporabniško ime in geslo. Za sisteme, ki zahtevajo večjo varnost, pa je to vsekakor premalo. V teh primerih se lahko uporabijo metode enkratnih gesel, za kar pa mora imeti uporabnik posebno napravo za generiranje gesel. Pričela se je tudi uporaba pametnih kartic, na katere uporabniki shranijo svoj podpis. Podpis je potrebno overiti pri elektronskem notarju, ki mu zaupata obe strani. Pri elektronskem poslovanju ni potrebno vzpostaviti fizičnega kontakta, zato se je pred morebitnimi zlorabami potrebno še dodatno zavarovati. Za podpis se v ta namen uporablja par nizov naključno generiranih števil. Prvi del

predstavlja javni ključ, drugi del pa zasebni ključ, ki ga mora vsak uporabnik sam varovati. S kombinacijo obeh ključev so sporočila ali podatki učinkovito šifrirani, prebere jih lahko le naslovnik. Kodiranje se izvede s pomočjo določenih algoritmov, težava, ki ostaja, pa je garancija, ali je javni ključ določenega uporabnika res njegov. Težavo reši elektronski notar, ki s svojim podpisom jamči o pristnosti elektronskega podpisa.

Pri transakcijskem poslovanju je potrebno poskrbeti tudi za potrjevanje vsake transakcije in ob posebnih zahtevah za ugotavljanje resničnosti podatkov (Zimšek, 2000, str. 49).

2.5. Grožnje in nevarnosti

Vsiljivcev, ki želijo na kakršenkoli način in z različnimi nameni kompromitirati varnost informacijskih sistemov, je več vrst, v grobem jih lahko razdelimo na naslednje vrste (Sanderson in Forcht, 1996, str. 32):

- organiziran kriminal,
- teroristične organizacije,
- tuje obveščevalne službe,
- agenti industrijske špijonaže,
- privatni raziskovalci,
- posredniki informacij, ki prodajajo nezakonito pridobljene tajne, zaupne podatke,
- hekerji z namenom osebne finančne koristi.

Glede na znanje in razpoložljiva finančna sredstva se razvijajo različna programska orodja, nekatere najbolj značilne grožnje in nevarnosti podajam v nadaljevanju.

Virusi, črvi, trojanski konji, časovne bombe

Računalniški virus je vsak program, ki se samodejno replicira s pomočjo dodajanja lastne kode v izvršilne programe (.exe, .com, .vbs, .reg,…) ali dokumente. To delovanje je podobno biološkim virusom, ki okužijo celice ter se s pomočjo njih razmnožujejo. Če je računalnik okužen z virusom, so lahko vidne neobičajne spremembe v delovanju, kot so izginjanje teksta iz dokumentov, samodejno pošiljanje elektronske pošte, samodejno zaganjanje raznih programov, nezmožnost povezave na svetovni splet ali določene spletne strani (zelo velikokrat je onemogočen dostop do kakršnihkoli protivirusnih programov na spletnih straneh), vedno več pa je virusov, ki delajo prikrito in jih lahko zaznajo le protivirusni programi.

- Črvi so virusi, ki se širijo s pomočjo mrežnih storitev (spletni ali poštni strežniki,..).
- Trojanski konji so virusi, ki se širijo pod pretvezo, da so nekaj drugega (glasba, film,…).

- Prenešenci (angl. Downloaders) so trojanski konji, virusi, ki se sami pretočijo z določenih spletnih strani na računalnik.
- Časovne bombe so vse oblike virusov, ki se sprožijo na določen dan.

Zaščita pred virusi so protivirusni programi, ustrezno dodeljevanje uporabniških pravic ter filtriranje vsebin na svetovnem spletu in v elektronski pošti.

Prekoračitev medpomnilnika

Zaradi varnostne pomanjkljivosti napadalec določenemu sistemu ali programu lahko pošlje določeno zahtevo po storitvi, ki je oblikovana tako, da preobremeni količino spomina (angl. Buffer), ki jo sistem uporablja in se začnejo zahteve pretakati (angl. Overflow) v sosednje spominske prostore, kar lahko povzroči, da se sistem ponovno zažene ali pa da se te zahteve pričnejo izvajati kot koda v tem ali drugih procesih (Norberg, 2001, str. 25). Tako lahko poleg teh zahtev napadalec pošlje tudi svojo kodo, ki lahko vsebuje viruse, programe za oddaljen nadzor in podobno. Napadalec lahko ta sistem poškoduje ali nad njim prevzame nadzor.

Pred takimi napadi je najučinkovitejša zaščita požarni zid, ki onemogoča dostop do računalnika, zelo pomembno pa je tudi posodabljanje operacijskega sistema in programov, ki se povezujejo s svetovnim spletom.

Vohunski programi

»Spyware« je oznaka za vse vrste spletnih nadlog, ki po definiciji niso virusi, torej se ne replicirajo s pomočjo dodajanja lastne kode v izvršilne programe ali dokumente, ampak so programi ali dodatki k programom, ki jih je potrebno namestiti, ali pa se namestijo samodejno.

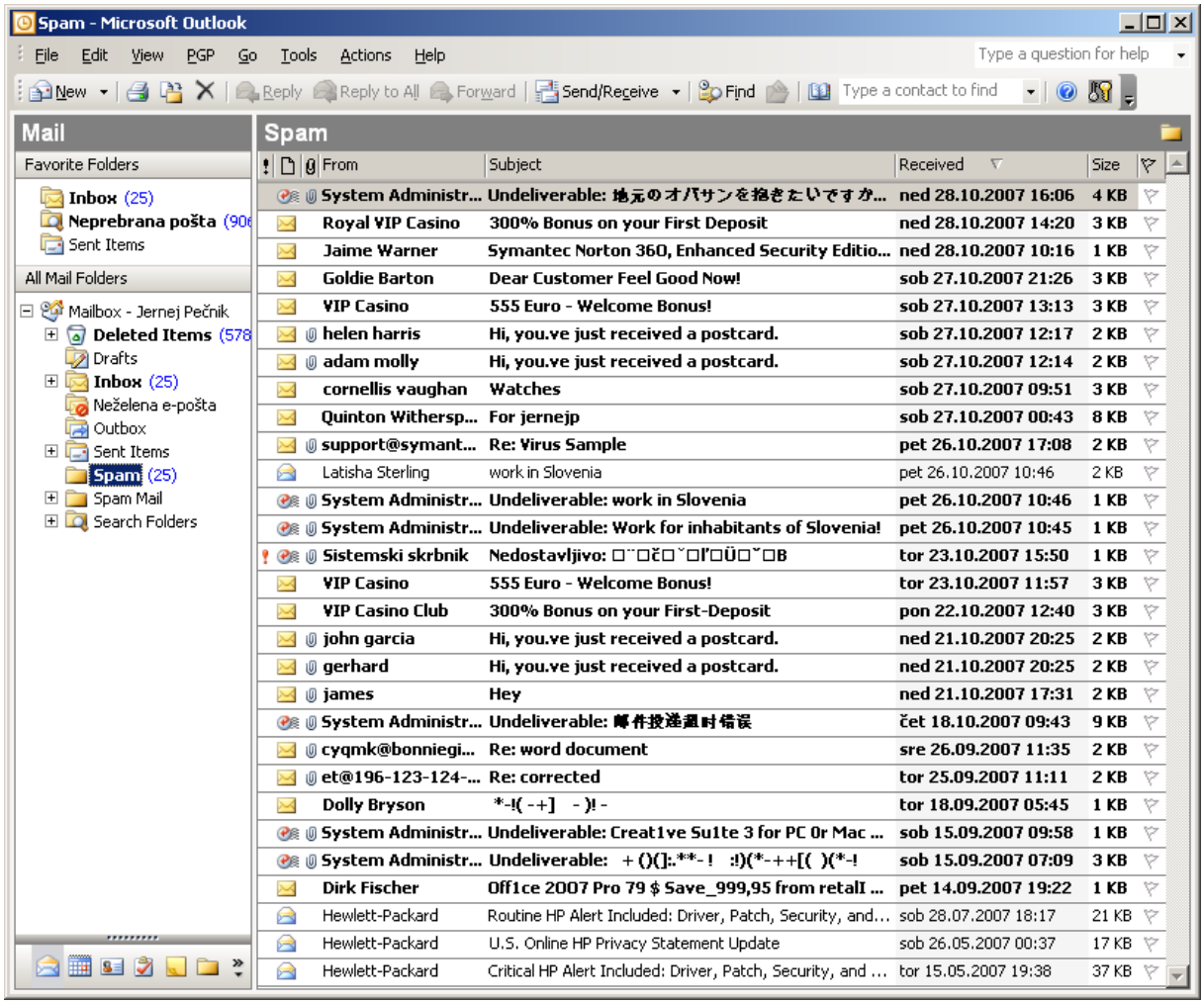
- Vohunski programi (angl. spying software), »spyware«, v sistemu zbirajo informacije o obiskih spletnih strani, spremljajo vsebino poštnih sporočil, zbirajo informacije o nameščeni programski opremi, lahko si tudi zapisujejo (»keyloger« so programčki, ki preberejo vtipkane znake na tipkovnici) uporabniška imena in gesla, ki se vpisujejo v brskalnik ali programe, z namenom izkoriščanja teh informacij v reklamne namene. Tisti, ki kradejo gesla, pa so večinoma namenjeni za bančne in ostale prevare. Večina teh programov deluje prikrito, da ne bi opozorili uporabnika na njihovo prisotnost.
- Reklamni programi (angl. advertising software), »adware«, posredujejo uporabnikom reklame, včasih naključno, včasih glede na informacije zbrane preko vohunskih programov. Reklame so v obliki nezaželene (angl. Spam) elektronske pošte, samodejnega odpiranja oken orodnih vrstic v brskalniku, njihov namen je popolnoma komercialne narave.
- Škodljivi programi (angl. malicious software), »malware«, že mejijo na področje virusov, saj delujejo izključno za škodljive namene, kot na primer pokvariti vsebino datotek ali zaustaviti delovanje sistema.

Zaščita pred temi programi so protivohunski programi, ki jih je potrebno redno posodabljati. Odsvetuje se obisk spletnih strani sumljive narave, predvsem pa je potrebno paziti, kaj se prenaša s svetovnega spleta. Če se poslužujemo dostopa do svetovnega spleta prek klicne linije, je potrebno biti pozoren tudi na telefonsko številko, s katero se računalnik poveže na svetovni splet. V primeru, ko se telefonska številka spremeni, lahko to pomeni, da je zlonamerno nameščeno programsko orodje Klicalec (angl. Dialer).

E-poštne prevare

Najpogostejša oblika e-poštnih prevar se v svetovnem spletu imenuje ribarjenje (angl. phishing), ki izvira iz analogije, da spletni hudobneži ribarijo in postavljajo vabe, za katere nevedni uporabniki zgrabijo. Pogosto so v ribarjenje vpletene dobro organizirane kriminalne združbe, ki uporabljajo poštno sporočilo kot vabo. Primer: Uporabnik dobi sporočilo, da je problem z njegovim bančnim računom in naj s klikom na povezavo odpre bančno stran (ki je v resnici le kopija bančne strani, izgled pa je lahko avtentičen). Tam se uporabniku ponudi možnost vpisa uporabniškega imena in gesla, ko ga uporabnik vnese, pa se ne zgodi nič,…).

Slika 2: Primer nezaželene elektronske pošte.



Vir: lastni vir.

Zaščita pred ribarjenjem je v izobraževanju zaposlenih. Če kdorkoli obljublja denar, ga gotovo ne bo dal; če kdo zahteva gesla, gotovo nima dobrih namer!

Nezaželeno elektronsko pošto ponavadi pošiljajo avtomatizirani poštni strežniki z namenom reklamirati, prodati ali celo oškodovati (v primeru ribarjenja) prejemnika. Zaščita pred nezaželeno elektronsko pošto je običajno nameščena na poštnem strežniku, zato to ni v pristojnosti uporabnika, lahko pa si uporabnik prepreči prekomerno prejemanje te pošte s tem, da previdno posreduje svoj elektronski naslov zlasti podjetjem in posameznikom na svetovnem spletu. Na veliko spletnih straneh so okenca, ki pozivajo, da uporabnik vpiše svoj elektronski naslov, pa bo dobil določene informacije, ugodnosti,… Ta okenca se lahko uporabljajo v nepoštene namene, elektronski naslov pa se posreduje tretjim osebam. Podobno je z objavo elektronskega naslova na spletnih straneh.

Neželena elektronska pošta je danes velik svetovni problem in lahko v podjetju zasede tudi več kot polovico elektronskega poštnega prometa. Na Sliki 2 (glej stran 19) je primer mojega osebnega elektronskega poštnega predala s primeri neželene elektronske pošte.

Orodja za brisanje sledi

Orodja za brisanje sledi se pogosto uporabljajo za zakritje napadalčevih sledi. S pomočjo teh orodij se skrije prisotnost zlonamernih programov v sistemu (orodja izvedejo zamenjavo določenih sistemskih datotek s prirejenimi datotekami). V primeru, da napadalec namesti zlonamerni program, ki je kasneje odkrit, lahko s tem napadalec izgubi nadzor ali dostop do sistema v prihodnosti. Takšne zlorabe lahko dajejo skrbniške pravice nepooblaščenim uporabnikom (Šinigoj, 2005, str. 413).

Korenski kompleti

Korenski komplet (angl. rootkit) je zbirka programov, ki omogoča skrivanje datotek, procesov ali drugih objektov ter omogoča prikrito delovanje na sistemu tako za uporabnika kot tudi za aplikacije (Harley in Lee, 2006, str. 4).

Korenski komplet v osnovi ni virus, črv ali kakršnakoli druga nezaželena programska oprema. Tehnologije korenskih kompletov so način prikrivanja aktivnosti, niso pa nujno uporabljene v zlonamerne namene. Te tehnologije so uporabljene z namenom obdržati nadzor nad sistemom. Ponavadi gre za posredno okužbo: virus ali drug predstavnik nezaželene programske opreme, neposodobljen operacijski sistem, fizičen dostop do računalnika, korenski komplet kot dodatek uporabnemu programu.

Korenski kompleti so v obliki, kot jih poznamo danes, prvič nastali sredi devetdesetih let prejšnjega stoletja, v sistemih Unix. Glede na uporabljeno metodo implementacije se korenski kompleti delijo na štiri podkategorije (Strosar, 2007, str. 100 – 103):

- programski (binarni) korenski kompleti,

- jedrni korenski kompleti,
- virtualni korenski kompleti,
- knjižnični korenski kompleti (angl. Library Rootkits).

Najpreprostejši so programski korenski kompleti, ki enostavno izvedejo zamenjavo originalnih datotek s trojanskimi oziroma prirejenimi datotekami. Programski korenski kompleti pogosto zamenjajo nekatere sistemske datoteke z modificiranimi različicami, katerih programska koda je prirejena tako, da filtrira prikazovanje določenih parametrov, ki jih napadalec predhodno definira v konfiguracijski datoteki korenskega kompleta. Tako lahko prepreči izpisovanje naslovov IP, programskih vrat, datotek, procesov in uporabnikov.

Podobno metodo uporabljajo korenski kompleti na ravni knjižnic, le da namesto programov zamenjujejo sistemske knjižnice. Napadalcu tako ni potrebno zamenjevati sistemskih programov, saj bodo ti že prejeli »prečiščene« informacije. Z zamenjavo sistemskih klicev lahko vsiljivec preusmeri izvajanje, tako da se namesto izvirnega programa dejansko izvede trojanska različica.

Danes se vse pogosteje uporablja jedrna oblika korenskih kompletov, ki prikrivajo svoje delovanje s prestrezanjem funkcij API, s katerimi preusmerjajo izvajanje na drug pomnilniški naslov. Tam je alternativna funkcija, operacija ali namenska koda, ki izvede specifične modifikacije (najpogosteje filtriranje določenih parametrov) in vrne nadzor funkciji, ki je izvedla klic.

Navidezni korenski kompleti delujejo na podlagi spremembe zagonskega zaporedja v sistemu in poženejo najprej sovražno kodo namesto samega operacijskega sistema. Ko je komplet naložen v pomnilniku, se sproži nalaganje operacijskega sistema, vendar ima ta vlogo gostujočega sistema. Ker virtualni korenski komplet deluje kot gostitelj, deluje na nižji ravni, zato lahko prestreza in kontrolira sistemske klice. Ta pristop bo najverjetneje naslednji velik korak v razvoju korenskih kompletov, saj je virtualizacija v velikem razmahu.

Socialni inženiring

Socialni inženiring se vse pogosteje omenja na predavanjih in konferencah na temo informacijske varnosti, v različnih člankih in literaturi o varnosti informacijskih sistemov. Pojavlja se na svetovnem spletu, širši javnosti pa je v primerjavi s pojmi, kot so virusi, črvi in podobno, praktično nepoznan, zato mu namenjam v tem magistrskem delu posebno pozornost v nadaljevanju. Na kratko povzemam, da so ljudje, gledano z varnostnega vidika, ena izmed glavnih ranljivosti informacijskih sistemov. Potencialni napadalec z lažno identiteto lahko preko telefona ali z drugim načinom (elektronska pošta, prevzemanje identitete drugega zaposlenega v podjetju in podobno) doseže, da mu zaposleni zaupajo pomembne informacije, kot na primer svoje geslo, in mu s tem omogočijo dostop do informacijskega sistema ter drugih podatkov in informacij.

Aktivni napadi s svetovnega spleta

Za vse napade s svetovnega spleta je vedno nekdo odgovoren. Obstaja več vrst ljudi, ki se »ukvarjajo« s spletno varnostjo (Sluga, 2005, str. 13):

- Hekerji (angl. hack – sekati) so programerji, ki se jih je prijela negativna oznaka, da so hudobneži s svetovnega spleta, a so v resnici ljudje, ki skrbijo za varnost sistemov na svetovnem spletu, s tem da odkrivajo nepravilnosti in luknje ter jih razkrivajo kot varnostne pomanjkljivosti.
- Krekerji (angl. crack – zlomiti, vdreti) so programerji, katerih cilj je podreti varnostno zaščito (programov, zaščitnih sistemov) za osebno slavo ali finančno korist. Svojo pozornost usmerjajo na podjetja ali vladne inštitucije.
- »Script kiddies« ali informacijski delikventi so ljudje (otroci), ki za zabavo izkoristijo javno objavljene programe, viruse ter javno objavljeno poznavanje varnostnih pomanjkljivosti za ustvarjanje škode, ne da bi se zavedali, kaj so pravzaprav naredili. Svojih tarč ne izbirajo po nobenem ključu, važno je, da se zabavajo (Levine in Kessler, 2002, str. 11.1).

Najpomembnejša zaščita pred napadi s svetovnega spleta je požarni zid ter posodobljeni operacijski sistemi in programi za dostop do svetovnega spleta.

Usmerjeni napadi

Za razliko od tipičnih napadov zlonamernih kod, katerih cilj je prizadeti čim več sistemov, se usmerjeni napadi osredotočajo na specifične uporabnike ali organizacije. Zlonamerne kode postanejo bolj kompleksne, saj so cilji kriminalcem, ki napadajo velike korporacije, veliko bolj ambiciozni (finančna kraja, ustvarjanje mrež botov oziroma računalnikov pod nadzorom prevarantov, kraja kritičnih podatkov, sabotaže, industrijsko vohunjenje in drugo). Tovrstni napadi so pogosto nadzirani s strani organiziranih skupin ali konkurenčnih podjetij. Velika podjetja so potencialno ranljiva tudi za usmerjene napade, s katerimi nameravajo izsiljevati žrtev. Kriminalci lahko zahtevajo tudi denar v zameno, da ne izvedejo napadov za zavrnitev storitev (DoS) ali podobnih napadov na podjetje. Podjetja o večini tovrstnih podatkov ne poročajo pogosto, saj se želijo izogniti dodatnim težavam in negativni publiciteti.

Napad za zavrnitev storitve

Pri napadih za zavrnitev storitve (angl. Denial Of Service, DOS) gre za napad na razpoložljivost sistema oziroma oviranje njegovega delovanja (Levine, Kessler, 2002, str. 11.1). Navadno napadalec to stori tako, da napadenemu sistemu pošlje veliko količino strežniških zahtevkov. Ker ima napadeni sistem omejena sistemska sredstva, mu vseh zahtevkov ne uspe obdelati in njegovo delovanje se upočasni ali pa celo popolnoma preneha. Proti napadu DOS se je mogoče boriti z blokiranjem prometa iz zlonamernega strežnika, zato se za oviranje delovanja računalniških sistemov pogosteje uporablja distribuirani napad DDOS (angl. Distributed Denial Of Service). Tu gre za podoben napad, ki pa simultano poteka iz večjega števila računalnikov, zato se ga je teže ubraniti.

Napadov za zavrnitev storitev je več vrst, angleška imena zanje pa so (Levine in Kessler, 2002, str. 11.1): Destructiv Devices (uničevanje naprav), E-mail Bombing (bombardiranje z elektronskimi sporočili), Buffer Overflow (prekoračitev pomnilnika), Bandwith Consuption (zasedanje pasovne širine), Routing and Domain Name System Attacks (sistemski napadi na domenske strežnike, SYN Flooding (poplavljanje sinhronizacij), Resource Starvation (zasedanje vseh vrst virov), Java, Router Attacks (napadi na preklopnike), Bonk and Boink, Arnudp, Cancelbot, Trinoo, Tribe Flood Network, Stacheldraht, TFN2K in druga.

USB ključ kot hekersko orodje

Za prevzem nadzora nad tujim računalnikom ni več potrebno biti heker, saj je na trgu že mogoče kupiti programsko opremo, ki to delo opravi sama. Z nakupom USB ključa Snoopstick ni potrebno niti nameščati namenskih programov, saj se namestitev opravi povsem samodejno. Na ključu se nahajata dve programski opremi. Prva omogoča prevzem nadzora nad računalnikom preko oddaljenega dostopa, medtem ko druga zagotavlja možnost oddaljenega nadzora dela v realnem času, omogoča tudi izdelavo arhiva o deskanju po svetovnem spletu, prejetih in poslanih e-sporočilih ter vsebin spletnih klepetalnic. Za namestitev vohunske opreme potrebuje ključ le slabo minuto. Ključ Snoopstick je bil v osnovi pripravljen za nadzor nad delom otrok na domačem računalniku, seveda ni izključeno, da ga ne bodo uporabljali tudi nepridipravi. Cena vohunskega ključa je 45 € (Računalniške novice, 2007, str. 32) in (www.snoopstick.com).

Ostale nesreče

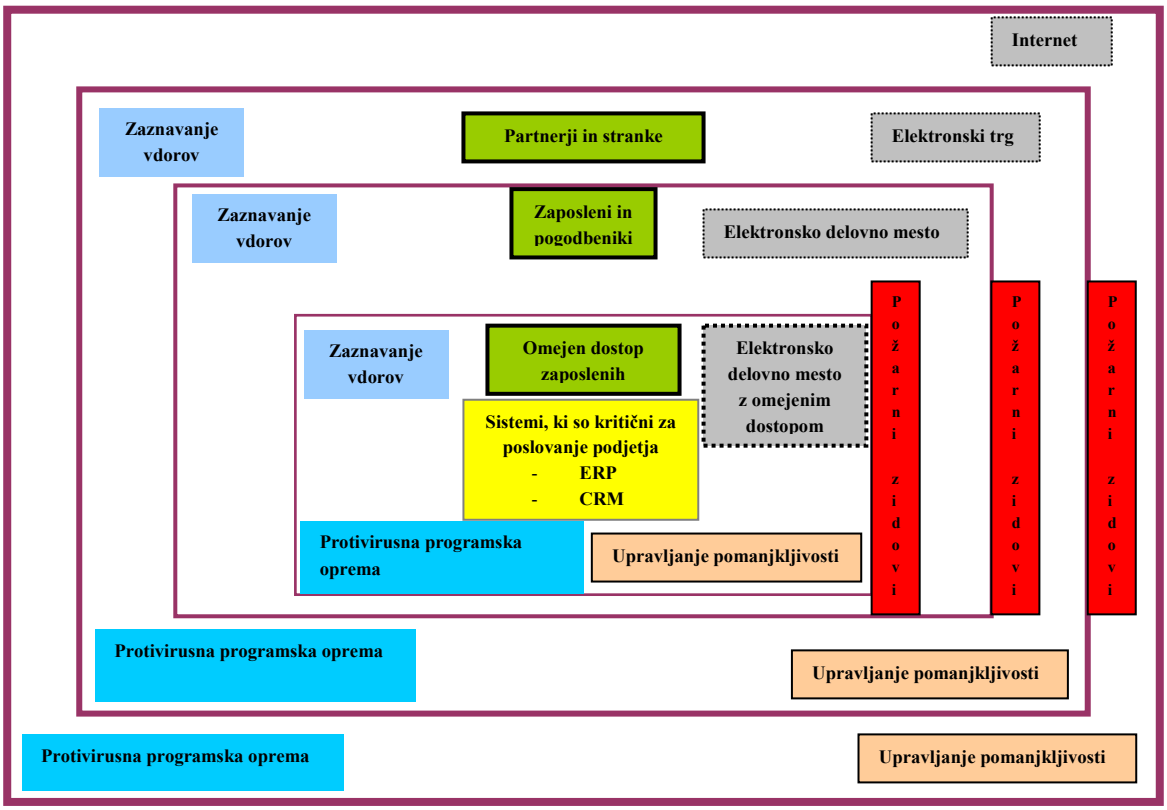
Večina izmed prej naštetih nesreč ogrozi predvsem delovanje informacijskega sistema, posledično pa podporo poslovno kritičnim poslovnim procesom. Omeniti je potrebno še naravne nesreče (požar, poplave, nevihte, epidemije, potres, snežne nevihte, tornado), fizično krajo, terorizem, poslovne krize (izguba dobaviteljev, politična situacija, izguba tovora, ugrabitev, zakonodaja, medijski pritiski, izguba strank, smrt zaposlenih, tožbe, spolni škandali, stavke) in podobno. V vseh teh primerih se lahko elektronska in papirna dokumentacija uniči ali poškoduje, kar predstavlja nepopravljivo škodo. Organizacije morajo tudi za vse te primere imeti pripravljen načrt okrevanja, tipično pa je ta zapisan v dokumentu varnostne politike (Šinigoj, 2005, str. 414).

2.6. Tehnološka zaščita

Tehnologija je sestavni element učinkovitega sistema za varovanje informacij. Na trgu je veliko število ponudnikov, ki pa povzročajo zmedo s svojimi pretiranimi trditvami o zmožnostih njihove opreme. Prav vsak ponudnik zagotavlja, da bo njegova tehnologija izpolnila vse varnostne zahteve. Pomembno je upoštevati dejstvo, da sama tehnologija še ne bo rešila vseh težav z varnostjo informacij. Če podjetja to področje preveč poudarjajo in se osredotočajo samo na tehnologijo, imajo lažen občutek varnosti in so lahko izpostavljena nepotrebnemu tveganju (Egan in Mather, 2005, str. 29).

V učinkoviti arhitekturi vseh programov za varovanje informacij morajo biti tudi plasti, ki omogočajo več ravni obrambe, to lahko imenujemo večplastno varovanje (glej Slika 3, stran 24). Računalniško okolje je potrebno razdeliti na več področij in omogočiti zaščito vseh ravni omrežja, tudi ravni prehodov (povezava med dvema deloma računalniškega okolja, npr.: svetovni splet in notranje omrežje podjetja), strežnikov (to so računalniki v skupni rabi, ki izvajajo aplikacije ali zahteve več zaposlenih) in odjemalcev (to so posamezni računalniki, ki jih uporabljajo zaposleni, prenosni računalniki ali drugi digitalni osebni pripomočki).

Slika 3. Program za varovanje poslovanja podjetja.



Vir: Egan, Mather, 2005, str. 30.

V smislu tehnološke zaščite je potrebno ovrednotiti in upoštevati naslednje komponente:

- **Preverjanje pristnosti, pooblaščanje in vodenje računov** (angl. authentication, authorization and accounting)

Varnost je kršena, ko nepooblaščeni uporabnik dobi dostop do sredstev ali ko uporabnik preseže svojo dodeljeno raven dostopa do zavarovanega sistema (Overly, 1999, str. 71). Preverjanje pristnosti je postopek, ki določi identiteto uporabnika in je najzanesljivejše v kombinaciji štirih načinov (Sandhu, 2002, str. 16.2 – 16.5):

- Kaj poznaš (angl. What you know): gesla, fraze.
- Kaj imaš (angl. What you have): pametne kartice, ključi.

- Kaj si (angl. What you are): mirujoči biometrični izkazi - prepoznava prstnih odtisov, očesne mrežnice in šarenice.
- Kaj delaš (angl. What you do): gibljivi biometrični izkazi - glas, pisava.

Pooblaščanje določi, do česa ima uporabnik dostop, vodenje računov pa je orodje, ki preverja te postopke. Uporabniška imena in gesla so najosnovnejša oblika preverjanja pristnosti in so kot elektronski ključ za vstope v različne sisteme. Ker so to temeljni sestavni deli sistema za varovanje informacij, je potrebno te ključe pazljivo nadzorovati in skrbeti, da ne pridejo v napačne roke. Če si heker pridobi ključ, se lahko izdaja za nekoga drugega, pridobil pa si je tudi pripadajoči dostop do računalnika in omrežja (Overly, 1999, str. 73).

Naprednejša tehnologija omogoča še več varnosti med postopkom preverjanja. Sem spada uporaba pametnih kartic (te hranijo dodatne informacije za identifikacijo uporabnika) in biometričnih sistemov (edinstvene biološke značilnosti uporabnika, skeniranje prstnih odtisov ali očesne mrežnice). Na trgu obstaja tudi že tehnologija, ki omogoča ugotavljanje položaja s sateliti za globalno določanje položaja.

- Požarni zidovi / virtualna zasebna omrežja (angl. Firewall / VPN-virtual private networks)
Požarni zidovi sestavljajo »elektronsko« ograd okoli računalniškega okolja. Vsebujejo filtre, ki samo določenim vrstam omrežnega prometa dovolijo vstop v omrežje podjetja in zavrnejo vse podatke, ki ne izpolnjujejo določenih meril.

Požarni zid je program ali naprava, ki preprečuje prehod na računalnik ali v računalniško omrežje iz javnega omrežja (svetovnega spleta) s tem, da zapre dostopne poti (vrata, angl. port) do mrežnih storitev, kot so na primer za okolje Oken (Norberg, 2001, str. 177-178) spletni strežnik (vrata 80), poštni strežnik (vrata 110, 143, 25,..), omrežne datoteke Oken (vrata 135-139) in ostalih vrat od 1-65535, razen tistih, ki so izrecno dovoljene.

Požarne zidove lahko razvrstimo v naslednje kategorije:

- *Požarni zidovi, ki filtrirajo pakete*
  Paketni požarni zidovi varujejo tako, da pregledajo glavo ali informacije o naslovu paketa ali sporočila, ne iščejo pa morebitne nevarnosti v telesu paketa.
- *Požarni zidovi s tehnologijo nadzora suverenosti* (angl. statefull inspection)
  Ti požarni zidovi nadzorujejo stanje transakcije paketa in preverijo, ali se naslov prejemnika prihajajočega paketa ujema z virom predhodne izhodne zahteve (požarni zid preverja legitimnost, to pa stori na podlagi tabele povezav).
- *Požarni zidovi na ravni aplikacij ali strežnikov proxy* (namestnik, zastopnik - angl. proxy)
  Najvarnejši požarni zidovi delujejo na ravni aplikacij ali na osnovi strežnikov proxy. Ti preberejo in ponovno napišejo vsak paket, tako zagotavljajo prehod skozi omrežje

> samo veljavnim sporočilom. Ta postopek je varnejši, ker hekerji težko napišejo neustrezno vsebino v telo paketa. Slaba stran tega postopka je zmanjšanje prepustnosti. Strežniki proxy varujejo omrežje tako, da ponujajo zaščito z uporabo vmesne postaje, kar pomeni, da se spletni brskalnik povezuje s strežnikom proxy in ne neposredno s spletnim mestom. To pomeni, da bo tarča napada ali poskusa vdora v zasebnost proxy strežnik in ne računalniki uporabnikov ali drugi strežniki (Gralla, 2004, str. 189).

Ne glede na strojno ali programsko različico požarnega zidu je pomembno, da ga informatiki razumejo. Požarni zidovi so bistveni del varnosti omrežij, vendar ne morejo biti odgovor na vse varnostne izzive. Požarni zidovi so le zmogljivi del celotne varnostne politike. Primerjamo jih lahko z vhodnimi vrati. Dobro jih je imeti, a če jih ne zaklepamo, nam ne koristijo kaj dosti. Prav tako debela vrata prav nič ne koristijo na hiši s trhlimi zidovi. Požarni zidovi tudi ne morejo obvarovati pred zlonamerno programsko kodo. Ne glede na napredek analize stanja, ki zmore v sodobnih požarnih zidovih zavračati določene neprimerne vsebine, bo vedno mogoče napisati zlonameren program, ki bo požarni zid zaobšel.

Orodja VPN omogočajo izdelavo varne zasebne povezave med dvema mestoma z uporabo javnega omrežja, običajno kar svetovnega spleta. VPN zaščiti podatke tako, da jih šifrira, s čimer nepooblaščeni osebi onemogoči branje. Povezava se vzpostavi s kombinacijo strojne in programske opreme na obeh straneh. To možnost imajo tudi nekateri požarni zidovi. Omrežja VPN so stroškovno učinkovit način vzpostavljanja zasebnega omrežja, predvsem v primerjavi z najemom lastne linije, ki pa je verjetno smiselna za zagotavljanje varnosti podatkov v finančnem sektorju.

- Protivirusna programska oprema

Protivirusna programska oprema pomaga preprečiti okužbe računalnikov z virusi, s črvi in trojanskimi konji. Vse to lahko opredelimo tudi z zlonamerno kodo. Hekerji izdelajo na stotine virusov vsak mesec, kar pomeni, da je potrebno protivirusno programsko opremo redno posodabljati z novimi opisi virusov. Računalniški virusi se širijo na različne načine, tudi z elektronsko pošto, vendar za širjenje potrebujejo uporabnika. Nevarnejši so računalniški črvi, ki se znajo sami razmnoževati in za širjenje ne potrebujejo uporabnika. Protivirusna programska oprema uporablja dva načina za zaščito sistemov pred zlonamerno kodo, to sta podpisi virusov in hevristika. Prvi način je reaktiven, ker je potrebno podpis virusa poznati vnaprej, če želimo, da protivirusni program sploh spozna virus. Če avtor virusa naredi novo različico virusa, je potrebno narediti tudi nov opis virusa. Samo s tem načinom je nemogoče biti korak pred izdelovalci virusov. Ker so virusi tako dinamični, je protivirusna industrija razvila bolj proaktiven način, ki se imenuje hevristika. V tem načinu protivirusna programska oprema išče vzorce, ki lahko zaznajo morebitne viruse, pri tem pa se nanaša na zbirko podatkov o znanih vrstah virusov. Ta način še ni dovolj uspešen in lahko povzroči lažen alarm.

- Upravljanje pomanjkljivosti

Upravljanje pomanjkljivosti pomeni proaktiven način odstranjevanja pomanjkljivosti iz sistema za varovanje informacij. Učinkovit varnostni program vključuje uporabo samodejnih orodij za upravljanje pomanjkljivosti, ki identificirajo mogoče ranljive točke v računalniškem okolju. Orodja za upravljanje pomanjkljivosti primerjajo okolje z zbirko podatkov o znanih ranljivih točkah in določijo, ali ima to okolje katero od teh pomanjkljivosti. Ta orodja lahko delujejo na osnovi omrežja (pregleduje se promet v omrežju) ali pa na osnovi gostitelja (pregleduje se fizične naprave, na primer strežnike). Čeprav se za nameščanje varnostnih popravkov porabi veliko časa, redno pregledovanje okolja in nameščanje ustreznih popravkov močno izboljša varnost in je precej boljše kot primoran odziv na napad, ki je izkoristil ranljivo točko v okolju (Tulloch, 2005, str. 301 – 317).

- Zaznavanje vdorov

Sistemi za zaznavanje vdorov (angl. intrusion detection systems) nadzorujejo promet in dogodke v omrežju in pri odjemalcih. Iščejo vzorce, ki bi lahko pomenili, da napad ravno poteka ali je bil izveden v preteklosti (Bace, 2002, str. 37.2). Orodja se nanašajo na dva načina zaznavanja vdorov in sicer na prepoznavanje na osnovi podpisov in zaznavo nepravilnosti. Za prvi način je značilno primerjanje določenih vzorcev dogajanja z znanimi scenariji napadov. Tak primer je »Ping-of-Death« (napad smrti), ki ima značilen vzorec, ker pošilja veliko število ukazov ping (preprost ukaz, ki služi za ugotavljanje prisotnosti drugega računalnika) in poskuša tako preobremeniti sistem. Drugi način, zaznava nepravilnosti, najprej določi vzorec običajnega vedenja omrežja in nato zazna vedenje, ki se razlikuje od običajnega. Če bi se na primer uporabnik poskusil povezati z naključnim omrežnim gostiteljem, s katerim se običajno ne povezuje, bi sistem zaznal razliko v primerjavi z običajnim vedenjem in jo prijavil (Norberg, 2001, str. 166). Običajno vedenje omrežja se lahko zelo razlikuje med posameznimi omrežji, napadalci pa lahko uporabijo različne vzorce napadov, zato lahko orodja za zaznavanje vdorov prijavijo veliko nepotrebnih alarmov. Zaradi tega lahko osebje v prihodnje te alarme obravnava kot manj pomembne.

- Filtriranje vsebine

Na svetovnem spletu je ogromna količina informacij, večina je koristna in primerna za vse ljudi. Po drugi strani se je svetovni splet izkazal kot učinkovit medij za razpečevanje neprimernih vsebin. Orodja za filtriranje vsebine lahko filtrirajo take informacije in tako zagotovijo, da zaposleni ali otroci ne morejo imeti dostopa do takih vsebin. Dve največji kategoriji filtriranja sta filtriranje spleta in filtriranje elektronske pošte. Filtriranje spleta sestoji s prepovedjo dostopa do določenih naslovov (zbirke podatkov z znanimi spletnimi naslovi ali URL-ji iz kategorij neprimernih vsebin, kot so pornografija, igranje na srečo, sovraštvo), lahko pa vsebujejo tudi ključne besede, ki naj bi bile neprimerne. Filtriranje elektronske pošte se običajno izkaže za učinkovito z blokado večine tipov priponk, sploh tipa *.exe, in *.bat. Skozi filter se spusti le nekaj znanih, običajno neškodljivih tipov datotek, kot so *.doc, *.xls in podobno.

Če programi za filtriranje postanejo preveč nadležni, se zaposleni lahko čutijo ogrožene, ker imajo občutek, da so cenzurirani in opazovani. To težavo podjetja običajno rešijo z internimi akti. Vsekakor pa neželena pošta in uporaba (zloraba) svetovnega spleta ter elektronske pošte v privatne namene med delovnim časom močno vplivata na produktivnost (se zmanjša) zaposlenih, povečanje skupnih stroškov, poleg tega to resno vpliva na skupno varnost informacijskega sistema (Overly, 1999, str. 3).

- Šifriranje

Šifriranje je postopek pretvorbe podatkov v obliko, ki jo nepooblaščena oseba težko prebere. Dve moderni obliki šifriranja sta (Overly, 1999, str. 75-76):

- simetrično šifriranje, kjer obe strani uporabljata isti skrivni ključ za šifriranje in dešifriranje sporočil,
- asimetrično šifriranje, kjer obe strani za šifriranje in dešifriranje uporabljata javni ključ in lastne zasebne ključe. Pošiljatelj sporočila mora imeti javni ključ prejemnika in z njim šifrirati sporočilo. Prejemnik nato lahko s svojim zasebnim ključem dešifrira tako sporočilo. Nihče ne more samo z javnim ključem dešifrirati sporočila ali odkriti zasebnega ključa.

Danes se v elektronskem trgovanju največ uporablja tehnologija SSL (plast varnih vtičnic, angl. Secure Sockets Layer), ki uporablja asimetrično in simetrično šifriranje. Večina sistemov, ki uporablja zaupne informacije, kot so številke kreditnih kartic, uporablja to tehnologijo.

3. Standard BS 7799

Po vstopu v EU so prilagoditve organizacij potrebne tudi na področju zagotavljanja visoke kakovosti in zanesljivosti storitev.

Zaradi kompleksnosti informacijskih sistemov se v poslovnih okoljih pojavlja potreba po sistematičnem obvladovanju varnosti na organizacijskem nivoju. Takšen celovit način upravljanja varnosti vpeljujejo razni standardi in priporočila, ki obravnavajo področja varovanja informacij. Med najbolj znanimi tovrstnimi dokumenti, na katere se lahko organizacije oprejo pri oblikovanju sistema za upravljanje informacijske varnosti, so (Brezavšček in Zupan, 2006, str. 2-3):

- COBIT – zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije,
- ITIL – zbirka najboljše prakse za upravljanje informacijskih storitev,
- BS 7799-1 in 2 - kodeks za upravljanje informacijske varnosti in zahteve, ki jim mora SUIV v organizaciji ustrezati,

- BS ISO/IEC 13335 – smernice za upravljanje varovanja informacijske tehnologije,
- ISO/IEC TR 18044 – smernice za upravljanje incidentov pri varovanju informacij,
- PAS 56 – vodnik za upravljanje neprekinjenega poslovanja,
- PD 3000 – serija petih vodnikov, ki nudijo uporabnikom pomoč pri vzpostavitvi in vzdrževanju SUIV v organizaciji,
- NIST 800-14 – splošno sprejeti koncepti in prakse za varovanje informacijskih sistemov,
- OCTAVE – metodologija za operativno ocenjevanje kritičnih groženj, dobrin in ranljivosti,
- OECD – smernice za varovanje informacijskih sistemov in omrežij.

Poleg naštetih dokumentov so v strokovni literaturi še drugi standardi, priporočila (GASSP) in smernice, ki obravnavajo specifična, ožja področja, kot so šifriranje podatkov, varovanje komunikacij, kartice za preverjanje istovetnosti zaposlenih, za informacijsko tehnologijo (GMITS ISO, okvir COBIT) in podobno.

V tem magistrskem delu se osredotočam na standard BS 7799 (angl. British Standard), ki je eden najbolj pogosto uporabljenih standardov na tem področju. Je mednarodno veljaven standard in predstavlja model za učinkovit sistem upravljanja varovanja informacij. Standard določa smernice in splošna načela za začetek, vpeljavo, vzdrževanje in izboljševanje upravljanja varovanja informacij v organizaciji. Cilji, ki so začrtani v tem standardu, dajejo splošna navodila glede sprejetih ciljev upravljanja varovanja informacij.

Z vpeljavo ciljev kontrol in kontrol tega mednarodnega standarda se izpolnijo zahteve, določene z oceno tveganja. Standard lahko služi kot praktična smernica za razvoj varnostnih standardov v organizaciji in za učinkovito izvajanje varstvenih ukrepov, s tem pa hkrati pripomore k vzpostavitvi medsebojnega zaupanja pri poslovanju med organizacijami.

Standard je kot kodeks upravljanja informacij prvič izšel leta 1995 v Veliki Britaniji, izdal ga je British Standard Institution. V Sloveniji je leta 1997 standard kot kodeks dobil tudi status slovenskega standarda.

Zadnjo, prenovljeno verzijo standarda, ki je izšla v drugi polovici leta 2005, sestavljata dva dela:

- BS ISO/IEC 17799:2005,
- BS ISO/IEC 27001:2005.

Standard vsebuje 11 poglavij o varnostnih kontrolah, ki skupaj vključujejo 39 glavnih varnostnih kategorij in eno uvodno poglavje, ki predstavi oceno in obravnavo tveganja.

Osnovna poglavja standarda so (število v oklepaju predstavlja število glavnih varnostnih kategorij):

a) varnostna politika (1),
b) organizacija varovanja informacij (2),
c) upravljanje sredstev (2),
d) varovanje človeških virov (3),
e) fizična zaščita in zaščita okolja (2),
f) upravljanje s komunikacijami in produkcijo (10),
g) nadzor dostopa (7),
h) nabava, razvoj in vzdrževanje informacijskih sistemov (6),
i) upravljanje incidenta pri varovanju informacij (2),
j) upravljanje neprekinjenega poslovanja (1),
k) združljivost (3).

Vsaka glavna kategorija varovanja vključuje:

- cilj kontrole, ki navaja, kaj je treba doseči,
- eno ali več kontrol, ki jih je treba uporabiti za doseganje cilja kontrole.

Revidirana verzija standarda ponuja organizacijam pomembno orodje za upravljanje tveganj na področju varovanja informacij, izboljšane sposobnosti za obvladovanje incidentov in podporo zagotavljanju neprekinjenega poslovanja. S tem pomaga organizacijam pri izkoriščanju tržnih priložnosti. Ključni namen je omogočiti podjetjem varovanje zaupnosti, celovitosti in razpoložljivosti občutljivih in kritičnih informacij.

3.1. Zagotovilo pri opravljanju varnosti informacij

Pridobljen certifikat po standardu BS 7799 pomeni vodilo za vse aktivnosti zagotavljanja varnosti pri posredovanju in hrambi informacij. Je orodje stalnega izboljševanja poslovnega procesa v smislu upravljanja varnosti informacij. Vzpostavljen notranji informacijski sistem je potrebno vzdrževati in ga stalno izboljševati. Ravno v tem je standard BS 7799 soroden s standardi (angl. Information Security Standard) ISO 9001 (kakovost), ISO 14000 (opisuje sistem ravnanja z okoljem, obvladovanje nenamernih proizvodov), ISO 1800 (zdravje zaposlenih) (Ključevšek et al, 2001, str. 3). Ti standardi se po svoji strukturi zbližujejo z namenom zniževanja stroškov pri vzpostavitvi in vzdrževanju dveh ali več standardov v isti organizaciji.

Standard BS 7799 še v nobeni državi ni zakonsko obvezen; slovenska zakonodaja izjemoma za banke predpisuje usklajenost bank z njim, ne pa tudi certificiranja.

Uporaba standarda prinaša poslovne koristi. Pri vpeljavi standarda organizacije dobro spoznajo tveganja, s katerimi se srečujejo in jih zmanjšajo na želeno raven. V stikih s partnerji organizacije v skupno zadovoljstvo varujejo lastne in partnerjeve informacije, kar prispeva k dobrim odnosom in zmanjševanju nesporazumov ali zamer. Pri elektronskem poslovanju in njegovem ritmu dela je opora na standard skoraj nujna, da se organizacije izognejo nepreglednemu poslovanju in ravnanju z informacijami. Ko organizacije upravljajo z varnostjo informacij, šele res postanejo njeni dobri gospodarji (Ključevšek et al, 2001, str. 3). Organizacije, ki želijo v prihodnosti pridobiti certifikat skladnosti z novim standardom, morajo izvesti podrobno primerjavo med varovalnimi ukrepi, ki so v organizaciji že vpeljani, in kontrolami, ki jih predlaga nova verzija standarda. V primeru odstopanj morajo izvesti ustrezno analizo tveganja. Organizacije morajo imeti jasno definirane vloge in odgovornosti, povezane z zagotavljanjem informacijske varnosti, kakor tudi sankcije v primeru njihovega neizvajanja.

Temeljne zahteve standarda BS 7799 so:

- izgradnja formalnega upravljavskega okvira,
- določitev obsega,
- določitev seznama viro,
- izdelava formalne ocene tveganj,
- določanje in upravljanje sprejemljive meje tveganja,
- izbira primernih varnostnih kontrol (izjava o primernosti),
- zavezanost vodstva,
- razdelitev odgovornosti,
- varnostno ozaveščanje in šolanje,
- poročanje o varnostnih dogodkih,
- neprestane izboljšave,
- izdelana dokumentacija.

Standard ISO/IEC 17799:2005 je kodeks varovanja informacij in certifikacija po tem standardu ni mogoča, ker standard ni bil načrtovan s tem namenom in tudi ni primeren za ta namen. V ta namen je pripravljen standard ISO/IEC 27001 Information Security Management System, ki je revidirana verzija standarda BS 7799 Part 2:2002. Postopek certifikacije je podoben certifikaciji po standardu ISO 9001 Quality management System (QmS) in standardu ISO 14001 Environmental Management System (EMS).

Proces certifikacije sestoji iz treh faz. V prvem delu se organizacija pripravlja na certifikacijo, razvije in implementira svoj sistem upravljanja varovanja informacij. Vzpostavljen sistem integrira v svoje vsakodnevne poslovne procese in aktivnosti, usposobi svoje zaposlene in izvaja proces vzdrževanja sistema upravljanja varovanja informacij.

V drugem delu organizacija najame akreditiran certifikacijski organ, ki izvede presojo sistema upravljanja varovanja informacij, presojevalec pa se osredotoči na vzpostavljenost in dokumentiranost sistema upravljanja varovanja informacij, ki zajema:

- pregled varnostne politike in ciljev,
- pregled obsega sistema, podpornih postopkov in kontrol,
- poročilo o oceni tveganja, vpeljane programe in ukrepe za zniževanje tveganj,
- izjavo o primernosti in podobno.

Drugi del presojevalčeve presoje je izveden s poudarkom na izvajanju in učinkovitosti sistema vodenja varovanja informacij, izpolnjevanju zahtev standarda ISO/IEC 27001, zakonskih zahtev in določb ter zahtev zainteresiranih strank.

Organizacija pridobi certifikat, če je presoja uspešna. Certifikat se podeljuje za obdobje treh let, po tem obdobju je potrebna ponovna certifikacija. Tretja faza je faza vzdrževanja in izboljševanja sistema upravljanja varovanja informacij, v kateri certifikacijski organ v rednih časovnih intervalih obiskuje organizacijo in preverja izpolnjevanje predpisanih zahtev.

Koristi opiranja na standard BS 7799 v organizacijo so (Zupan, 2005, str. 39):

- standard omogoča osnovo za vpeljavo najboljših praks,
- je upravljavsko, tehnološko in organizacijsko neodvisno orodje ter dovolj splošen, da je primeren za vse vrste organizacij,
- s standardom zagotovimo celovito pokrivanje področja informacijske varnosti (zmanjšamo možnost, da bi spregledali pomembna področja),
- standard BS 7799 omogoča sistematičen in konsistenten pristop ne samo pri vpeljavi, temveč tudi pri vzdrževanju sistema za upravljanje informacijske varnosti,
- uporaba standarda za varovanje informacij omogoča osnovo za ugotavljanje odstopanj in predvideva tudi vire za varovanje,
- opiranje zgolj na izkušnje posameznikov ni več potrebno, saj se pri zapisovanju politike in nadzorstev, ki zagotavljajo ustrezen nivo varnosti, lahko naslonimo na standard.

Koristi uvedbe standarda BS 7799 v organizacijo so (Zupan, 2005, str. 39-40):

- povečanje produktivnosti,
- revizije omogočajo nepristranski zunanji pogled na poslovanje, odkrivanje možnosti za izboljšanje,
- standard vpeljuje discipline, kot so ocenjevanje tveganja in hranjenje zapisov,
- povečanje zanesljivosti delovanja celotnega informacijskega sistema,
- omogoča hitro in učinkovito uvajanje novih sodelavcev,

- povečanje zaupanja poslovnih partnerjev in drugih interesnih skupin,
- povečanje ugleda,
- povečanje prednosti pred tekmeci,
- izboljšanje osnov za marketing in trženje storitev,
- izpolnjevanje zakonskih zahtev,
- izpolnjevanje zahtev poslovnih partnerjev in odjemalcev.

Zakonske zahteve za skladnost z BS 7799 v Sloveniji so trenutno najbolj zavezujoče za banke. Julija 2004 je Banka Slovenije objavila, da mora banka pri svojem poslovanju upoštevati slovenska standarda SIST BS7799-2:2003 in SIST ISO/IEC 17799:2003, poleg tega za banke velja mednarodni standard Basel II, ki banke tesneje kot standard BS 7799 zavezuje k ureditvi področja informacijske varnosti prek zagotavljanja ustreznega nivoja tveganj in zmanjšanja operativnih tveganj. Za ostale panoge posebna zakonska določila glede skladnosti s standardom ne obstajajo, vendar pa podjetja sama opažajo veliko potrebo po varnem in zaupanju vrednem poslovanju (Zupan, 2005, str. 38-39).

Cerifikat BS 7799 lahko pomeni izkaz urejenega poslovanja, saj omogoča boljše prepoznavanje in zmanjševanje varnostnih tveganj na želeno raven, izboljšanje poslovnih partnerstev (večja zaupnost medsebojno izmenjanih informacij) ter boljše obvladovanje procesov varovanja informacij.

3.2. Vpeljava sistema za upravljanje varovanja in zaščito informacij

V smislu varovanja in zaščite informacij je predvsem potrebno zagotoviti (Zupan, 2005, str. 40-41):

- *zagotavljanje zaupnosti* (zaščita informacij v kakršnikoli obliki, pisni, ustni, elektronski, neelektronski, pred vsakršnim nepooblaščenim vpogledom),
- *zagotavljanje celovitosti* (zagotavljanje točnosti in popolnosti informacij med njenim shranjevanjem, prenašanjem in obdelovanjem),
- *zagotavljanje razpoložljivosti* (zagotavljanje dostopnosti informacij, kadar jih ti potrebujejo in kjer jih potrebujejo).

Za potrebe varnega poslovanja v sodobnem poslovnem okolju morajo podjetja vzpostaviti in implementirati sistem za upravljanje varnosti informacij, ki ga je potrebno nadalje stalno nadzorovati in izboljševati. Ta pristop je zagotovilo, da sistem resnično zmanjšuje tveganja. Tak sistem mora temeljiti na ciljih varovanja ter v ustrezni izbiri strategije v odvisnosti od načina in obsega poslovanja, velikosti podjetja, razpoložljivih resursih, organizacijski strukturi in kulturi ter zrelosti organizacije. Bistvo vpeljave sistema upravljanja varnosti informacij je vpeljava sistema za upravljanje tveganj. Standard BS 7799 vpeljuje pomemben princip, imenovan PDCA, Načrtuj – Izvedi – Preveri – Ukrepaj (angl. Plan – Do - Check -

Act). Ta princip pokriva vse faze delovanja sistema za upravljanje informacijske varnosti, od njegove vzpostavitve do zrele faze delovanja. V nadaljevanju so naštete aktivnosti, ki se morajo izvajati v vsaki od posameznih faz (Zupan, 2005, str. 41-42):

- *načrtovanje in vzpostavitev sistema za upravljanje informacijske varnosti* (obseg, varnostna politika, pristop k ocenjevanju tveganja, izvedba ocene tveganj, izbira nadzorstva za zmanjševanje tveganj, izjava o primernosti nadzorstev, odobritev vodstva),
- *vpeljava in izvajanje sistema za upravljanje informacijske varnosti* (oblikovanje načrta ravnanja s tveganji, terminski plan uvedbe, seznam priporočenih nadzorstev, usposabljanje za ozaveščanje zaposlenih, vodenje in izvajanje ustreznih postopkov),
- *spremljanje in preverjanje sistema za upravljanje informacijske varnosti* (izvajanje nadzorovalnih postopkov, pregledovanje učinkovitosti sistema za upravljanje informacijske varnosti, pregledovanje preostalih in sprejemljivih tveganj, redno izvajanje notranjih presoj, izvajanje vodstvenih pregledov, beleženje dejanj in dogodkov),
- *vzdrževanje in izboljševanje sistema za upravljanje informacijske varnosti* (uvedba prepoznanih možnih izboljšav, vpeljava korektivnih in preventivnih ukrepov, prek komuniciranja in posvetovanja doseganje potrebnega nivoja strinjanja vseh vpletenih),
- *dokumentacija sistema za upravljanje informacijske varnosti* (krovne varnostne politike in cilji, definicije obsega sistema za upravljanje informacijske varnosti, poročila o oceni tveganj in načrti ravnanja s tveganji, izjave o primernosti nadzorstev, področne varnostne politike, dokumentirani postopki in delovna navodila, zapisi in dnevniki, ki se ustvarjajo pri delovanju sistema za upravljanje informacijske varnosti).

4. Varnost informacijskih sistemov in etika

Zakaj poglavje o etiki v magistrskem delu na temo varnost informacijskih sistemov? V informacijski dobi je veliko možnosti napačnih uporab in zlorab informacij, kar povzroča podjetjem varnostne težave. V primeru informacijske varnosti se etika nanaša na sistem moralnih principov, povezanih s prednostmi in slabostmi določenih dejanj, ter na poštenost in nezakonitost motivov in zaključkov teh dejanj (Linderman, 2002, 30.2). Zlato etično pravilo, princip, ki je temeljen in brezčasen, je: *Ne delaj drugim, kar ne želiš, da drugi naredijo tebi*. Kljub modernim tehnologijam, ki so ustvarile nove možnosti za neetično vedenje, ni potrebno razvijati novih načel za obravnavanje etike. Kot primer: večina načel za vodenje prodaje od vrat do vrat (vključujejo vljudnost, uglajenost, olikanost, izbranost in podobno) velja tudi za spletno tehnologijo. Pomanjkljivo regulacijo novih pojavov nadomeščajo kodeksi računalniške poklicne etike in netikete kot pravila obnašanja na svetovnem spletu (Pivec, 2001, str. 1). Informacijska etika nosi v sebi potencial makroetike, saj je informacija univerzalna entiteta, ki odslikava vsa stanja in delovanja.

Informacijska družba je prisotna tudi v Sloveniji, zato so tudi za nas aktualna vprašanja (Rogerson, 2001):

- Ali informacijska družba uveljavlja socialno in ekonomsko pravičnost?
- Ali se v informacijski družbi vzpostavlja reciprociteta ali pa ostaja moč odločanja v rokah manjšine?
- Ali je v ospredju korist vseh ali le nekaterih?
- Ali gre prvenstveno za ljudi ali za tehnologijo?
- Ali se v informacijski družbi ekonomija usklajuje s socialnimi in ekološkimi prioritetami?
- Ali je informacijsko komunikacijska tehnologija v službi reverzibilnosti ali ireverzibilnosti razvoja?

Vsa vprašanja so etično motivirana in zahtevajo ločevanje dobrega od slabega.

4.1. Opredelitev in zgodovina etike in morale

Kljub dejstvu, da etika kot filozofska disciplina že dolgo obstaja, smo v razvitih delih sveta priča čedalje večjemu pomenu etike, tako na zasebnem kot tudi na poslovnem področju. Mnoga podjetja, organizacije, združenja ter poklici urejajo etično ravnanje s predpisi, smernicami in kodeksi etike.

Etika obsega sistematično obravnavanje morale nasploh, išče vzporednice v vsakdanjem življenju ter razvija orodja za banaliziranje moralnih zadev na osebni in na družbeni ravni (Tavčar, 1994, str. 136).

Etika se je razvila iz razlag nravstvenih pojavov v verstvih davnih civilizacij in v pravno političnih ureditvah. Etika kot filozofska stroka se je pojavila z nastankom filozofije v Grčiji, za začetnika lahko smatramo Sokrata in Platona, prvi celoviti znanstveni etični sistem pa je Aristotelova Nikomahova etika. Za Aristotela je najvišji cilj vse človeške dejavnosti srečnost (evdaimonija), ki jo vedno iščemo zaradi nje same in nikoli ne zaradi česa drugega (Fürst in Halmer, 1990, str. 158). S helenizmom so se etiki odprla nova obzorja, ukvarjali so se s problemom duševnega miru in bivanjskega ravnotežja. Renesansa je v etiki postavila na mesto boga človeka. Glavni predstavniki etike v novem veku so Kant, Leibniz, Hegel, Lenk. V zadnjih desetletjih se z moralno-etično tematiko ukvarjajo tudi empirične znanosti, zlasti sociologija, socialna antropologija in psihologija.

Etika je filozofska disciplina ali panoga, ki se ukvarja s tematiko človeškega hotenja in ravnanja z vidika dobrega in zlega, moralnega in nemoralnega. Etika je teoretična filozofska refleksija o nravnosti, o pojavih in procesih, ki so moralno relevantni. Glede na dve poglavitni vrsti svojih nalog se deli na dve področji (Sruk, 1986, str. 139):

- teoretična etika (deskriptivna),
- praktična normativna etika.

Če prva pojasnjuje, kaj je moralna sodba, potem druga moralno sodi. Če prva ugotavlja, kaj je moralna opredelitev, druga moralno opredeljuje. Teoretična etika razglablja o pojmu moralni princip, normativna etika pa formulira in pojasnjuje moralna načela. Prva raziskuje, kakšna in kolikšna je vloga karakterja, pobude, namere, cilja, motiva ali ravnanja človeka pri nravstvenem presojanju, medtem ko druga določa, kakšen je značaj, kakšna pobuda, namera, kakšen je cilj, motiv in katero dejanje je moralno pozitivno ter katero negativno. Teoretična etika je blizu sociologiji, psihologiji, antrolopogiji, preučuje in opisuje ljudi, kulturo in družbo nasploh, primerja in opisuje moralne sisteme, kodekse, prepričanja, principe, vrednosti in navade. Teoretična etika je podlaga za praktično normativno etiko, saj priskrbi osnovni material, na katerega se praktična etika naslanja. Temelj normativne etike je etika zdrave pameti, ki združuje vrednote in načela ljudi v preprosta izkustvena pravila, kot so: ravnaj po zakonih, bodi pravičen, ne laži in ne goljufaj, ne škoduj drugim.

Etična vprašanja so vprašanja o pravilnosti, primernosti in vrednosti dejanj (Fürst in Halmer, 1990, str. 170). Ljudje skušajo pri ocenjevanju dejanj in odločitev doseči soglasje. Potrjevanje različnosti je hkrati tudi iskanje konsenza. Pri tem nastajajo težave, saj ni nujno, da je to, kar je za dva človeka sporazumno pravilno, tudi že dokončna resnica.

Morala je skupek družbenih predpisov, norm, ki so sankcionirane s posebno notranjo sankcijo, katero subjekt, individuum uporablja na sebi samem zaradi kršitev omenjenih predpisov. Morala je toliko bolj učinkovita, kolikor bolj je ponotranjena, kolikor bolj jo oseba posvoji. Neredko se morala spopada z navadami in običaji. Slaba vest lahko privede človeka do obupa, moralnega zloma, neredko do samomora (Sruk, 1986, str. 283-285).

Znanstvena vednost postmoderne (postindustrijske) družbe, kot na primer informatika in kibernetika, temelji na enotnem strojnem jeziku digitalnega koda, ki ukinja sleherno dvoumnost (ambivalentnost) in večpomenskost (polivalentnost). V tej splošni transformaciji narava vednosti ni ostala nespremenjena. Vednost se lahko pretaka po novih kanalih, oziroma sploh stopa vanje, le če spoznanje lahko prevedemo v informacijske količine. Zato se je postavila napoved, da bodo v prihodnosti vse zdajšnje oziroma zgodovinsko opredeljene vrednosti, ki niso prevedljive na ta način, preprosto zanemarili, usmerjenost novih raziskovanj pa se bo podrejala pogoju prevedljivosti v strojni jezik (Fürst in Halmer, 1990, str. 173).

Vednost je zapadla zakonu ponudbe in povpraševanja. S tem postane vednost ena od temeljnih produktivnih sil, mogoče najpomembnejše orožje v konkurenčnem boju za svetovno prevlado. Lahko si predstavljamo, da se bodo nacionalne države v prihodnosti prav tako bojevale za prevlado nad informacijami, kot so se v preteklosti bojevale za prevlado nad ozemlji in potem za to, da so lahko izkoriščale surovine in poceni delovno silo. Na ta način se

odpira novo polje industrijskih, gospodarskih pa tudi vojaških in političnih strategij (Fürst in Halmer, 1990, str. 173).

Ta radikalna preobrazba vednosti v golo sredstvo širjenja strateške moči prinaša tudi nove etične vidike. Etična problematika znanosti in tehnike se kaže v povezavi s tem, da lahko človek vse bolj svobodno razpolaga z neantropomorfnim okoljem, z novimi možnostmi manipulativnih posegov v življenje, tudi v človekovo življenje. Z uvajanjem tehnike, ki jo utemeljuje znanost, so zmožnosti človekovega poseganja na omenjena področja narasle do razsežnosti, ki si jih prej sploh nismo mogli predstavljati (Fürst in Halmer, 1990, str. 174).

Posebno usoden preobrat je povzročila nova tehnika obdelave podatkov. Iz hitrega razvoja mikroelektronike, računalniško vodene organizacije sistemov, vse večje avtomatizacije javnih služb lahko razberemo, da se ti sistemi vedno bolj nagibajo v tehnokracijo, v kateri se birokracija, tehnokracija in elektro(no)kracija spajajo v nadvse učinkovito zvezo, ki v programsko tabelo visoko razvitih industrijskih držav vpisuje zelo realistično oznanilo o skorajšnjem prihodu tehnokratskega »velikega brata« (Fürst in Halmer, 1990, str. 174).

Razvoj računalniške tehnike, elektronske obdelave podatkov in informacij začenja dobesedno proizvajati problem organizacijsko – znanstveno – tehnokratskega celotnega nadzora nad osebami, ki se kaže kot kombiniran zbir njihovih osebnih podatkov. Ogrožanje nedotakljivosti vsega zasebnega ter tajnost podatkov sproža pravno vprašanje varovanja podatkov, predvsem osebnih podatkov, pred njihovim komercialnim in družbenim izrabljanjem. Vprašanje, ki ima seveda tudi znaten etični pomen (Fürst in Halmer, 1990, str. 174).

Možni razlog za naraščajoč pomen etičnosti najdemo tudi pri Lipovcu. V preteklosti je bila kontrola nad ljudmi precej bolj neposredna in ni bilo težko odkriti neetičnega vedenja. Danes so podjetja vse kompleksnejša, kar pomeni, da so lastniki vse bolj prepuščeni na milost in nemilost ravnateljev. Lastniki vse težje vplivajo na ravnatelje in vse težje prepoznavajo neetična dejanja. Etičnost postaja vse pomembnejša, saj bo etično načelo vse bolj nadomeščalo oziroma izpodrivalo prej prevladujoče ekonomsko načelo. Ta prehod ne bo enostaven, potrebno bo veliko časa, da se bo spremenila miselnost vseh ljudi ali vsaj večine ljudi (Lipovec, 1997, str. 15).

4.2. Etični kodeksi

Računalništvo kot veda je bilo presenečenje tako za pravo kot za etiko, pomanjkljivo in neprilagojeno regulacijo so nadomeščala tehnična pravila in odločitve gospodarjev informacijskih sistemov (državna uprava, vojska, korporacije) (Pivec, 2001, str. 2). Tudi očetje svetovnega spleta so bili prepričani, da ga bodo vselej urejali le s tehničnimi pravili, vendar so se problemi neusmiljeno kopičili in postalo je očitno, da jih brez ustreznega normiranja ne bo mogoče razrešiti. Na podlagi konsenza in pod močnim vplivom vodilnih osebnosti so se oblikovali vzorci poklicnega obnašanja, ki so se sčasoma zapisali v obliko

kodeksov. Zanje so se zavzela strokovna združenja, velike korporacije, akademske organizacije, civilno-družbena gibanja, virtualne skupnosti in podobno.

Strokovne organizacije in združenja sprejemajo pravila obnašanja - kodekse etike, s katerimi zavezujejo svoje člane k moralnemu in etičnemu obnašanju, hkrati pa z njimi sporočajo javnosti, da so one in njihovi člani vredni javnega zaupanja in sposobni sami in znotraj svojih organizacij razreševati konflikte, do katerih prihaja pri vsakodnevnem strokovnem delu in predvsem v odnosu do širšega družbenega okolja. Informatika kot stroka pri tem ni nobena izjema (Krisper, 1998, str. 5).

Etični kodeksi so uporabno in priljubljeno sredstvo za zagotavljanje etičnega ravnanja, potrebno pa jih je izvrševati tudi v praksi, sicer ne uresničijo svojega namena. Vsi zaposleni ali vsi člani neke organizacije morajo biti seznanjeni s kodeksom, ga razumeti in poleg tega tudi sprejeti in se začeti obnašati ter odločati v skladu s pravili kodeksa.

Etične kodekse v podjetjih sestavlja mešanica tehničnih, pravnih in moralnih pravil. Podpirali naj bi dobro, koristno, blaginjo in pravico ter prepovedovali slaba, nekoristna in nepravična dejanja. Kodeksi so pomembni, ker seznanjajo ljudi o tem, kaj se od njih pričakuje, dajejo smernice, kako nekaj narediti, odražajo vrednote in s tem spodbujajo zaposlene, poleg tega pa tudi zvišujejo standarde. Kodeks ne sme biti samemu sebi namen.

Slabosti kodeksov so (Donaldson, 1992, str. 55):

- vrednote so lahko izražene preveč splošno, v tem primeru nihče temu ne nasprotuje in hkrati to nikogar ne motivira,
- sama stopnja etičnosti v kodeksih etike je lahko zelo nizka,
- etičnost je prostovoljna, vendar pa tisti, ki ima moč, lahko drugim vsili svojo moralo,
- ni nobenih učinkov, v primeru, da se kodeks ne uveljavi,
- neuveljavljanje pravil povzroči izogibanje.

Moralna vest je glavna sankcija za neetično ravnanje, njena razširjenost in moč pa je odvisna od etičnega prepričevanja, kar je drugo ime za etično izobraževanje (Pivec, 2002, str. 1).

Etični kodeksi informatike imajo običajno nadaljevanje v projektih etičnega izobraževanja informatikov. Cilji takšnega izobraževanja so doseganje moralne senzibilnosti, sposobnost moralne presoje, krepitev moralne motivacije in oblikovanje moralnega značaja.

V zadnjem času je v ospredju etična problematika uporabe svetovnega spleta, o čemer veliko sestavljavcev etičnih kodeksov niti ne razmišlja. Praznino do določene meje rešujejo posebne »etikete« (angl. netiquette) obnašanja na svetovnem spletu.

Neetična ravnanja informatikov imajo bolj ali manj enake korenine kot pri vseh drugih: šibkost volje, moralna tveganja, pomanjkanje prave vizije, pomanjkanje pozitivnih zgledov, neizoblikovana zavest in pomanjkanje etične izobrazbe.

4.2.1. Kodeks etike Slovenskega društva INFORMATIKA

Kodeks etike Slovenskega društva INFORMATIKA je nastal na podlagi etičnega kodeksa ameriškega združenja ACM, ki je v prvi verziji izšel že leta 1972, dopolnjena in razširjena verzija pa leta 1992. Sekcija za razvoj informacijskih sistemov Slovenskega društva INFORMATIKA je ta kodeks izbrala kot podlago za pripravo kodeksa društva. Le-ta je bil sprejet na izrednem občnem zboru 22. aprila 1999 v Portorožu in objavljen v reviji Uporabna informatika. Kodeks sestavlja 24 načel – zahtev, ki se nanašajo na osebno odgovornost informatikov. Kodeks je sestavljen iz štirih poglavij, kjer prvo poglavje izpostavlja splošna moralna vodila, medtem ko se drugo poglavje nanaša na specifična vprašanja strokovne odgovornosti informatikov. Tretje poglavje velja za posameznike, ki imajo vodilne funkcije na delovnih mestih kakor tudi v strokovnih organizacijah, kot je na primer društvo. V četrtem poglavju je zapisana zaveza članov organizacije določilom kodeksa. Zahteve so določene z imenom podpoglavij, ki jim sledijo pojasnila in smernice za uveljavljanje zahtev.

1. Splošna moralna vodila

Kot član društva se zavezujem, da (se) bom:

1.1 prispeval k blaginji družbe in posameznika

To načelo, povezano s kakovostjo življenja vseh ljudi, poudarja obveznost varovanja temeljnih človekovih pravic in spoštovanja raznolikosti vseh kultur. Informatike naj pri njihovem delovanju vodi načelo najmanjših možnih negativnih vplivov računalniških sistemov in rešitev (v nadaljevanju sistemov), predvsem na zdravje in varnost. Pri izgradnji in uporabi sistemov si morajo informatiki prizadevati, da se bodo njihovi izdelki in storitve uporabljali odgovorno in bodo v skladu s potrebami družbe ter brez škodljivih učinkov na zdravje in blaginjo.

Za človekovo blaginjo je razen varnega družbenega okolja pomembno tudi varno naravno okolje. Zato morajo biti informatiki, ki oblikujejo in razvijajo sisteme, pozorni na možno škodo lokalnemu in globalnemu okolju in o tem osveščati tudi druge.

1.2 izogibal škodovanju drugim

Škodovanje pomeni poškodbo ali negativne posledice, kot so izguba informacij ali premoženja, škoda na lastnini ali nezaželeni učinki na okolje. To načelo prepoveduje uporabo računalniške tehnologije na načine, ki škodijo uporabnikom, javnosti, delojemalcem in

delodajalcem. Škodljiva dejanja so tudi namerno uničenje ali prirejanje datotek in programov, ki vodi v pomembno izgubo sredstev ali v tratenje časa in napora, na primer za odpravljanje virusov v programih.

Tudi dobronamerna dejanja, celo tista, ki dosežejo želene cilje, imajo lahko škodljive posledice. V takšnih primerih je odgovorna oseba ali odgovorno osebje dolžno po svojih zmožnostih odstraniti ali ublažiti škodljive posledice. Nenameravani škodi se je mogoče izogibati z upoštevanjem možnih učinkov pri odločitvah v procesu oblikovanja in izvedbe.

Za zmanjšanje možnosti posrednega škodovanja drugim morajo informatiki zmanjševati napake, tako da ravnajo v skladu s splošno sprejetimi standardi za oblikovanje in preizkušanje sistemov. Nadalje je pogosto treba oceniti učinke programov na družbo in s tem predvideti možnosti škodovanja drugim. Če so bile lastnosti sistema napačno predstavljene uporabnikom, sodelavcem ali predstojnikom, je informatik odgovoren za vso nastalo škodo.

V delovnem okolju je informatik dodatno odgovoren za poročanje o možnih nevarnostih v zvezi s sistemi, ki bi lahko povzročile znatno osebno in družbeno škodo. Če njegovi predstojniki ne preprečijo in ublažijo takšne nevarnosti, je treba na to opozoriti in s tem pomagati pri rešitvi problema in zmanjševanju tveganja. Na drugi strani pa je pomanjkljivo in zavajajoče poročanje prav tako škodljivo. Pred poročanjem o zlorabi morajo biti vse razsežnosti incidenta natančno ocenjene. Še posebej verodostojni morata biti oceni tveganja in odgovornosti. Priporočljivo je poiskati nasvet pri drugih informatikih.

1.3 pošten in vreden zaupanja

Poštenost je bistvena sestavina zaupanja. Brez zaupanja organizacija ne more učinkovito delovati. Pošten informatik nikoli ne ocenjuje sistema ali njegove zasnove namerno napačno ali zavajajoče, temveč v celoti prikazuje in opozarja na njegove omejitve in probleme.

Informatik mora biti pošten glede svojih strokovnih kvalifikacij in glede vseh okoliščin, ki bi lahko povzročile konflikt interesov.

Članstvo v prostovoljnih organizacijah, kot je društvo, lahko posameznika včasih pripelje v položaj, v katerem se njegove izjave in dejanja interpretirajo v imenu večje skupine strokovnjakov. Član društva mora skrbeti, da društva, njegovih stališč in politike ali društev, s katerimi je povezano, ne predstavlja v slabi luči.

1.4 pravičen in se izogibal razlikovanja

Pri tej zahtevi gre za vrednote, kot so: enakost, toleranca, spoštovanje drugih in načelo enakopravnosti. Razlikovanje, ki temelji na rasi, spolu, veri, starosti, invalidnosti, nacionalnosti ali podobnih dejavnikih, je groba kršitev načel društva in ni sprejemljivo.

Razlikovanje med različnimi skupinami ljudi lahko vodi v zlorabo informacij in tehnologije. V pravični družbi morajo imeti vsi posamezniki enake možnosti sodelovati in pridobivati koristi z uporabo računalnikov, ne glede na raso, spol, vero, starost, invalidnost, nacionalnost ali podobne dejavnike. Ti ideali pa ne upravičujejo nepooblaščene uporabe računalnikov in ne upravičujejo katerekoli kršitve drugih etični zahtev iz tega kodeksa.

1.5 spoštoval lastniške pravice, avtorske pravice in patente

Kršitve avtorskih pravic, patentov, poslovnih skrivnosti in licenčnih dogovorov so za informatika nesprejemljivo vedenje. Kopije programske opreme so možne le na podlagi ustreznega pooblastila. Nepooblaščeno kopiranje gradiva ni dopustno.

1.6 spoštoval intelektualno lastnino

Informatiki so obvezani varovati celovitost intelektualne lastnine. Prepovedano si je pripisovati tuje ideje, tudi če niso izrecno zavarovane z avtorskimi pravicami, patentom in podobno.

1.7 spoštoval zasebnost drugih

Računalniška in komunikacijska tehnologija omogočata zbiranje in izmenjavo informacij v obsegu kot še nikoli v zgodovini. S tem je tudi povečana možnost za ogrožanje zasebnosti posameznika in skupin. Odgovornost informatikov je skrbeti za varovanje zasebnosti in celovitosti podatkov. To zajema varnostne ukrepe, ki zagotavljajo točnost podatkov in jih varujejo pred nepooblaščenim dostopom ali naključnim razkritjem nepooblaščenim posameznikom. Nadalje, posameznikom mora biti zagotovljen dostop do njihovih podatkov in popravkov, če niso pravilni.

Po tej zahtevi sistem naj vsebuje le tisto količino osebnih podatkov, ki je nujna, da sta njihovo hranjenje in uporaba jasno določena in zagotovljena, in se osebni podatki, zbrani za specifičen namen, lahko uporabljajo v druge namene samo s privolitvijo posameznika. Ta načela veljajo za elektronske komunikacije in tudi elektronsko pošto in prepovedujejo postopke, v katerih se uporabljajo ali opazujejo podatki uporabnikov ali njihova sporočila, brez dovoljenja uporabnikov ali bona fide pooblastila za vzdrževanje sistema. Podatki uporabnikov se morajo pri vzdrževanju sistema obravnavati z najstrožjo zaupnostjo, razen v primerih, v katerih je dokazana kršitev zakonov, organizacijskih predpisov ali tega kodeksa. V teh primerih morata biti narava in vsebina teh informacij predstavljena pristojnim organom.

1.8 spoštoval zaupnost

Načelo poštenosti se nanaša na zaupnost, kadarkoli je ta izrecno zahtevana. To velja tudi, če ta ni izrecno zahtevana, v primeru, da ima posameznik dostop do osebnih podatkov, ki neposredno ne zadevajo opravljanja njegovih nalog. Etično je spoštovanje vseh obvez zaupnosti do uporabnikov, strank in zaposlenih, razen v primerih, ko je s predpisi ali s tem kodeksom drugače določeno.

2. Posebne strokovne odgovornosti

Kot član društva se zavezujem, da (si) bom...

2.1 prizadeval doseči najvišjo kakovost dela in izdelkov

Prizadevanje za odličnost je najpomembnejša obveznost informatika. Informatik si mora prizadevati za kakovost. Računati mora z možnimi znatnimi posledicami slabe kakovosti aplikacij.

2.2 pridobil in vzdrževal visoko raven strokovnega znanja

Odličnost je odvisna od posameznikov, ki si prizadevajo pridobiti in vzdrževati strokovno znanje. Informatik se mora uveljavljati pri ustvarjanju meril za primerno raven znanja in si prizadevati, da bodo ta merila dosežena. Izboljšanje strokovnega znanja se lahko doseže z neodvisnimi raziskavami, z udeležbo na seminarjih, posvetovanjih in tečajih in s članstvom v strokovnih organizacijah.

2.3 poznal in spoštoval obstoječe predpise, ki se nanašajo na strokovno delo

Člani društva se morajo podrejati lokalnim, državnim, regionalnim in mednarodnim predpisom, razen v primerih, ko gre za dejanja v nasprotju z etiko. Prav tako so dolžni spoštovati usmeritve in pravila organizacij, v katerih so zaposleni oziroma včlanjeni. Kršitev predpisov je lahko etična, če je zakon ali pravilo v nasprotju z moralnimi načeli ali če je v nasprotju z drugim zakonom, ki je po presoji pomembnejši. Pri odločitvi za kršitev predpisa zaradi presoje o njegovi neetičnosti ali iz drugega razloga, mora informatik prevzeti polno odgovornost za svoja dejanja in njihove posledice.

2.4 sprejemal in si prizadeval za strokovno oceno

Kakovostno strokovno delo, posebej v informatiki, je odvisno od strokovne ocene in kritike. Kadarkoli je to potrebno, morajo člani zahtevati in omogočati kolegom kritičen vpogled v svoje delo in ga zagotavljati tudi drugim.

2.5 seznanjal zainteresirane z razumljivimi in temeljitimi ocenami aplikacij in njihovih učinkov ter z analizo možnih tveganj

Informatiki si morajo prizadevati za razumljivost, temeljitost in objektivnost ocen, predlogov, opisov in možnih alternativ aplikacij zaposlenim, strankam, uporabnikom in javnosti. Pri ocenjevanju morajo biti tudi pozorni na možne interesne konflikte, kot je zapisano v zahtevi 1.3, in nanje opozarjati.

Kot izhaja iz obrazložitve zahteve 1.2 o izogibanju škodi, mora biti vsaka možna nevarnost, ki izhaja iz sistemov, sporočena tistim dejavnikom, ki so pooblaščeni in odgovorni za rešitev problema (smernice za zahtevo 1.2 za podrobnosti o škodi, vključno z obveščanjem o strokovnih zlorabah).

2.6 spoštoval pogodbe, dogovore in predpisane obveznosti

Spoštovanje sprejete naloge zadeva doslednost in poštenost informatika. To se nanaša tudi na zagotovilo, da bodo elementi sistema delovali v skladu s pričakovanji. Tudi če je posameznik v pogodbenem razmerju z drugo stranko, je njegova odgovornost, da jo obvešča o napredovanju del.

Informatik je tudi odgovoren, da zahteva spremembo katerekoli naloge, za katero meni, da ne more biti izpeljana, kot je načrtovano. Informatik lahko sprejme nalogo le po temeljiti presoji in odkriti predstavitvi tveganj in pomislekov delodajalcu ali stranki. Temeljno načelo je sprejem osebne odgovornosti za strokovno delo. V nekaterih primerih imajo lahko druga etična načela večjo težo.

Zgolj mnenje, da določena naloga ne bi smela biti izpolnjena, ne zadostuje. Po razjasnitvi problemov in pomislekov se lahko zgodi, da se od informatika zahteva, na podlagi zakona ali pogodbe, da nadaljuje delo, kot je bilo predhodno določeno. Etična presoja informatika naj bo odločilna ali z nalogo nadaljuje ali ne. Ne glede na odločitev pa mora prevzeti odgovornost za posledice.

Izpolnitev nalog proti njegovi presoji informatika ne oprosti odgovornosti za možne negativne posledice.

2.7 pospeševal razumevanje informatike in njenih posledic v javnosti

Informatiki so odgovorni, da posredujejo svoje strokovno znanje javnosti in spodbujajo razumevanje informatike, vplivov računalniških sistemov - aplikacij in njihovih omejitev. Ta zahteva se nanaša na obveznost informatika, da se zoperstavi napačnim pogledom na informatiko.

2.8 uporabljal računalniško in komunikacijsko opremo le, če bom za to pooblaščen

Kraja ali uničevanje fizične in elektronske lastnine je prepovedana z načelom 1.2 - "Izogibaj se škodovanju drugim." Ta zahteva se nanaša na vdor in nepooblaščeno uporabo računalniških in komunikacijskih sistemov. Vdor pomeni vstop v komunikacijske mreže in računalniške sisteme ali račune in datoteke, ki so z njimi povezani, brez izrecnega dovoljenja. Vedno je potrebno dovoljenje za uporabo sistemov, to je tudi za komunikacijska vrata, pomnilne enote, druge vhodno izhodne enote in računalniški čas.

3. Zahteve za vodenje in organiziranje

Kot član društva in vodja - organizator bom:

3.1 zagotavljal družbeno odgovornost članov organizacijske enote in spodbujal popolno sprejemanje te odgovornosti

Ker organizacije vseh vrst vplivajo na javnost, morajo tudi sprejemati družbeno odgovornost. Dejanja organizacije in njeno obnašanje, ki upošteva kakovost in blaginjo družbe, zmanjšujejo možno javno škodo in s tem služijo javnemu interesu in izpolnjevanju družbene odgovornosti. Vodje organizacij naj spodbujajo družbeno odgovorno ravnanje in si prizadevajo za kakovost dela oziroma delovnih pogojev.

3.2 upravljal z osebjem in sredstvi za načrtovanje in izdelavo aplikacij, ki povečujejo kakovost, učinkovitost in dostojanstvo dela

Vodje organizacij so dolžni, da z aplikacijami povečujejo kakovost dela in je ne zmanjšujejo. Pri uvajanju aplikacij naj organizacije upoštevajo osebnostni in strokovni razvoj, fizično varnost in osebno dostojanstvo vseh zaposlenih. Pri načrtovanju aplikacij in na delovnem mestu je treba zagotoviti primerno raven ergonomskih standardov na relaciji človek - računalnik.

3.3 upošteval in podpiral pravilno in pooblaščeno uporabo računalniške in komunikacijske opreme v organizaciji

Ker lahko računalniške rešitve postanejo orodje za povzročanje škode ali koristi organizaciji, je vodstvo odgovorno za jasno opredelitev tako primerne kot tudi neprimerne uporabe računalniške opreme. Obseg teh pravil naj bo čim manjši, vendar naj bodo strogo in v celoti spoštovana.

3.4 zagotavljal, da bodo potrebe uporabnikov in tistih, na katere rešitve vplivajo, upoštevane pri vrednotenju in načrtovanju uporabniških zahtev

Sedanji in potencialni uporabniki rešitev in druge osebe, na katere te rešitve lahko vplivajo, so upravičeni, da se njihove potrebe ovrednotijo in upoštevajo. V nadaljevanju naj bo opravljena tudi presoja ustreznosti rešitve opredeljenim zahtevam.

3.5 izvajal in podpiral ravnanje, ki varuje dostojanstvo uporabnikov in drugih, na katere rešitve vplivajo

Načrtovanje in uvajanje rešitev, ki namerno ali nenamerno ponižujejo posameznike in skupine, je etično nesprejemljivo. Informatiki, ki so na vodilnih položajih, morajo preverjati, ali so rešitve načrtovane in uvedene tako, da varujejo zasebnost in osebno dostojanstvo.

3.6 ustvarjal pogoje za izobraževanje članov organizacije o načelih in omejitvah računalniških rešitev

Ta zahteva se navezuje na zahtevo 2.7. Ustvarjanje pogojev za izobraževanje je bistveno za zagotavljanje optimalne participacije vseh članov organizacije. Vsem članom organizacije mora biti zagotovljena možnost za izboljšanje strokovnih znanj in za seznanjanje s posledicami in z omejitvami posameznih delov rešitev. Še posebej se morajo strokovnjaki zavedati nevarnosti razvoja rešitev na poenostavljenih modelih, pri čemer ni možno vnaprej predvideti vse pogoje, ki bi lahko nastopili pri njihovem delovanju in drugih vprašanj, ki se nanašajo na kompleksnost njihovega poklica.

4. Privolitev v kodeks

Kot član društva bom:

4.1 sledil in opozarjal na načela tega kodeksa

Prihodnost poklica informatika je odvisna tako od strokovne kot tudi etične odličnosti. Za informatike ni zgolj pomembno, da se držijo pravil tega kodeksa, temveč da pri tem vzpodbujajo in podpirajo tudi druge člane.

4.2 razumel kršitve tega kodeksa kot nezdružljive s članstvom v društvu

Spoštovanje tega kodeksa je v pretežni meri prostovoljno. V primeru, da član z grobimi kršitvami njegovih pravil ne spoštuje kodeksa, bo izključen iz društva.

Kodeks etike (Krisper, 1998, str. 10) naj bo predvsem vodilo za etično sprejemanje odločitev in za spodbujanje odgovornosti članov organizacije. Družbena odgovornost informatikov je še posebej izpostavljena zaradi izrednega razvoja informacijske in telekomunikacijske tehnologije in njune vseprisotnosti na vseh področjih dela in življenja. Sprejem kodeksa in

oblikovanje zavesti o spoštovanju njegovih pravil je pomembno tudi za javno podobo in uveljavitev strokovnega združenja, kot je Slovensko društvo INFORMATIKA.

Po Pivcu (2002) v etičnem kodeksu manjkajo opredelitve do arbitrarnega izbora etičnih žarišč:

- ženske med informatiki,
- vpliv virtualnih skupnosti,
- marginalci v informacijski družbi,
- enklave informatikov in socialna solidarnost,
- zaščita otroštva v elektronskih komunikacijah,
- posledice biometrične identifikacije,
- upravljanje medicinske informatike,
- nove oblike politične reprezentacije na podlagi informacijsko telekomunikacijskih tehnologij,
- monopolizacija organizacije znanja,
- piratstvo programske opreme,
- tehnologije elektronskega nadzorovanja,
- svoboda govora na spletu,
- etika iskalnikov,
- etika podatkovnega rudarjenja (angl. data mining),
- etika vmesnikov,
- etika elektronskega dopisovanja (nezaželena pošta,..),
- računalniški kriminal,
- kibernetični (angl. cyber) kriminal.

Za vsa ta področja velja, da teh etičnih problemov brez delovanja informatikov sploh ne bi bilo, da so jih oni ustvarili ali najmanj soustvarili. Rutinska poklicna etika za ta področja nima posluha in tudi ne normira etičnih ravnanj informatikov v zvezi z njimi.

4.3. Poslovna etika in varnost informacijskih sistemov

Zadnja leta so se v okviru splošne etike začele razvijati tudi posebne etike, ki uveljavljajo splošno etiko na posebna področja – raziskujejo moralo na specializiranih področjih človeškega delovanja. Tako so se razvile mnoge etike, med njimi tudi poslovna etika. Poslovna etika raziskuje razmerja med dobrim in slabim v poslovanju. Ljudje v poslovnem svetu morajo upoštevati ista etična načela kot vsi drugi. Poslovna etika je sistematična uporaba vrednot v poslovanju podjetja (Donaldson, 1992, str. 2).

Poslovna etika odraža navade in presoje ravnateljev, ki zadevajo tako njihovo delo kot delo drugih v nekem podjetju. Temu delu in presojam je podlaga posameznikov sistem moralnih

vrednot, ki je pogosto prisiljen ali vsaj v skušnjavi, da bi spremenil prioriteto svojih vrednot, ko se sooča s kontekstom delovanja, kjer so v ospredju pritiski mnogih institucij, poslovnih izidov in včasih enostavno pritiski, povezani z doseganjem in ohranjanjem moči (Nash, 1990, str. 5).

Poslovna etika lahko pomaga reševati moralne probleme v poslovanju bolj sistematično. Omogoča boljši vpogled v same vzroke problemov, ki jih drugače sploh ne bi zaznali in posledično vpeljevanje samih izboljšav. Potrebno se je zavedati, da sama etika ne bo nikogar naredila etičnega. Poslovna etika predpostavlja, da tisti, ki se vanjo poglablja, lahko postane oziroma je že moralen in zna presoditi, kaj je prav in kaj narobe. Poslovna etika ne more prisiliti poslovneža v neko aktivnost, ki je označena kot dobra, če on sam ne čuti želje ali potrebe po njej.

Etično ozaveščanje zaposlenih na vseh ravneh in v vseh delih je nujen predpogoj za zviševanje ravni v morali delovanja organizacije. Pri tem pomaga vrsta ciljnih dejavnosti, kot so razne prireditve, nastopi, ki izpričujejo etično naravnanost organizacije ter vidno nagrajujejo posameznike in skupine, ki se vedejo po njej. Najpomembnejše pri uvajanju in dojemanju etičnosti ima izobraževanje, poleg tega pa še naslednji prijemi (Tavčar, 1994, str. 161):

- soočanje z zadevami, ki terjajo etično presojanje in moralno ravnanje, ne pa prikrivanje in odkrivanje teh zadev,
- spodbujanje komuniciranja o etičnih zadevah, ki temelji na dejstvih in enakopravnosti,
- vključevanje ravnateljev z nižjih ravni ter sodelavcev nasploh v procese etičnega odločanja v organizaciji,
- zavzemanja za čim trdnejše in stalnejše vrednote ravnateljev in drugih sodelavcev, ki uživajo v organizaciji posebno avtoriteto,
- sprotno seznanjanje s posledicami neetičnih odločitev in ravnanja za organizacijo ter širše okolje,
- vpletanje sodelavcev v področja, ki zlasti terjajo etično presojanje,
- zaupanje odgovornosti in pristojnosti za etično presojanje v skladu s sposobnostmi in stopnjo osebnega razvoja.

Na izpolnjevanje etičnih standardov vpliva tudi sama struktura organizacije. Čeprav je struktura organizacije praviloma posledica vsebine, pa primerna urejenost bistveno vpliva na izboljševanje etičnosti. Tu je mišljena predvsem jasnost postopkov, poti, pristojnosti, odgovornosti, urejenosti, jasna opredelitev vodstva in podobno. V proces presojanja zadev je potrebno vključiti kar najširši krog sodelavcev z vseh ravni organizacije.

Ne glede na to, kako sofisticiran je informacijski sistem, se morajo organizacije na določeni točki zanesti le na človeška bitja (Wood, 1997, str. 79). Ljudje namestijo operacijski sistem, izberejo začetno geslo, periodično menjujejo kriptirne ključe in izvajajo druga opravila v povezavi z informacijsko varnostjo. Naj se informatiki v podjetjih še tako trudijo, da izbirajo varna gesla in jih posredujejo po varni poti do končnih uporabnikov, še vedno imajo nekateri uporabniki na monitorjih ali stenah nalepljene lističe z raznimi gesli za dostop do elektronske banke, za prijavo v lokalno omrežje ali druge zaupne storitve. Želja zaposlenih je, da bi nemoteno opravljali svoje delo in se pri vsem tem čim manj ukvarjali z varnostjo. V tovrstnih primerih tradicionalne varnostne zaščite odpovejo in le dobro načrtovana, celovita in dokumentirana varnostna politika lahko vaj deloma prepreči veliko škodo.

4.4. Varnost informacijskih sistemov in etika v Sloveniji

V Sloveniji je malo znanih objavljenih primerov vdorov v informacijske sisteme podjetij. Podjetja prav tako ne poročajo javno o okužbah z virusi, o izgubah podatkov, o škodi, ki so jo utrpela zaradi kakršnihkoli zlih namenov ali kriminalnih dejanj tretjih oseb ali zaradi lastne neprevidnosti in malomarnosti. Večina zlorab ostane skrita pred mediji in javnostjo. Informacije o okužbah ali drugih težavah pricurljajo v javnost nenamenoma, preko zaposlenih, ki vede ali nevede posredujejo podatke novinarjem, lahko pa tudi kolegom, ki nato ne znajo držati jezika za zobmi. To izkušnjo sem tudi sam doživel, v mesecu decembru 2006, ko so bile priprave na evro na vrhuncu. Med prijaznim klepetom ob kavi mi je zunanji sodelavec, sistemski inženir, omenil, kako je »ena izmed slovenskih bank zaradi pomote namesto v testnem okolju začela z evrokonverzijo na produkcijskem okolju. Še pred koncem so napako odkrili in povrnili celoten sistem v stanje pred konverzijo«. Ne glede na to, ali je bila zgornja izjava resnična ali neresnična, prikrojena ali zelo napihnjena, v nobenem primeru ni od zunanjega partnerja primerno, dopustno in etično, da jo posreduje katerikoli tretji osebi. Na srečo informacija ni prišla v javnost, saj bi to pomenilo omadeževan ugled banke, tudi če bi se izkazalo, da gre le za neslano šalo v najbolj neprimernem trenutku, objava v medijih bi lahko kompromitirala ali postavila v dvom celoten slovenski uspeh prehoda.

Svoje razmišljanje brez ustrezne strokovne podlage oziroma literature razvijam v naslednji smeri: Zakaj smo v Sloveniji prepričani, da smo varni pred hekerji, da hekerjev v Sloveniji ni oziroma jih je zelo malo, da jih naše organizacije ne zanimajo? Ta vprašanja bi lahko enačili s vprašanji, ali in kako je razvit kriminal na splošno v Sloveniji, ali se dogajajo veliki, spektakularni bančni ropi! Že samo bežen pogled v dnevno kroniko pove, da je kriminala v Sloveniji ogromno, vsakodnevno se dogajajo oboroženi vlomi, kraje vseh vrst, malverzacije, prekupčevanja, prevare. Eden večjih primerov v zadnjem obdobju je rop trezorja SKB banke. Kako si lahko podjetja pri vsem tem slepijo oči, da so varna pred domačimi hekerji, ker da jih ni, tujih pa ne zanimajo!? V Sloveniji obstaja ogromno znanja, ki ga lahko zlonamerneži izkoristijo za svoje nepoštene namene. Sicer pa lahko vsak, ki je malo bolj vešč, poišče to znanje na svetovnem spletu, kjer obstajajo posebne strani s tovrstno škodljivo vsebino, uporabnikom že kar prijazni programi z zlonamerno kodo. Tudi tečaji, seminarji ali detajlnejši

članki v specializiranih revijah, ki so sicer namenjeni izobraževanju ljudi, ki skrbijo za varnost v podjetjih, so izvrsten vir sredstev in navodil, kako izvesti napad, kako zakriti sledi in podobno. Vsako tovrstno znanje se lahko izkoristi za zle namene. Informatiki pa so že po naravi ljudje, ki jih zanima raziskovanje, vedno iščejo kaj novega, priložnost pa naredi človeka tatu. Eden izmed konkretnih primerov sta članka Napadi na omrežja WLAN in Vdori v brezžično omrežje avtorja Tomaža Bratuše v peti številki revije Moj Mikro, letnik 2006, kjer avtor z vso natančnostjo opiše postopek, orodja, celo ukazi so podrobno prikazani, kako lahko praktično vsak, ki dobi v roke revijo in ima računalnik ter brezžični dostop do svetovnega spleta, vdre v neko drugo pomanjkljivo zaščiteno omrežje, strežnik ali računalnik. Avtor obenem celo podaja nasvete, kako ravnati v določenih primerih, podaja in komentira možne situacije in odzive ter svetuje, kako uporabljati zvijače.

Vsakega vodjo informatike zanima, kako varna so uporabniška gesla, ki jih uporabljajo zaposleni v podjetju. Na raznih seminarjih o informacijskih varnostih kar naravnost povedo, kje na svetovnem spletu se nahajajo ustrezni programi za prestrezanje gesel, sicer pa je do teh programov enostavno priti tudi že samo s poizvedovanjem po svetovnem spletu. Če vodja informatike na ta način pride do gesel uporabnikov, lahko seveda ukrepa ali pa gesla izkoristi, na primer za branje elektronske pošte drugih uporabnikov, kar je ena milejših oblik zlorabe. Kaj pa v primeru, da tak ali podoben program požene na svojem računalniku drug zaposleni, študent, praktično vsakdo, ki ima dostop do svetovnega spleta? Ali če ta raziskovalec prinese zlonamerno kodo kar s sabo (od doma) na USB ključu ali drugem prenosnem mediju?

Ali sploh obstajajo in kakšni so načini, da podjetje odkrije hekerja, ki si je to podjetje izbral za žrtev? Po katerih diskih se je heker sprehajal, katere identitete je prevzemal, kateri podatki so šli z njim in v kakšni obliki? Morda si je nadel digitalno identiteto tajnice direktorja podjetja in nabiral strateške skrivnosti. Zelo verjetno je skušal skočiti v čevlje upravitelja in izkoristiti njegove pravice do glavnega računalnika in zbirke podatkov podjetja. Je poskusil pisati po bazi? Podjetje niti ne ve, koliko časa ga oskrbuje z informacijami in kako ji je/bo izkoristil. Seveda pravi heker ne bo pustil nobene informacije v dnevniških zapisih. Če podjetje ni popolnoma in sistematsko namestilo vseh sistemov na novo, je potuhnjeni slepi potnik zelo verjetno še vedno v sistemu podjetja. Kako podjetje ve, da vsi super varnostni mehanizmi delujejo, da ni nekdo podkupil vratarja ali celo upravljavca, skrbnika uporabniških računov? Izdelovalci vseh varnostnih rešitev jamčijo, da njihova oprema res zagotavlja visok nivo varnosti. Ponudniki varnostnih rešitev povedo, da so namestili in testirali opremo na (naključna številka) mestih in da deluje. Tudi visoka cena govori v prid rešitve, da jo veliko podjetij uporablja, predvsem pa konkurenčna podjetja, zato je priporočljivo, da jo kupi tudi podjetje!

Je za vse nas res tako dobro, da smo v varnost svojih kreditnih kartic tako popolnoma prepričani? Ljudje verjamemo javnim floskulam, da je vse super varno, da se ni treba bati za svoje kartice, v najslabšem primeru škodo tako ali tako povrne zavarovalnica. Ali ni mogoče,

da bodo kar naenkrat »ušle« zdravstvene kartoteke, digitalni zapisi biometričnih podatkov za potne liste, nekdo se bo lahko poigral s številkami v pokojninski bazi,…?

Zakaj je potrebna etika za strokovnjake s področja informacijskih tehnologij? Dajanje moči posamezniku (skupini) ima vedno za posledico etična vprašanja: *Če želiš spoznati pravi obraz posameznika, mu daj moč*. Moč strokovnjakov informacijskih tehnologij je v dobrem poznavanju poslovnih procesov podjetja, za katerega razvijajo informacijske rešitve, v dobrem poznavanju varnostnih mehanizmov informacijskih sistemov ter v dostopu do zaupnih informacij v znanju ali vlogi v produkciji ali distribuciji informacij.

Vsa podjetja, ki imajo svoj informacijski sistem, imajo običajno tudi svojega administratorja (skrbnika računov). Ti imajo praktično brezmejen dostop do vseh informacij, vsaj do tistih, ki se zbirajo, obdelujejo in ustvarjajo s pomočjo informacijske tehnologije, v vseh fazah njihovega življenjskega ciklusa (Panian, 2001, str. 84–85). Na ta način imajo administratorji veliko strateško prednost pred ostalimi zaposlenimi v podjetju (informacija pomeni moč). Administratorji bi morali te svoje privilegije uporabljati v dobrobit celega podjetja in vseh zaposlenih, vendar takšen položaj lahko povzroči tudi izziv, ki lahko labilne osebe spravi v skušnjavo, da ga izkoristijo v zle namere.

Mogoče najboljši način kontrole podjetja nad administratorji (Panian, 2001, str. 87) je pozicioniranje njegove funkcije v podjetju dovolj visoko v upravljavski hierarhiji ter angažiranje kompetentnih in zaupanja vrednih ljudi za opravljanje tovrstnih del in nalog. Če so to notranji strokovnjaki z dobrimi delovnimi navadami, je izpostavljenost riziku, da administrator prekorači svoja pooblastila, zmanjšana. V primeru, da so angažirani zunanji strokovnjaki, jih je pred delom potrebno preveriti s standardnimi načini pregleda delovne preteklosti in osebnega življenja ter z njimi opraviti ustrezne razgovore (Hunton, 2004, str. 99-103).

Poleg administratorjev informacijskih sistemov imajo med zaposlenimi tovrstne pravice tudi vodje informatike (CIO), inženirji informacijske varnosti (angl. Information Security Manager), administratorji baz podatkov (angl. Database Administrator), administratorji požarnih zidov in usmerjevalnikov (angl. Firewall Administrator) (Peltier, 2002, str. 255 – 260), pa tudi revizorji varnosti (Egan, 2005, str. 77). Vsak posebej je po svoje odgovoren za svoje delo, obenem pa po etični plati ne sme izkoriščati možnosti raznih dostopov, ki jih ostali zaposleni nimajo. Kot primer navajam dostop do sistemskih struktur in datotek, kjer ima računovodski oddelek shranjene podatke o zaposlenih in njihovih plačah. Neomejen dostop do teh datotek lahko imajo vsi administratorji, predvsem iz varnostnih razlogov, na primer za obnove podatkov in podobno (angl. restore), vendar zaradi dovolj visokih etičnih norm teh informacij administratorji običajno ne pregledujejo, če pa jih že zaradi narave dela dobijo na vpogled, jih obdržijo zase. Podoben primer je možnost vpogleda v osebne račune bančnih komitentov, v zavarovalne police zavarovalcev in podobno. V primeru nezakonitega

posredovanja teh informacij in podatkov nepooblaščenim ali tretjim osebam se takšna dejanja smatrajo kot kazniva dejanja, delodajalec pa ima pravico takšnega delavca odpustiti z dela.

4.5. Etični heking, etični hekerji

Etični heker je računalniški in omrežni strokovnjak, ki izvaja napad na računalniški sistem na podlagi zahteve lastnika tega sistema. Pri tem išče pomanjkljivosti, ki bi jih zlonamerni heker lahko izkoristil (Žnidar, 2006, str. 18). Za preverjanje varnosti sistema uporablja etični heker iste metode kot pravi heker, vendar ugotovitve ne izkoristi v zli namen, temveč jo napiše v poročilo in ga preda le naročniku. Rezultat storitve je pregled stanja računalniških sistemov in omrežja ter njihove varnostne šibke točke. Etični heking je znan tudi pod imenom »red teaming«. Beseda izhaja iz ZDA, kjer so vojaške ranljivosti iskali tako, da so nasproti »dobrim fantom« modre ekipe postavili »slabe fante« v rdeči ekipi, ki so poskušali odkriti ranljivosti in slabosti modre ekipe. V povezavi s hekerji se uporabljata še dve oznaki, »white hat« in black hat«, prihajata pa iz vesternov, kjer so dobri fantje običajno nosili bele klobuke, slabi pa črne.

Poznamo različne vrste preverjanja varnosti informacijskih sistemov. Vsi analizirajo različne vidike informacijskega sistema in se v grobem ločijo po količini vloženega časa in denarja. Etični heking predstavlja v tem okviru eno vrsto preverjanja, ki jo zamenjujemo z dvema drugima storitvama. Preverjanje ranljivosti (angl. vulnerability scanning) pomeni avtomatsko preverjanje znanih ranljivosti v omrežju. Gre za kratke in razmeroma poceni teste, ki so namenjeni le hitremu preverjanju bolj znanih ranljivosti. Penetracijski test (angl. penetration test) se ukvarja z varnostnim preverjanjem le enega sistema ali naprave z glavnim ciljem pridobiti privilegiran dostop do sistema.

Metodologija, ki jo uporabljajo etični hekerji, je v osnovi podobna napadom, ki jih izvajajo hekerji:

- *Analiza okolja* (angl. Reconnaissance). Napadalec si z nabiranjem podatkov o ciljnih sistemih pridobi informacije za pripravo napada, kot so načrt omrežja, seznam sistemov, delujoči servisi in njihove slabosti, pregled portov in podobno.
- *Preiskovanje in napad* (angl. Probe and Attack). Na podlagi prej odkritih slabosti in ranljivosti heker preveri možnosti izkoriščanja ranljivosti za vstop v sistem. V tej fazi preveri vse možne ranljivosti, ugiba ali razbija gesla, išče slabo napisane aplikacije, pozabljene upravljavske datoteke, rezervne kopije in podobno.
- *Noga med vrati* (angl. Gaining a toehold). Napadalec odkrite ranljivosti uporabi za pridobivanje dostopa v sistem. Nepooblaščeno poskuša zagnati program, spremeniti datoteko, prestreči komunikacijo in podobno, da bi dobil dostop do napadanega sistema.
- *Napredovanje* (angl. Advancement). Če napadalcu uspe dobiti nepriviligiran dostop do sistema, poskuša v tem koraku napredovati v privilegiranega uporabnika.

- *Faza prikrivanja* (angl. Stealth phase). Skrivanje sledov pomeni, da heker poskuša zakriti vse sledove, ki bi upravljavcu sistema vzbudili sum vdora, briše sistemske in druge dnevnike, briše in skriva napadalna orodja, poskuša pretentati upravljavska in nadzorna orodja. Pri storitvi etičnega hekinga se ta faza običajno ne izvaja, oziroma etični heker celo pusti sledi kot dokaz vdora.
- *Prisluškovalna faza* (angl. Listening phase). Heker poskuša priti do koristnih informacij za napad z uporabo prisluškovanja komunikacijski povezavi, zaslonu, tipkovnici ali sistemskim datotekam.
- *Prevzem* (angl. Takeover). V primeru prevzema enega sistema poskuša heker razširiti dostop še do drugih sistemov v omrežju. Velikokrat se zgodi, da je dostop do prvega sistema dobro varovan (na primer s požarno pregrado), dostop med posameznimi sistemi za požarno pregrado pa manj.
- *Čiščenje* (angl. Cleanup).

Osnovna delitev storitve etičnega hekinga obsega izvajanje *zunanjega (spletnega)* ali *notranjega (omrežja organizacije) testiranja*. Pri zunanjem gre za preverjanje ranljivosti sistemov, priključenih neposredno na svetovni splet, ki so s tem izpostavljeni celi paleti napadalcev, od vseh vrst hekerjev, prek programov, ki po svetovnem spletu iščejo žrtve, do virusov, črvov in podobno. Testiranje je v teh primerih omejeno s številom zunanjih sistemov in je usmerjeno v intenzivno iskanje vseh mogočih lukenj in razpok v teh sistemih. Pri notranjem testiranju se izvaja preverjanje ranljivosti v notranjem omrežju organizacije, kjer je ranljivost običajno večja. Število sistemov v notranjem omrežju je bistveno večje in varnostne zahteve nižje, zato je testiranje usmerjeno v najbolj izstopajoče ranljivosti, kot so nedovoljeni programi, nenameščeni varnosti popravki, izključeni protivirusni programi. To preverjanje ugotavlja spoštovanje varnostne politike podjetja (na primer prisotnost nedovoljenih programov) in ugotavlja potrebo po njenem dopolnjevanju in popravljanju.

Naročnik si lahko zaželi tudi *slepega testiranja* (angl. blind test). V tem primeru izvajalec testa dobi minimalne podatke, običajno nekaj IP naslovov. V okviru testiranja se lahko izvaja testiranje brezžičnih naprav, možni dostopi do internega omrežja prek njih, način šifriranja, avtentikacije, dostopnost signala zunaj podjetja. Taka vrsta storitve običajno zahteva nekaj več časa.

Poznamo tudi *dvojno slepo testiranje*, ko se poleg slepega testiranja tudi upravitelje sistemov ne obvesti o predvidenem izvajanju testiranja. S takim testiranjem se preverja postopke reagiranja odgovornih v primeru internetnega napada.

Ob običajnih testih so upravitelji sistemov obveščeni o začetku testiranja in lahko do neke mere sodelujejo z izvajalcem pri izmenjavi informacij o tarčah in poteku testiranja.

Testiranje izpada storitve (angl. DoS-Denial of Service) je ena od možnosti storitev, ki se običajno ne izvaja. Izkušnje so namreč pokazale, da je glavni faktor uspeha pri tovrstnih

napadih pasovna širina internetne povezave napadalca, da je napad zlahka uspešen in da se iz njega organizacija ne nauči kaj posebno novega. Dodatno pride v primeru uspešnega napada do onemogočanja storitve, kar ima lahko za posledico izpad poslovanja.

Pred začetkom izvajanja storitve etičnega hekinga mora podjetje - naročnik pripraviti seznam IP naslovov in posebno pooblastilo. Naročnik mora pripraviti seznam IP naslovov, ki jih bo izvajalec testiral, izvajalec pa mora preveriti in potrditi, da naslovi v resnici pripadajo naročniku in da je naročnik pooblaščen za naročanje take storitve. Poleg tega mora naročnik dodatno podpisati posebno pooblastilo za preizkus ranljivosti informacijskega sistema, ki izvajalcu storitve zagotavlja varnost pred, na primer, policijo, če jo varnostni upravitelji obvestijo o ugotovljenem vdoru.

Namen etičnega hekinga je zmanjševanje tveganja, ki ga prinaša uporaba informacijske tehnologije v podjetju. Če podjetje pričakuje, da se na ta način tveganje ne bo zmanjšalo ali da se bo celo povečalo, je bolje, da testiranja sploh ne začne. Podjetje mora razmišljati o zaupanju do izvajalca, etiki udeleženih, delu, varovanju in hranjenju rezultatov ter o zaupnosti informacij, ki se zbirajo ob izvajanju storitve.

4.6. Pravna odgovornost informatikov

Vodja informatike v podjetju bi moral poznati nekatera določila zakonov s področja informacijske družbe (ZEPEP, ZVOP, ZDIJZ, ZVDAGA, ZEKOM, ZASP). V primeru Zakona o varstvu osebnih podatkov bi moral poznati ves zakon, v primeru Zakona o elektronskih komunikacijah pa na primer le člene, ki govorijo o obdelavi podatkov. Slovenska zakonodaja loči med osebnimi in tajnimi podatki, informacijami javnega značaja, poslovno skrivnostjo, statističnimi podatki, davčno tajnostjo, področjem intelektualne lastnine (avtorske pravice za programe, zbirke podatkov, dokumenti, večpredstavnost).

Večina informatikov zagotovo ne pozna dovolj problematike, ki njihovo delo povezuje s pravom, obenem pa o tem področju malo vedo tudi pravniki v podjetjih. Če hoče pravnik pravilno razumeti te stvari, mora biti vsaj malo seznanjen z informacijsko tehnologijo in zbirkami podatkov.

Za pravne kršitve, ki so povezane z informatiko, na primer z varstvom osebnih podatkov, odgovarja odgovorni v podjetju, ki mora biti opredeljen v notranjih aktih podjetja, na primer v Pravilniku o varovanju osebnih podatkov. Če tak odgovorni ni določen, se običajno za odgovornega šteje vodstvo. Tisti, ki je opredeljen v notranjih aktih, je odgovoren tudi za kršitve. Pravno gledano obstaja več vrst odgovornosti, ki urejajo sankcije za delikte v zvezi z obdelavo podatkov (Sušnik, 2006, str. 24). Civilna odgovornost ureja škodo, ki nastane zaradi civilnih kršitev, upravna odgovornost ureja prekrške, v najhujših primerih pa pride v poštev tudi kazenska odgovornost. Z vidika varstva osebnih podatkov je najbolj aktualna upravna odgovornost.

Informatiki v podjetjih bi morali poskrbeti, da bi bili v podjetju sprejeti ustrezni pravilniki, oziroma da bi zaposleni podpisali izjavo o tem, da se strinjajo, da ima podjetje vpogled v razne podatke kot na primer, katere spletne strani je zaposleni obiskal med delovnim časom. Podobno velja tudi za zasebna elektronska sporočila. V tem primeru se pojavi dilema, ali je takšno zasebno elektronsko sporočilo last podjetja.

V nadaljevanju navajam dva člena iz Kazenskega zakonika RS:

Neupravičen vstop v informacijski sistem. 225. člen

(1) Kdor neupravičeno vstopi v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v ali iz informacijskega sistema, se kaznuje z denarno kaznijo.
(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje z zaporom do dveh let.
(3) Poskus dejanja iz prejšnjega odstavka je kazniv.
(4) Če je z dejanjem iz prvega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Vdor v informacijski sistem. 242. člen

(1) Kdor pri gospodarskem poslovanju neupravičeno uporabi, spremeni, preslika, prenaša ali uniči ali v informacijski sistem vnese kakšen svoj podatek, ovira prenos podatkov ali delovanje informacijskega sistema, ali kako drugače vdre v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.
(2) Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je šlo storilcu za to, da sebi ali komu drugemu pridobi tako premoženjsko korist ali drugemu povzroči tako premoženjsko škodo, se kaznuje z zaporom do petih let.

V javnih občilih oziroma črni kroniki izredno redko naletimo na objavljena kriminalna dejanja, ki bi ustrezala zgornjima členoma. Še največkrat je zapisano, da je tat odtujil računalniško opremo, kot so računalniki, zasloni, tiskalniki in podobno, o kraji podatkov ter o vdorih v informacijske sisteme praktično ni objav. Ena od odmevnejših objav (Dnevnik, 10.11.2006) je bil primer zlorabe preko spletne poslovalnice NLB Klik, ko se je oglasil uporabnik NLB Klika, ki so mu nepridipravi z računa pobrali 770.000 SIT. Še največkrat zasledimo objave in svarila pred zlorabami plačilnih kartic. Ali lahko torej predpostavljamo, da spletnega kriminala ni? Ali so informacijski sistemi podjetij in domačih uporabnikov tako dobro zaščiteni, da kriminalci nimajo nobenih možnosti? Tudi na svetovnem spletu je tovrstnih objav malo, uradnih podatkov o spletnem kriminalu in zlorabah v finančnem sektorju v Sloveniji praktično ni. Kot primer oziroma v razmislek navajam izsek iz črne

kronike na VALu 202, z dne 29.10.2007 ob 6:45; avtor Gašper Klarič pove, da so v pretekli noči morali policisti posredovati zaradi 35 tatvin ali vlomov. Moj komentar na to je, da so spletni kriminalci verjetno spali.

5. Varnost informacijskih sistemov in socialni inženiring

Socialni inženiring je proces pridobivanja zaupnih podatkov s pomočjo zvijače. Socialni inženir ponavadi uporabi telefon ali svetovni splet in z zvijačo poskuša prepričati ljudi v posredovanje občutljivih informacij. Pogosto se socialni inženir predstavi kot skrbnik uporabniških računov (administrator) in od uporabnika pridobi geslo za dostop do pomembnih informacij. V resnici administratorji računalniških sistemov ne potrebujejo gesel uporabnikov za ureditev skrbniških, upravljavskih, administrativnih nalog.

Socialni inženiring je umetnost in znanost podrejati ljudi po svojih željah. Socialni inženiring ni eden od načinov nadzora nad človekovo voljo, prav tako se s socialnim inženiringom ne da prisiliti ljudi, da bi izvajali naloge izven njihovega siceršnjega normalnega obnašanja (Brenner, 1997, str. 1). Socialni inženiring je milejši izraz za nekaj, kar bi imenovali varanje, sleparija (Cuadra, 2006).

Socialni inženiring je poskus nepooblaščenega dostopa do kateregakoli sistema ne glede na platformo ali kvaliteto nameščene strojne in programske opreme (Arthurs, 2001). Socialni inženiring obstaja na svetu skoraj že tako dolgo kot človeštvo. Socialni inženirji so poznavalci, ki izrabljajo človeške ranljivosti, kot so ignoranca, naivnost in posameznikova želja, da ugaja in je pripravljen pomagati.

5.1. Problematika socialnega inženiringa

Ko načrtujemo varna računalniška omrežja, običajno pomislimo na tehnično napredne požarne zidove, sisteme za odkrivanje vdorov, sisteme za preverjanje uporabnikov in podobno. Požarni zidovi in drugi varnostni sistemi so pomemben člen v verigi varnega omrežja, ne pa edini. Tehniki pogosto pomislijo samo na tehnične rešitve, prepogosto pa pozabijo na najšibkejši člen v varnostni verigi, na končne uporabnike. Končni uporabniki predstavljajo notranjo nevarnost za omrežje (nevarnost je že za požarnim zidom), zato lahko ta zaščita predstavlja dodatne izzive. Če se vodja informatike te nevarnosti zaveda, se lahko z njo spoprime prek tehničnih rešitev, delno pa je varnost omrežja v rokah uporabnikov, ki so izpostavljeni izkušenim socialnim inženirjem. Ti znajo od uporabnika izvrtati zaupne informacije, na primer gesla. Taki napadi na omrežja so običajno usmerjeni napadi z izbrano, znano tarčo in zastavljenim ciljem. Napadalec skoraj vedno že predhodno naredi tudi »domačo nalogo« o cilju in tarči.

5.2. Kako in zakaj socialni inženiring deluje, različni scenariji in primeri iz prakse

Ljudje smo že v osnovi, v svoji biti, pripravljeni pomagati drugim ljudem, tudi neznancem. Napadalci to izkoriščajo, običajno imajo vnaprej izdelan svoj zviti način za pridobivanje zaupnih informacij. So pa tudi verbalno spretni, imajo pregled nad področjem, kjer bodo izvedli napad, in imajo določeno znanje.

Pridobitev zaupnih informacij od uporabnika zahteva njegovo zmanjšano previdnost, zato poskušajo socialni inženirji izbrati pravi trenutek za napad. Napadajo ob velikih, pomembnih dogodkih, kot je na primer svetovno prvenstvo v nogometu in podobno, ko se zaradi splošne evforije pozornost ljudi običajno lahko precej zmanjša.

Človek je najšibkejši člen v verigi varnostnega informacijskega sistema, ni ga mogoče »skonfigurirati« - prenastaviti, lahko se le izobražuje, z urjenjem se njegovo obnašanje spravi na neko raven, vendar to ne zagotavlja, da bo vedno ravnal ustrezno. Napadalec išče najšibkejši člen, to pa so v podjetjih običajno tisti ljudje, ki imajo stik s strankami. Navodila, ki jih dobijo uslužbenci, so si nasprotujoča: ustreči stranki in z dejanji ne ogroziti varnost.

Osnovne metode socialnega inženiringa so (Granger, 2001, str. 1-7):

- *Socialni inženiring po telefonu* (prevladujoča metoda). Heker se predstavi kot nekdo drugi, lahko imitira nadrejenega ali vodstveno osebo in poskuša pridobiti podatke od podrejenega. K tej metodi so posebej nagnjeni napadi na službe servisne pomoči (angl. Help desks). Zaposleni (velikokrat študentje) so naučeni, da so prijazni, da kličočemu pomagajo, kar je idealno za socialne inženirje.
- *Brskanje po smeteh* (angl. dumpster diving, uporablja se tudi izraz »trashing«). V podjetjih se velika količina informacij znajde med smetmi. Socialni inženir lahko uporabne informacije dobi z vpogledom v telefonske imenike podjetij (izbira tarče, lahko tudi izbira impersoniranega zaposlenega), organizacijske diagrame (pozicija zaposlenih), navodila o načinih varovanja podjetja, koledarje srečanj, dogodkov, dopustov (koledarji so odlični – napadalcu povedo, kdo od zaposlenih je odsoten), sistemska navodila (napadalcu lahko podajo natančen ključ, s katerim je omrežje zaklenjeno), liste občutljivih podatkov ali liste uporabniških imen (ter gesel), vsebino izvorne kode, s pridobitvijo zastarele strojne opreme (diski, trakovi, diskete,…).
- *Svetovni splet* je ogromno področje, kjer lahko socialni inženirji iščejo uporabniška gesla. Osnovna slabost uporabnikov je v tem, da uporabljajo povsod enako geslo, na primer za prijavo v svoj osebni elektronski račun (npr. email.si), za prijavo za delo s spletnim bančništvom (na primer Proklik), za vpogled stanja delnic v skladu, za nakup izdelkov v spletni trgovini (na primer mercator.si), za prijavo v sistem na delovnem mestu in podobno. Ena izmed možnosti je, da socialni inženir pošlje elektronsko sporočilo na določene elektronske naslove,

prejemnikom sporoči, da so dobili neko nagrado, za prevzem nagrade pa je potrebno le izpolniti priložen obrazec, eno izmed vnosnih polj je tudi geslo, ki naj bi veljalo le za komunikacijo med obema strankama. Zelo pogosto se socialni inženirji pretvarjajo, da so skrbniki uporabniških računov v podjetju, serviserji, IT podpora, pomočniki ali svetovalci direktorja, prijatelj ali sošolec zaposlenega.

- *Osnovne vrste prepričevanja* so: izdajati se za nekoga drugega (angl. impersonate), priliznjenost, podobnost (angl. conformity), razprševanje odgovornosti, prijaznost, naklonjenost, tudi flirtanje. Zelo značilno za socialne inženirje je, da nikoli ne vprašujejo po preveč informacijah hkrati, pač pa od vsake osebe, udeležene v napadu, pridobijo po delček, ki ga uporabijo za nadaljnje pridobivanje informacij pri drugi osebi, dokler ne dosežejo svojega cilja, običajno je to geslo.
- V literaturi se pojavlja tudi izraz *obrnjen socialni inženiring*. To je najnaprednejša metoda pridobivanja nezakonitih informacij, sestavljena iz sabotaže, oglaševanja in podpore. Socialni inženir zruši omrežje in s tem povzroči nastajanje težav. Socialni inženir nato oznani, da je on tisti, ki zna ali bo rešil vse probleme; ko pa pride reševat, od zaposlenih pridobi vse informacije, ki jih želi. Zaposleni ali organizacija ne vedo, da je bil pri njih na obisku socialni inženir, njihove težave z mrežo so odpravljene in vsi so srečni.

Scenarij 1 - primer telefonskega pogovora

Socialni inženir pokliče po telefonu uporabnika. Telefonsko številko, ime ter priimek pridobi predhodno na primer na svetovnem spletu. Predstavi se lahko kot oblikovalec ali skrbnik uporabniških računov podjetja, ki je na primer izdelalo spletno stran podjetja (izdelovalec oziroma avtor spletne strani je običajno vedno naveden na domači spletni strani podjetja), torej uporabniku verjetno ni povsem nepoznan. Če napadalec uspe uporabnika prepričati, da sledi njegovim navodilom, lahko kreira nov uporabniški račun na računalniku, s pripadajočim uporabniškim imenom in geslom, ki ga od tistega trenutka naprej pozna tudi napadalec. Če napadalec uspe izvedeti še ime računalnika ter njegov IP naslov, lahko v kratkem času prevzame nadzor nad računalnikom (posebej še, če ima računalnik dostop do svetovnega spleta, od koder socialni inženir nadzoruje in preverja celotno omrežje, nameša svoje programe in podobno.

Najenostavnejša in najučinkovitejša zaščita pred tovrstnim napadom je, da uporabnik ni lokalni skrbnik uporabniških računov na svojem računalniku (nima dovolj pravic, ne more narediti, kar predlaga napadalec). Velikokrat se namreč zgodi, da so uporabniki na svojih računalnikih lokalni skrbniki uporabniških računov. Na ta način lahko povsem sami nameščajo različne programe, verzije, dodatke, ki jih dobijo na svetovnem spletu, sami si lahko dodajajo druge strojne naprave, tiskalnike, optične čitalce in podobno.

Scenarij 2 - primer ankete

Socialni inženir izvede anketo o varnosti uporabniških gesel. V anketi zbira in povprašuje po vseh mogočih informacijah o geslih, kompleksnosti, dolžini, časovnem intervalu menjave, nenazadnje lahko tudi direktno povpraša po geslu. Napadalec lahko izvede anketo v organizaciji, ki si jo je sam vnaprej izbral. Elektronske naslove običajno najde na spletnih straneh organizacije, tudi če so tam objavljena le imena in priimki (običajno struktura podjetij s posameznimi vodji oddelkov ali služb).

Najboljša zaščita pred takimi napadalci so podučeni uporabniki, ki jih je potrebno redno izobraževati in seznanjati z nevarnostmi ter novostmi na področju varovanja informacij.

Tudi sam sem v okviru magistrskega dela izvedel podobno anketo, katere način, potek in rezultate predstavljam v naslednjem poglavju.

Scenarij 3 - neznane osebe

Napadalec si izbere cilj, na primer finančno institucijo. Poslovanje teh institucij ni samo za bančnimi okenci, pač pa glavnina zaposlenih deluje v drugih, ločenih prostorih, kamor lahko imajo dostop tudi nezaposleni. Prva ovira je vratar, ki ga je mogoče prelisičiti na več načinov, lahko že kar filmsko, na način kriminalcev. Napadalčev cilj je poiskati sobo, kjer trenutno za računalnikom ni zaposlenega, računalnik pa ni zaklenjen. Obstaja tudi možnost, da napadalec samo išče možnost, da v računalnik neopaženo vstavi USB ključ z že prej pripravljeno zlonamerno kodo. Napadalec gre od vrat do vrat, od oddelka do oddelka in vedno nekoga išče, v računovodstvu išče prodajni oddelek, v prodajnem oddelku išče računovodstvo in podobno. Lahko se predstavi tudi kot serviser fotokopirnih strojev, tiskalnikov, računalnikov. V primeru, da zaposleni posumijo o njegovi pristnosti, se enostavno začudi in ves zgrožen ugotovi, da ni prišel na pravi naslov in v pravo podjetje ter se prijazno zahvali in poslovi.

Najboljša zaščita pred tovrstnimi napadalci so izobraženi uporabniki.

Scenarij 4 - komunikacijska oprema

Danes ni več pomembno samo, kaj lahko nekdo odnese iz omrežja, pomembno je tudi, kaj se lahko v omrežje prinese. Spreten računalniški zanesenjak, socialni inženir, je lahko zaposlen v servisu nekega računalniškega podjetja. V sklopu popravila lahko na računalnik naloži poljubno zlonamerno programsko kodo (primer program GoToMyPC), ki mu kasneje lahko omogoči popoln nadzor nad računalnikom. Ne poznam primera oziroma organizacije, kjer bi preverjali vsebino računalnikov, ko ti pridejo s servisa.

Obramba pred tovrstnimi napadi je lahko ustrezen filter na aplikacijskem nivoju, ustrezni IPsec filtri, ustrezne uporabniške pravice in požarne pregrade.

Scenarij 5 – uporaba svetovnega spleta in elektronske pošte

Opisal bom primer, kako in kaj je storil socialni inženir julija 2004 za pridobitev uporabniških imen in gesel na spletnem poštnem strežniku www.hotmail.com. Na enem izmed novičarskih blogov je socialni inženir z izmišljenim imenom Manu objavil vsebino, v kateri se je pohvalil, da je on prvi in edini, ki mu je povsem slučajno uspelo odkriti, kako pridobiti geslo za katerikoli uporabniški račun na spletnem naslovu www.hotmail.com. Povedal je, da je to zelo zabavno početje (prijava v tuje uporabniške račune in s tem dostop do vse elektronske pošte kateregakoli uporabnika). Če bi se še kdo hotel tako zabavati, je Manu v nadaljevanju podrobno razložil sicer enostaven postopek. Vse, kar mora novopečeni heker storiti, je to, da mora na elektronski naslov forgotpasswordbot@hotmail.com poslati elektronsko pošto v točno določenem formatu. Najprej ime uporabniškega računa osebe, za katero želi izvedeti geslo, nato besedilo »@hotmail.com«, nato natančno tri vrstice prazne, zatem besedilo »My login: My password«, točno pod tem besedilo pa lastno uporabniško ime in geslo. Manu je poudaril, da je to slednje nujno potrebno, ker na ta način spletni poštni strežnik verificira, da je elektronsko sporočilo o zahtevi za pozabljeno geslo prišlo od verodostojne osebe. Pošiljatelju pošlje elektronsko sporočilo z želenimi podatki, to je »pozabljeno« geslo za uporabniški račun tretje osebe.

Socialni inženir Manu je tako v elektronski poštni predal z imenom » forgotpasswordbot« (ki ga je sam ustvaril in do katerega ima dostop) dobival elektronsko pošto od veliko naivnih ljudi, ki so mislili, da se bodo pošalili ali pogledali prijateljevo elektronsko pošto, v resnici pa so izdali sami sebe (http://www.governmentsecurity.org/arhive/t10264.html).

Kako se braniti pred socialnimi inženirji?

Prva in najpomembnejša zaščita je vsekakor izobraževanje vseh zaposlenih, od pomožnega osebja (čistilke), ki so ravno tako šibki člen v varnostni verigi (imajo ključe in dostop do vseh prostorov, navadno ne poznajo vseh zaposlenih v podjetju, pa tudi če bi jih, se jih navadno ne obvešča, da je nekdo zapustil podjetje), prek referentov, vratarjev, do vodij oddelkov in vodstva. Pomembna zaščita je seznanjanje z možnostmi in trendi. Znanje je potrebno redno osveževati.

Naslednje pravilo je, da se vsi sumljivi dogodki sporočajo na centralno lokacijo, kjer usposobljeni varnostni inženirji presodijo, ali gre za poizkus socialnega inženiringa ali druge oblike kriminala, in ustrezno ukrepajo. Sporočanje sumljivih dogodkov je pomembno, ker obstaja možnost, da socialni inženir ne bo poskusil samo pri enem uporabniku.

Vsaka organizacija bi morala imeti dobro opredeljeno in napisano varnostno politiko, v kateri bi bilo točno določeno, katere informacije se sme posredovati prek telefona, elektronskih sporočil, ustno ali kako drugače. Vsaka varnostna politika mora predvsem določati pravila za menjavo, kompleksnost in na novo določanje (angl. reset) gesla, kako se geslo sporoči

uporabniku, kdaj in kako lahko uporabnik zahteva novo geslo ali reset gesla in podobno. Varnostna politika mora vsebovati določila o prepovedi nameščanja modemov znotraj internega omrežja, ker se na ta način lahko zaobide katerikoli požarni zid ali se pusti odprta vrata. Posebna pravila morajo veljati tudi za službo za pomoč uporabnikom, na primer klicanje uporabnika nazaj zaradi preverjanja lokacije, v primeru komunikacije z elektronsko pošto pa uporaba digitalnih potrdil. Varnostna politika mora vsebovati tudi pravila o fizičnem uničenju vseh občutljivih dokumentov v papirni obliki zaradi možnosti scenarija brskanja po smeteh.

6. Varnost informacijskih sistemov v praksi

V empiričnem delu magistrskega dela sem imel namen izvesti tri ankete in analizirati rezultate:

- ankete med vodji informatike v finančnem sektorju,
- ankete med zaposlenimi v eni finančni instituciji,
- vsesplošne (vseslovenske) ankete med uporabniki naključno pridobljenih elektronskih naslovov.

Zaradi tehtnih razlogov, kot so vprašljiva (ne)legalnost in nejasnosti povezane predvsem s kriminalistično policijo, s katero sem bil v kontaktu, sem s tretjo anketo prekinil že v začetni, pripravljevalni fazi. Podrobnejši opis in rezultate anket predstavljam v nadaljevanju.

6.1. Anketa med vodji informatike v finančnih institucijah

Najprej sem izvedel anketo med vodji informatike v finančnih institucijah.

Raziskava med vodji informatike v slovenskih finančnih institucijah je potekala od julija do septembra 2006. Anketni vprašalnik sem poslal vsem anketirancem po elektronski pošti, poslanih je bilo 55 anketnih vprašalnikov, sestavil sem ga na osnovi namena magistrskega dela. Izpolnjene anketne vprašalnike je po elektronski pošti vrnilo 22 vodij informatike. Podjetja, kamor sem poslal anketne vprašalnike, so bila naključno izbrana, zadostovati pa so morala pogojema, da sodijo med finančne institucije in da sem uspel pridobiti elektronski naslov vodje informatike. V primeru, da nisem uspel pridobiti elektronskega naslova vodje informatike, anketnega vprašalnika nisem poslal. Elektronske naslove vodij informatike sem pridobival prek svetovnega spleta ali pa prek telefonskega kontakta s podjetji, v slednjem primeru žal velikokrat neuspešno. V telefonskem kontaktu sem se predstavljal s pravim imenom in priimkom ter kot študent Ekonomske fakultete v Ljubljani, vedno sem predstavil svoj pravi namen.

Anketni vprašalnik je bil sestavljen iz 30 vprašanj. Večina vprašanj je bila zastavljena z možnimi odgovori tipa »*da - ne*«. Že pri pripravi in oblikovanju vprašanj sem se zavedal visokega tveganja, da v primeru preveč konkretnih ter vsiljivih vprašanj ali vprašanj, katerih odgovori bi lahko pomenili izdajo poslovne skrivnosti ali razkritje določene ranljivosti informacijskega sistema, noben anketiranec ne bi niti odgovarjal, kaj šele, da bi rešen anketni vprašalnik vrnil. Vedel sem, da imajo verjetno vsi anketiranci vsaj enako kot jaz, če ne celo več izkušenj in znanja na področju varovanja informacijskih sistemov, da so to vsi visoko izobraženi ljudje. Poleg tega s(m)o informatiki ljudje posebnega profila, ki se običajno ne želijo izpostavljati, že samo odgovarjanje na tovrstno anketo pa pomeni določeno stopnjo tveganja. Nekatera vprašanja so zatorej ponekod bila bolj splošna, kot bi si jih želel, bila so kratka, pazil sem, da jih ni bilo preveč in da za odgovarjanje anketiranci na vsa vprašanja ne bi porabili več kot 10 minut. Izjemno pomembno se mi je zdelo dejstvo, da sem pri večini vprašanj ponudil nevtralen odgovor v smislu, da anketiranec *ne želi odgovarjati*.

6.1.1. Predstavitev rezultatov ankete med vodji informatike

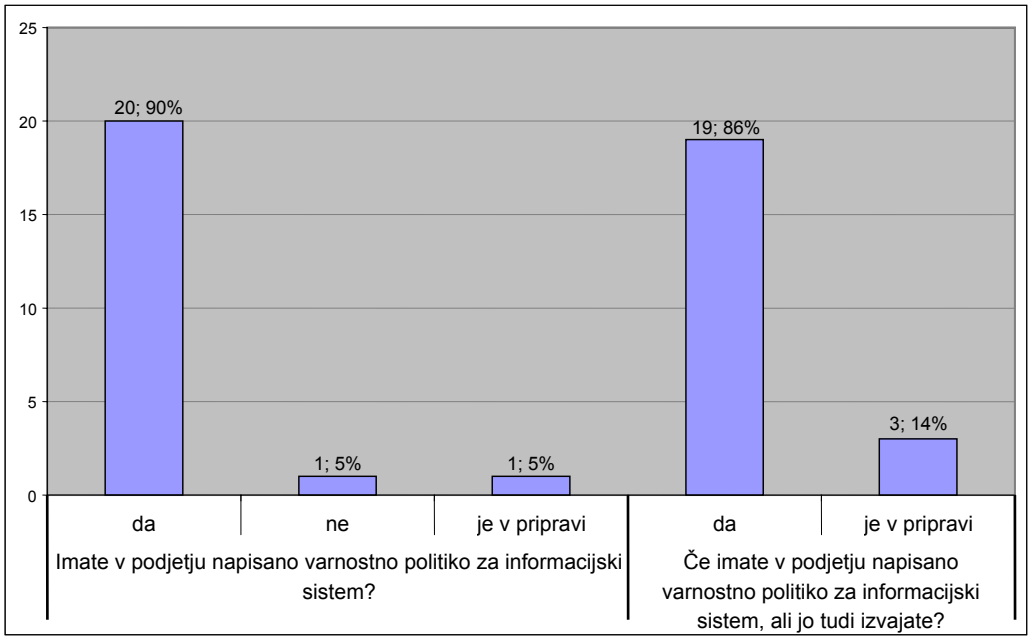
Anketni vprašalnik je bil sestavljen iz naslednjih tematskih sklopov:

- varnostna politika,
- prežeče nevarnosti,
- penetracijski test,
- certificiranje,
- zaposleni in varnost, socialni inženiring, gesla,
- etika, etični kodeks,
- provokativno vprašanje,
- osebni podatki.

V prvem sklopu vprašanj na temo ***varnostna politika*** (glej Graf 1, stran 62) sem dobil pričakovan odgovor, da ima večina podjetij pripravljen oziroma napisan dokument o varnostni politiki informacijskega sistema v podjetju in da varnostno politiko v podjetju tudi izvajajo. Anketirance sem obenem prosil, da na kratko opišejo, kako poteka nadzor nad izvajanjem varnostne politike.

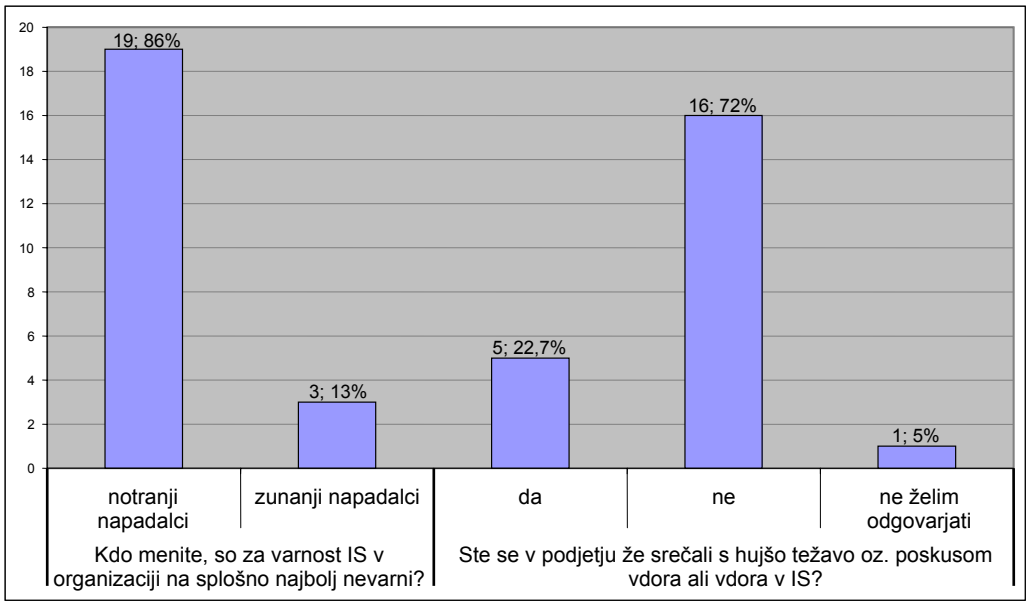
V drugem sklopu (glej Graf 2, stran 62), ki je obravnaval ***prežeče nevarnosti***, je nekaj rezultatov zelo zanimivih. Večina anketirancev (86%) je mnenja, da so za varnost informacijskih sistemov v organizaciji potencialno najbolj nevarni notranji napadalci, kar postavlja nevarnosti, kot so virusi, črvi, napadalci iz svetovnega spleta, hekerji in podobno, na stranski tir. Večina anketirancev meni, da je težav, povezanih s spletnimi napadi, malo, nobeden tega ne smatra kot resen problem, še največ se ubadajo z nezaželeno elektronsko pošto. V podjetjih anketirancev nimajo posebno velikih težav niti z notranjimi napadalci, so pa v 23% že imeli resne težave z vdori v informacijski sistem.

Graf 1. Varnostna politika za informacijski sistem v podjetju.



Vir: Lastni vir.

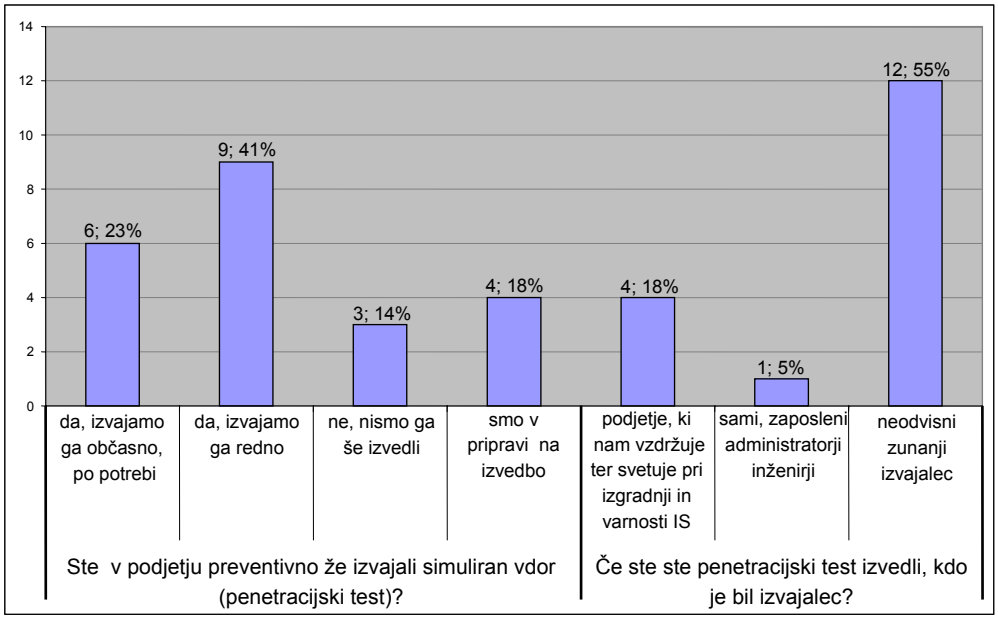
Graf 2. Prežeče nevarnosti.



Vir: Lastni vir.

Glede na to, da je anketa potekala v finančnih institucijah, je zanimiv rezultat tretjega sklopa, ***penetracijski test*** (glej Graf 3, stran 63), da simuliranega penetracijskega vdora oziroma preizkus varnostnih nastavitev pred nezaželenimi napadalci kar v 32% niso izvedli ali pa so šele v pripravi. V 55% je simuliran vdor izvedel zunanji neodvisni izvajalec.

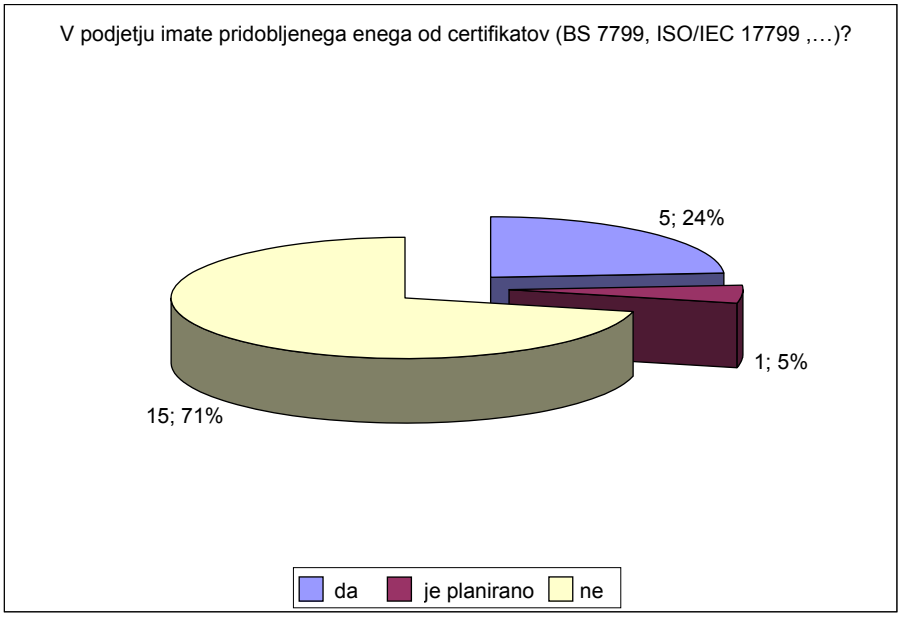
Graf 3. Izvedba penetracijskega testa.



Vir: Lastni vir.

V sklopu vprašanj o ***certificiranju*** (glej Graf 4, stran 63) se mi glede na odgovor, da kar 71% podjetij nima katerega od certifikatov kot na primer BS 7799, niti ne načrtuje njegove pridobitve, postavlja dvom, če sem anketno vprašanje sploh pravilno zastavil. Glede na kratke opise anketirancev sklepam, da niso ravno naklonjeni tovrstnemu delu, da se bolj zanašajo na lastno prakso in izkušnje. Nihče od anketirancev ni mnenja, da je certificiranje izredno pomembno, 68% pa smatra, da je certificiranje srednje pomembno.

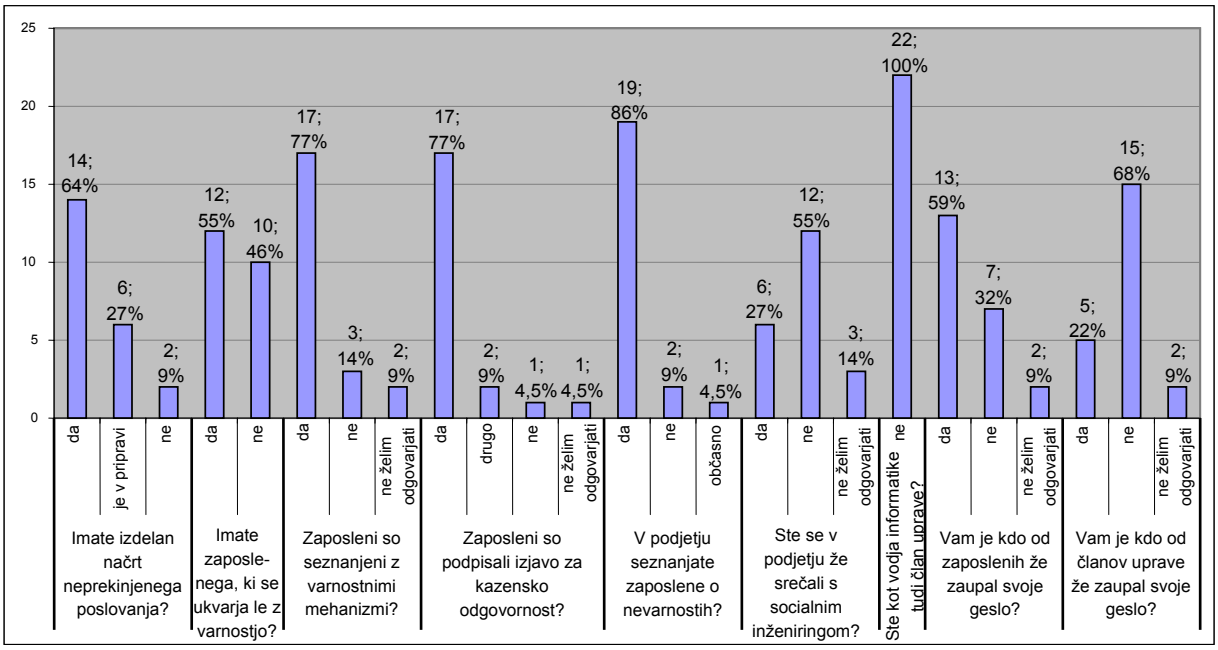
Graf 4. Pridobivanje cerifikatov.



Vir: Lastni vir.

Sklop vprašanj na temo ***zaposleni in varnost, socialni inženiring, gesla*** (glej Graf 5, stran 64) ponuja nekaj zanimivih odgovorov.

Graf 5. Zaposleni in varnost, socialni inženiring, gesla.



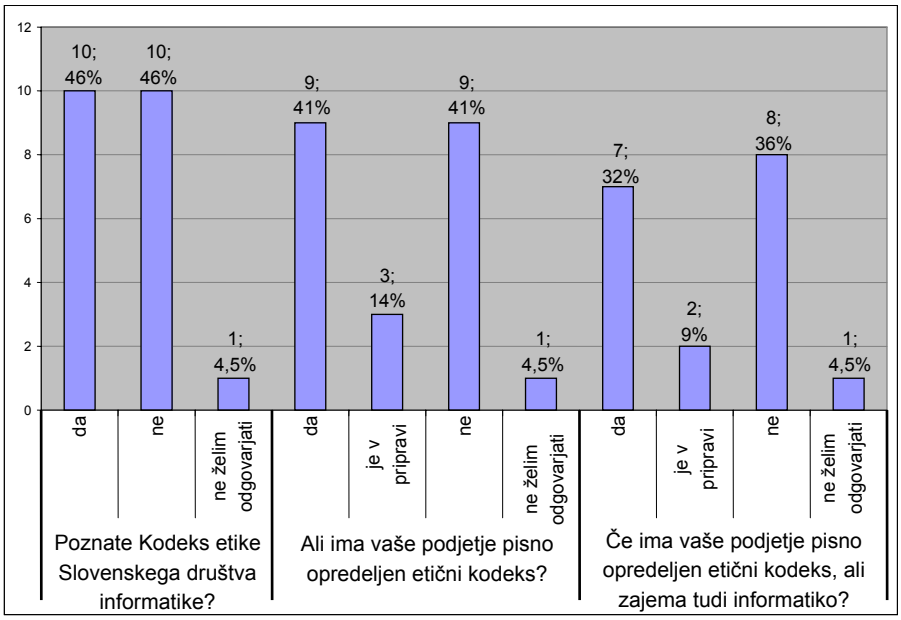
Vir: Lastni vir.

Kar 36 % podjetij še nima dokončanega načrta neprekinjenega poslovanja, pri čemer se postavi vprašanje, koliko in kako so ta podjetja tehnološko opremljena ter ali v podjetju namenjajo in zagotavljajo dovolj sredstev za namene varnosti informacijskih sistemov. Iz odgovorov ugotavljam, da v 23% podjetij niso vsi zaposleni seznanjeni z varnostnimi mehanizmi za varovanje informacijskih sistemov. Glede na to, da so se kar v 27% podjetij že srečali s poskusom socialnega inženiringa, ugotavljam, da socialni inženiring že predstavlja hudo težavo, da bi bilo potrebno v izobraževanja o varnosti informacijskih sistemov vključiti prav vse zaposlene, pri čemur nikakor ne gre pozabiti na snažilke, vratarje, kurirje in ostale pomožne delavce. Vodje informatike so v 91% odgovorili, da v podjetju redno oziroma po potrebi seznanjajo, obveščajo ali izobražujejo zaposlene o nevarnostih, ki pretijo informacijskim sistemom. Nihče od vodij informatike v podjetju ni član uprave. Zelo zanimiva je tudi ugotovitev, da je večini anketirancev kdo od zaposlenih že kdaj zaupal svoje geslo. Pri tem niso izjeme niti člani uprave. Zaposleni se po eni strani ne zavedajo svojih pravic in dolžnosti o varovanju svojega gesla, po drugi strani pa ali imajo tolikšno zaupanje v vodjo informatike ali pa jih je ta na nek način prepričal, da so mu zaposleni geslo zaupali.

Iz odgovorov v sklopu vprašanj ***etika, etični kodeks*** (glej Graf 6, stan 65) ugotavljam, da vodje informatike v finančnih institucijah v več kot polovici primerov še nimajo opredeljenega etičnega kodeksa niti za področje informatike niti za podjetje kot celoto. 46% vseh anketiranih vodij informatike ne pozna Kodeksa etike Slovenskega društva

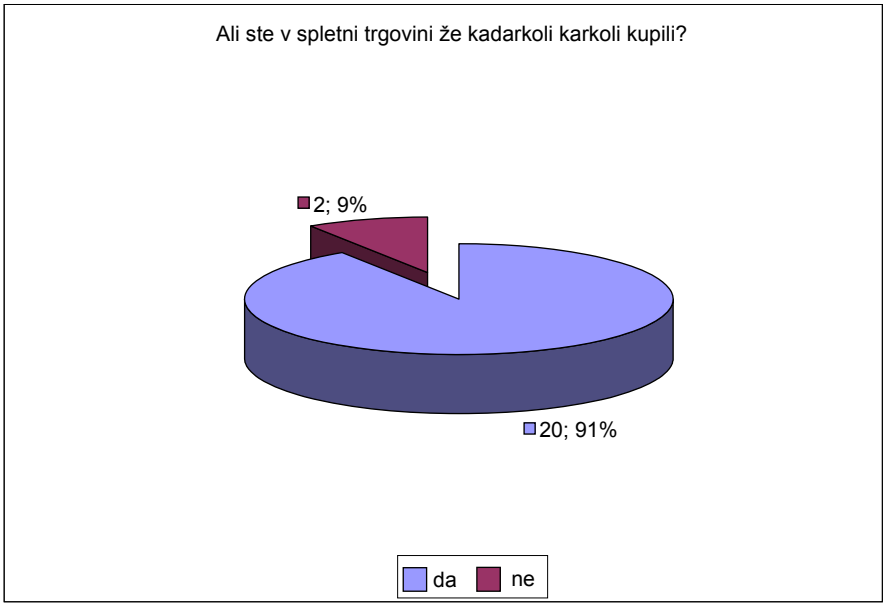
INFORMATIKA. Večina anketirancev bi primer neetičnega ravnanja sporočila nadrejenemu oziroma upravi.

Graf 6. Etika, etični kodeks.



Vir: Lastni vir.

Graf 7. Provokativno vprašanje.



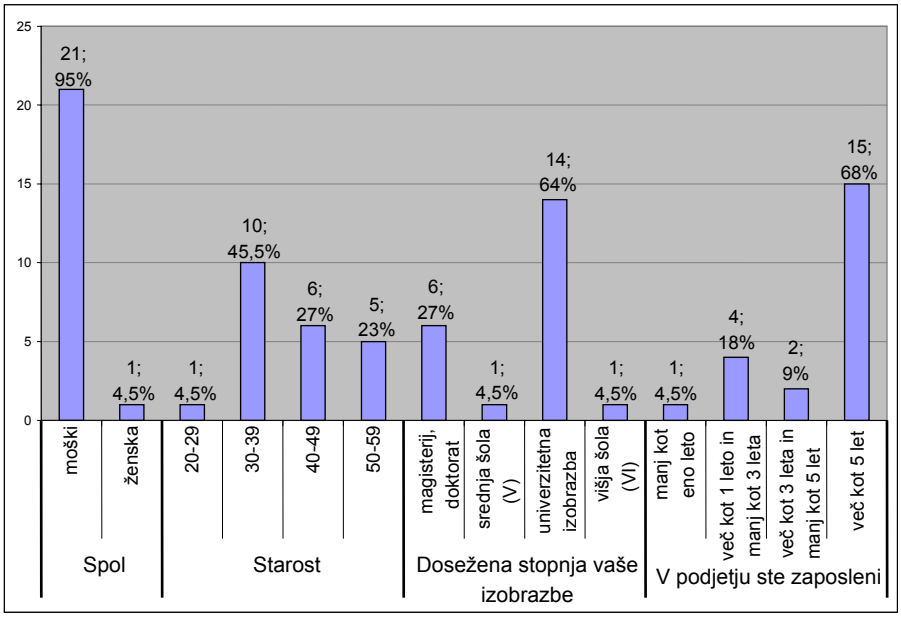
Vir: Lastni vir.

V sklop ***provokativno vprašanje*** (glej Graf 7, stran 65) sem uvrstil le vprašanje, ali je anketiranec že kadarkoli karkoli kupil v spletni trgovini. Kar 91% jih je v spletni trgovini že kupovalo. Iz tega lahko povzamem, da vodje informatike zaupajo v svetovni splet, njegovo varnost, posledično pa verjetno tudi v spletno bančništvo, spletno trgovanje in sorodne sodobne spletne možnosti. Vprašanje sem poimenoval provokativno, ker se dotika povsem

osebne strani anketirancev, v večini primerov je namreč za nakup v spletni trgovini potrebno pustiti osebne podatke in, kar je bistveno, številko kreditne kartice. V tem primeru pa nevarnost zlorabe osebnih financ skokovito naraste.

V zadnjem delu ankete (glej Graf 8, stran 66) sem anketirance prosil za ***osebne podatke***, kot so spol, starost, izobrazba. Ugotavljam, da je vodenje informatike predvsem domena moških (95%), da je 45% starih med 30 in 39 let. 64% anketirancev ima univerzitetno izobrazbo, 27 % magisterij ali doktorat. Večina vodij informatike (68%) je v podjetju zaposlena več kot 5 let.

Graf 8. Osebni podatki vodij informatike.



Vir: Lastni vir.

6.1.2. Povzetek ankete med vodji informatike v finančnih institucijah

Po analizi odgovorov iz ankete med vodji informatike v finančnih institucijah, med katerimi je potekala raziskava, povzemam:

- V večini (91%) finančnih podjetij imajo napisano varnostno politiko za informacijski sistem.
- V večini (86%) finančnih podjetij izvajajo varnostno politiko za informacijski sistem.
- Večina (86%) vodij informatikov meni, da so za varnost informacijskih sistemov v podjetju najbolj nevarni notranji napadalci.
- Podjetjem nevarnosti, kot so virusi, črvi, hekerji in podobno ne predstavljajo večjih težav, še največ težav jim povzroča nezaželena elektronska pošta.
- V večini (68%) finančnih podjetij izvajajo penetracijski test redno ali po potrebi, v teh primerih je v 80% izbran zunanji neodvisni izvajalec .

- V večini (68%) finančnih podjetij nimajo oziroma ne nameravajo pridobiti kateregakoli od standardov (BS 7799,…).
- V 64% finančnih podjetij imajo izdelan načrt neprekinjenega poslovanja.
- V 54% finančnih podjetij imajo vsaj enega zaposlenega, ki se ukvarja izključno z varnostjo informacijskih sistemov.
- V 73% finančnih podjetjih so zaposleni podpisali izjavo za kazensko odgovornost v primeru kršitve Pravilnika za varovanje informacij.
- V večini (86%) finančnih podjetij redno ali po potrebi seznanjajo zaposlene o nevarnostih, ki pretijo informacijskim sistemom.
- V 27% finančnih podjetij so se že srečali s socialnim inženiringom, poleg tega v 14% anketiranci niso želeli odgovoriti na to vprašanje.
- Noben vodja finančnih podjetij ni član uprave podjetja.
- 59% vodjem informatike v finančnih podjetjih je kdo od zaposlenih že zaupal svoje geslo, poleg tega 10% vodij informatike na to vprašanje ni želelo odgovarjati.
- 23% vodjem informatike je kdo od članov uprave že zaupal svoje geslo, poleg tega 10% vodij informatike na to vprašanje ni želelo odgovarjati.
- 45% vodij informatike ne pozna Kodeksa etike Slovenskega društva Informatika.
- 41% finančnih podjetij ima pisno opredeljen etični kodeks.
- 91% vodij informatike je že kupovalo v spletni trgovini.
- 95% vodij informatike je moških.
- 91 % vodij informatike ima vsaj univerzitetno izobrazbo.
- 68% vodij informatike je v podjetju je zaposlenih že vsaj 5 let.

6.2. Anketa med zaposlenimi v zavarovalnici

V empiričnem delu magistrskega dela sem izvedel tudi anketo med zaposlenimi v zavarovalnici. Namen te raziskave je bil med drugim tudi poskus socialnega inženiringa. O sami izvedbi ankete sem seznanil tudi del uprave zavarovalnice. Izpolnjene anketne vprašalnike je vrnilo 43 (86%) zaposlenih, poslanih anketnih vprašalnikov je bilo 50. Ker sem tudi sam zaposlen v zavarovalnici, kjer sem izvajal anketo in osebno poznam vse anketirance, ocenjujem, da je slika stanja o zavarovalnici, ki sem jo dobil z analizo anketnih odgovorov, realna, razen v delu, ki se je nanašal na socialni inženiring, kjer sem povpraševal po uporabniških geslih. Veliko zaposlenih je verjetno podalo svoje uporabniško geslo zaradi vsakodnevne relacije z mano in bi v primeru druge, neznane osebe odgovorili drugače oziroma bi bil odstotek posredovanih gesel bistveno nižji.

Pri pripravi vprašanj sem sledil naslednjim ciljem:

- ugotoviti,
  - kje se zaposleni naučijo dela z raznimi računalniškimi orodji,
  - ali zaposleni poznajo svoje delovno okolje in pojme informacijske varnosti,

    - kakšno je bilo zadovoljstvo zaposlenih z načinom prikaza računalniškega delovnega okolja ob zaposlitvi,
    - ali zaposleni tudi doma uporabljajo osebni računalnik in svetovni splet,
- v sklopu ankete in socialnega inženiringa med zaposlenimi pridobiti čim več uporabniških gesel.

Anketni vprašalnik je bil sestavljen iz 23 vprašanj, nekatera vprašanja so bila obširnejša, sestavljena iz podvprašanj. Glavni namen ankete je bil izvedba socialnega inženiringa. Za njegovo izvedbo sem imel več možnosti oziroma načinov:

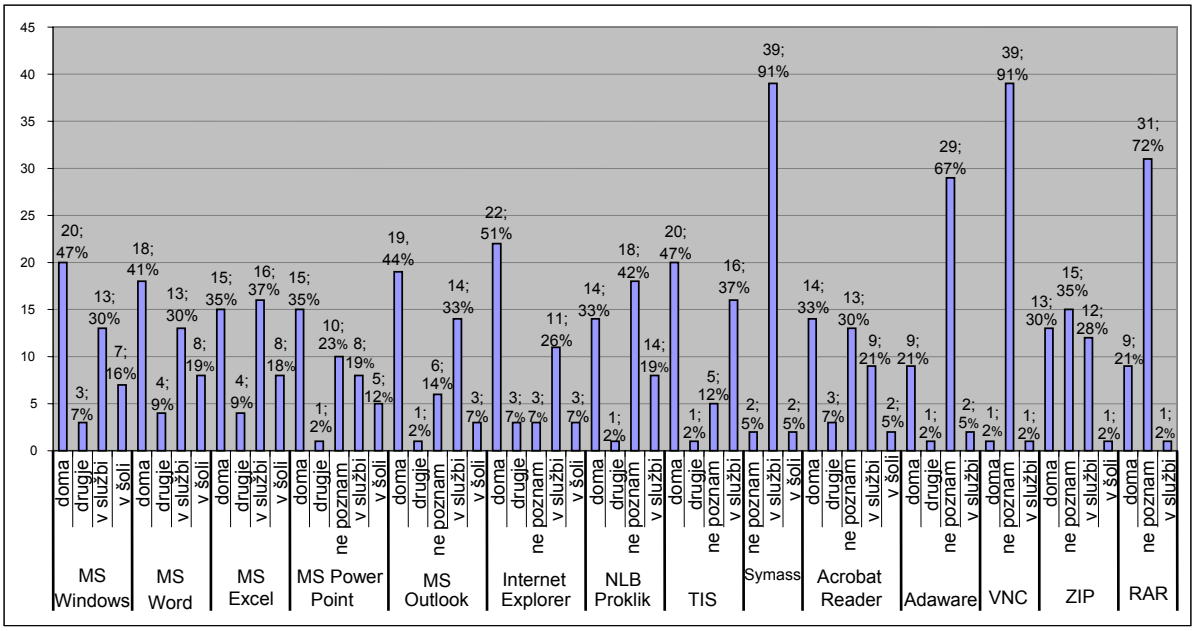
1. anketni vprašalnik poslati po elektronski pošti zaposlenim v zavarovalnici od povsem neznanega pošiljatelja, njegovo ime in uporabniški poštni račun bi ustvaril na primer kot janez.novakovic@gmail.com,
2. anketni vprašalnik poslati po elektronski pošti zaposlenim v zavarovalnici s podpisnikom, ki bi bil ali vodja informatike ali član uprave v zavarovalnici (vsi potrebni podatki so dostopni na spletni strani zavarovalnice), pošiljateljevo ime in uporabniški poštni račun bi ustvaril na primer kot clan.uprave@gmail.com,
3. anketni vprašalnik zaposlenim v zavarovalnici poslati po elektronski pošti z mojega obstoječega elektronskega poštnega računa, kjer je domena enaka drugim zaposlenim v zavarovalnici.

Odločil sem se za tretjo možnost, da anketo izvedem kot sodelavec, kot pravi Jernej Pečnik. Elementi socialnega inženiringa so bili tudi v tem primeru prisotni, saj uporabniških gesel nimam pravice zahtevati od zaposlenih na noben način. Zaposlenim nisem razkril pravega namena ankete, torej sem hotel njihova gesla pridobiti z zvijačo, kar že v osnovi predstavlja socialni inženiring.

6.2.1 Predstavitev rezultatov ankete med zaposlenimi v zavarovalnici

V prvem sklopu ankete sem zaposlene spraševal, kje so se naučili dela z določeno programsko opremo (glej Graf 9, stran 69). Ugotavljam, da se je na delovnem mestu kar 30% zaposlenih naučilo dela z osnovnimi programskimi orodji, kot so operacijski sistem, urejevalniki besedil, preglednice ali tabele. Ugotavljam, da so se zaposleni v izjemno majhnem deležu naučili uporabe raznovrstne programske opreme v šoli, pač pa so jo večinoma spoznali doma. Uporabe zavarovalniške aplikacije Symass se je 91% zaposlenih naučilo na delovnem mestu. Zanimivo je, da 14% zaposlenih ne pozna odjemalca elektronske pošte MS Outlook, čeprav ga prav vsi zaposleni redno dnevno uporabljajo. Vsi zaposleni imajo na svojih računalnikih naloženo tudi ostalo programsko opremo, po kateri sem spraševal, vendar ne poznajo programa Acrobat Reader v 30%, programa Adaware v 67%, programa VNC v 91%, programa ZIP v 35% in programa RAR v 72%. Vsak od teh programov je pri vseh zaposlenih viden na računalniškem zaslonu kot bližnjica.

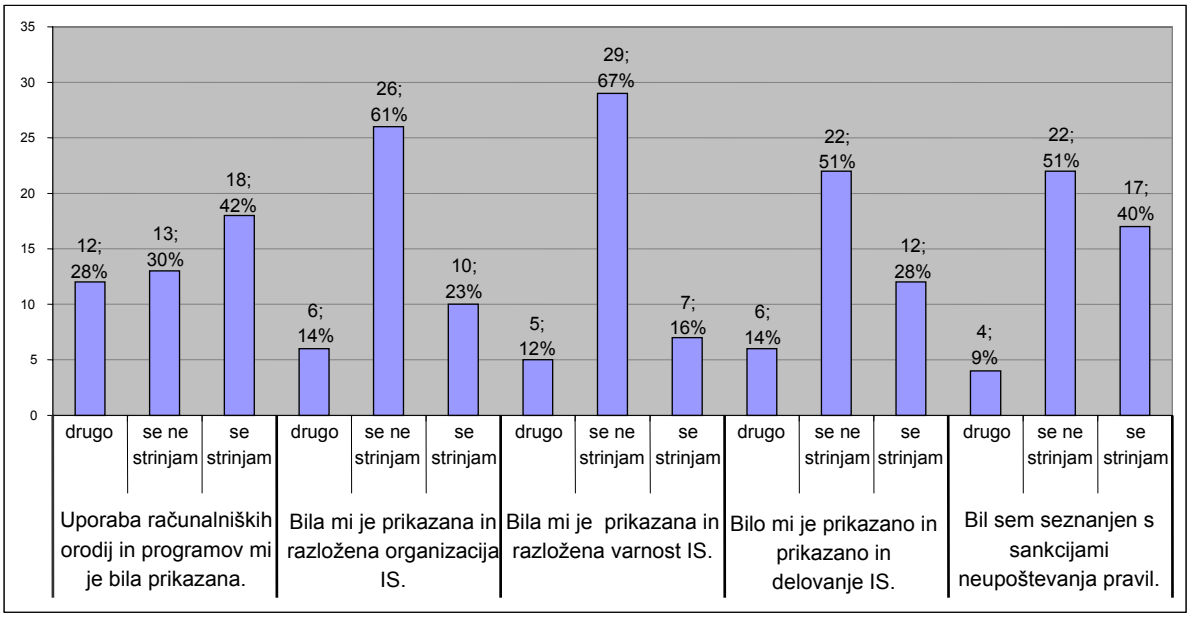
Graf 9. Kje so se zaposleni naučili uporabe programskih orodij.



Vir: Lastni vir.

Naslednji sklop vprašanj se je nanašal na zadovoljstvo zaposlenih o prikazu delovnega okolja ob prihodu na delovno mesto ob zaposlitvi (glej Graf 10, stran 69). Večina zaposlenih je izrazila nezadovoljstvo, da jim organizacija, varnost, delovanje informacijskega sistema ter sankcije ob neupoštevanju pravil niso bili dovolj nazorno razloženi. Bolj zadovoljni (65%) so zaposleni z informiranjem v obliki sestankov znotraj oddelkov.

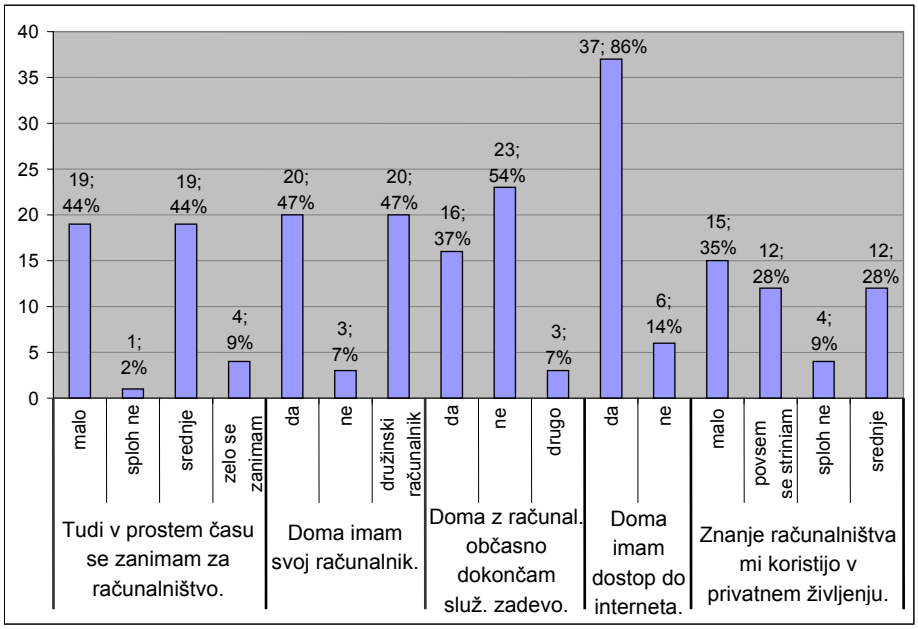
Graf 10. Prikaz delovnega okolja ob zaposlitvi.



Vir: Lastni vir.

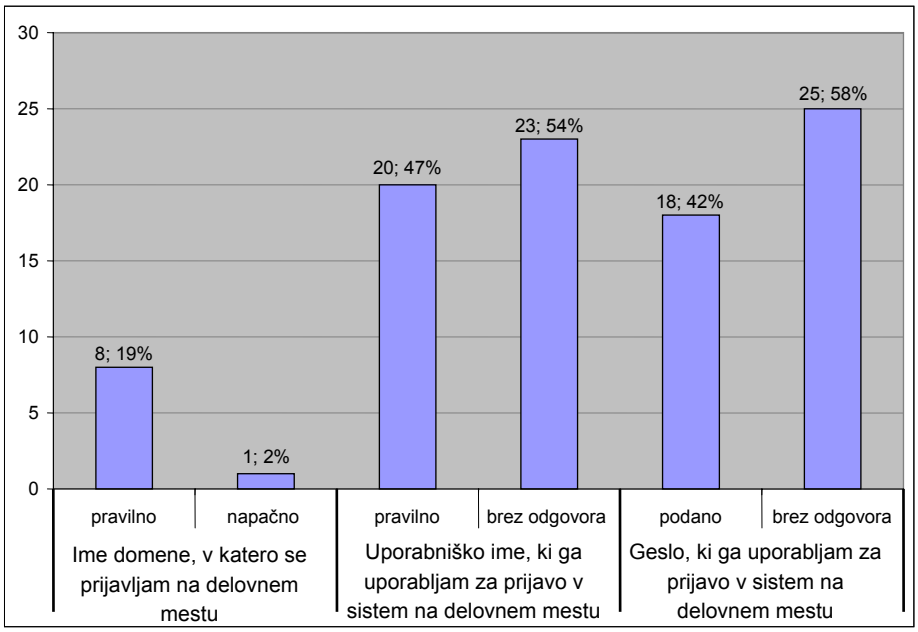
Naslednja tema se je nanašala na uporabo računalnika in svetovnega spleta doma (glej Graf 11, stran 70). Večina zaposlenih ima doma v skupnem gospodinjstvu vsaj en računalnik (93%), polovica od teh ima še svoj računalnik za lastno uporabo. 86% zaposlenih ima doma dostop do svetovnega spleta, 37% zaposlenih občasno ali redno doma uporablja računalnik tudi za službene zadeve.

Graf 11. Uporaba računalnika in svetovnega spleta doma.



Vir: Lastni vir.

Graf 12. Socialni inženiring med zaposlenimi v zavarovalnici.

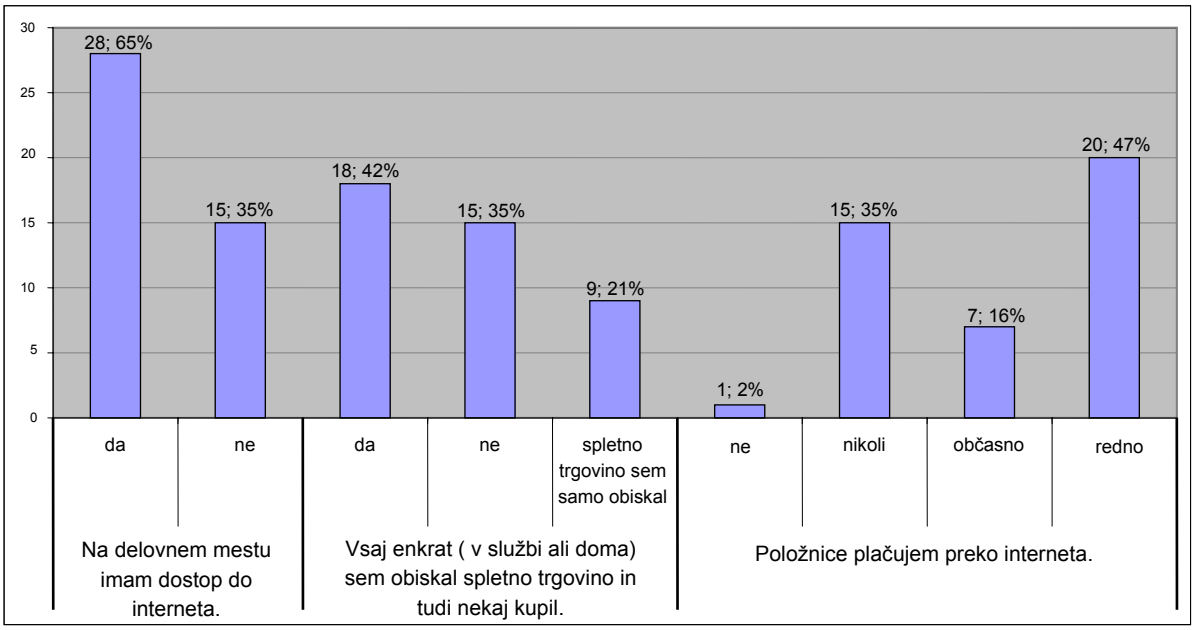


Vir: Lastni vir.

Najbolj zanimiv sklop vprašanj, povezan s socialnim inženiringom (glej Graf 12, stran 70), sem postavil malo pred koncem ankete, ko so se zaposleni že dodobra seznanili z načinom izpolnjevanja, ko so anketiranci ugotovili, da vprašanja niso težka, da nekaj že znajo, ko so lahko pred tem tudi malo pokritizirali delodajalca. Na ta način sem pridobil 42% uporabniških gesel zaposlenih v zavarovalnici, kar je preseglo vsa moja pričakovanja. Pravilnosti uporabniških gesel sicer nisem preverjal v produkcijskem niti kakšnem drugem sistemu, predvidevam pa, da so bila vsa prava, neizmišljena. Vsi, ki so podali svoje uporabniško geslo za prijavo v omrežje informacijskega sistema, so pravilno podali svoje uporabniško ime.

Naslednji sklop vprašanj se je nanašal na svetovni splet (glej Graf 13, stran 71). Vprašanja so bila splošna, namenjena temu, da bi anketiranci pozabili, da so bili nekaj trenutkov prej tarče socialnega inženiringa. Kljub temu so odgovori zelo zanimivi: 47% zaposlenih redno plačuje položnice prek sodobnih bančnih poti, 42% jih je že obiskalo spletno trgovino in tudi nekaj kupilo, na delovnem mestu ima dostop do svetovnega spleta 65% zaposlenih.

Graf 13. Uporaba svetovnega spleta na delovnem mestu.



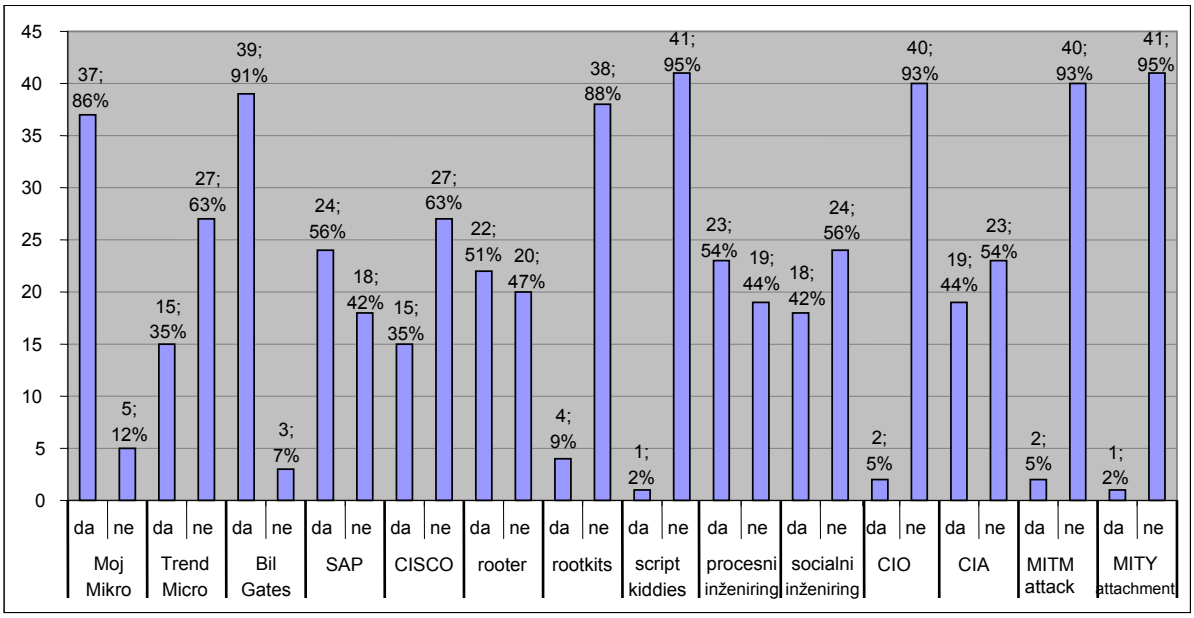
Vir: Lastni vir.

Predzadnji sklop vprašanj (glej Graf 14, stan 72) se je navezoval na prvi sklop; preverjal sem poznavanje informacijskih izrazov, kratic in pojmov ter zbranost anketirancev ob izpolnjevanju anketnega vprašalnika.

Kar 63% odgovarjajočih je navedlo, da še niso slišali za pojem »Trend Micro«, kljub dejstvu, da ima prav vsak uporabnik na svojem računalniku nameščen ta protivirusni program. To vprašanje je bilo namenoma postavljeno med vprašanjema o poznavanju pojma »Moj Mikro« in »Bil Gates«, pri katerih pa so bili odgovori pritrdilni v več kot 86%. Pojem »Bil Gates« v resnici ne obstaja, namenoma sem storil slovnično napako pri imenu lastnika ameriškega podjetja Microsoft, Billa Gatesa. Večina ostalih odgovorov je bila v okviru mojih pričakovanj

in znanja anketirancev, torej lahko trdim, da so anketiranci na vprašanja odgovarjali pošteno, ne »na slepo«.

Graf 14. Poznavanje informacijskih izrazov.

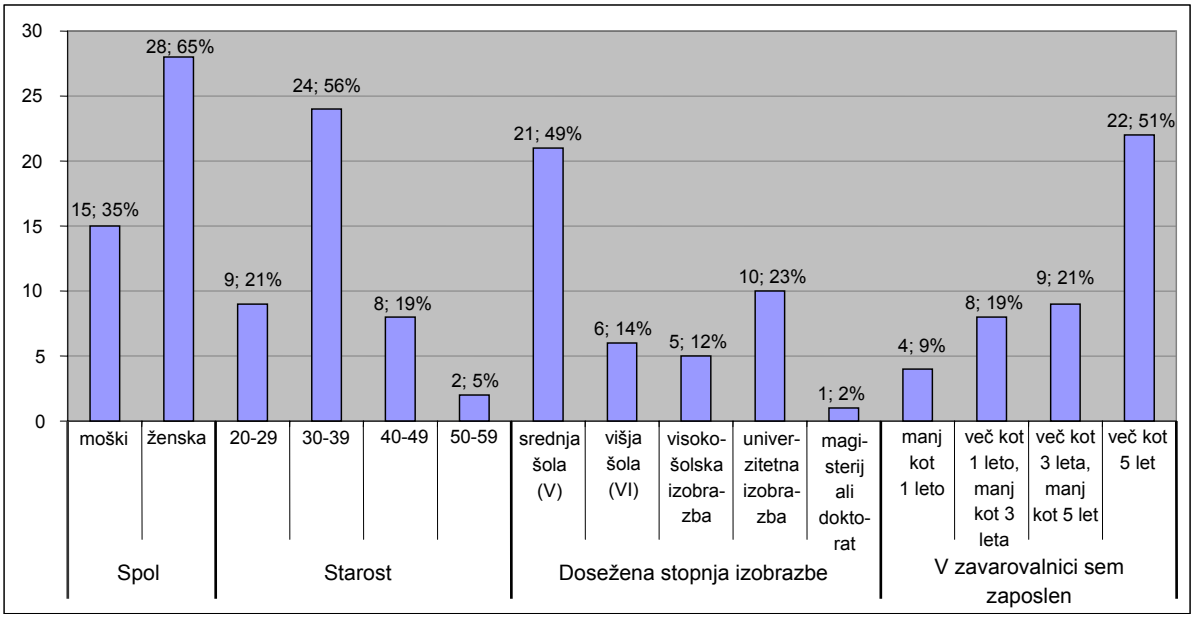


Vir: Lastni vir.

Večino vprašanj sem kombiniral med sabo (primer pojma »rooter« in »rootkits«), pri čemer sem naredil nekaj namernih napak; na primer pojem »rooter« ne obstaja, vseeno ga je poznalo 51% anketirancev! Seveda je za pojem »rooter« pravilna asociacija na pojem »router«, kar je angleška beseda za preklopnik. Pojem »MITY attachment« sem si povsem izmislil in ne obstaja v svetovni literaturi (zanj pa je slišal že en anketiranec!), uporabil sem ga v kombinaciji s poznavanjem pojma »MITM attack«, kar v slovenskem prevodu označuje napad, kjer se napadalec postavi na sredo med komunicirajoči stranki in poskuša ujeti ključ, šifro ali geslo. V kombinaciji s pojmom »procesni inženiring« sem uporabil pojem »socialni inženiring«, za katerega je že slišalo 42% anketirancev. Očitno pa ne poznajo njegovega dejanskega pomena , saj je 44% vseh, ki so že slišali za ta pojem, izdalo svoje uporabniško geslo za prijavo v zavarovalniško omrežje. Izmed vseh anketirancev je le eden slišal za pojem »script kiddies« (uporabnik iz oddelka informatike), tudi za pojem oziroma kratico »CIO« sta slišala le dva anketiranca. Glede na to, da je v zavarovalnici uveden tudi SAP sistem, je zanimivo, da kar 42% zaposlenih še ni slišalo zanj, dejstvo pa je, da ga ne uporabljajo v vseh oddelkih, pač pa samo v oddelkih računovodstva in financ.

V zadnjem sklopu vprašanj sem anketirance prosil za osebne podatke (glej Graf 15, stran 73). 65% vseh zaposlenih je žensk, 56% vseh zaposlenih je starih med 30 in 39 let, 49% zaposlenih ima končano srednjo izobrazbo, 51 % vseh zaposlenih je v zavarovalnici zaposlenih več kot 5 let.

Graf 15. Osebni podatki zaposlenih.



Vir: Lastni vir.

6.2.2. Povzetek ankete med zaposlenimi v zavarovalnici

Po analizi odgovorov iz ankete med zaposlenimi v zavarovalnici, med katerimi je potekala raziskava, povzemam:

- 79 % zaposlenih se je že udeležilo izobraževanj na temo računalništva.
- Rokovanja z uporabniškimi programi, kot so TIS, MS Word, Exel, PowerPoint, Internet Explorer, se je slaba polovica zaposlenih naučila doma.
- 91% zaposlenih se je uporabe zavarovalniške aplikacije naučila na delovnem mestu.
- Zaposleni so izrazili nezadovoljstvo glede prikaza in razlage organizacije informacijskega sistema, delovanja informacijskega sistema, nezadovoljni pa so tudi s sankcijami zaradi neupoštevanja pravil.
- 7% zaposlenih doma nima osebnega računalnika.
- 86% zaposlenih ima doma dostop do svetovnega spleta.
- 37% zaposlenih redno ali občasno z računalnikom dokonča ali pripravlja službene zadeve.
- 42% zaposlenih je podalo svoje geslo za prijavo v informacijsko omrežje zavarovalnice.
- Na delovnem mestu ima 65% zaposlenih dostop do svetovnega spleta.
- 42% zaposlenih je že kupovalo na svetovnem spletu.
- 63% zaposlenih redno ali občasno plačuje položnice preko svetovnega spleta.
- 86% zaposlenih je slišalo za pojem »Moj Mikro«.
- 63% zaposlenih ni slišalo za pojem »Trend Micro«, čeprav ima vsak zaposlen na svojem računalniku naložen ta protivirusni program.

- 91% zaposlenih je že slišalo za pojem »Bil Gates«.
- 56% zaposlenih je že slišalo za pojem »SAP«.
- 12% zaposlenih je že slišalo za pojem »DNS«.
- 67% zaposlenih je slišalo za pojma« konsolidacija« in »virtualizacija«.
- 2% zaposlenih je slišalo za pojem »Script kiddies«.
- 53% zaposlenih je slišalo za pojem »procesni inženiring«.
- 42% zaposlenih je slišalo za pojem »socialni inženiring«, od tega jih je 44% navedlo svoje uporabniško geslo za prijavo v informacijsko omrežje zavarovalnice.
- 35% zaposlenih v zavarovalnici je moških.
- 56% zaposlenih je starih med 30 in 39 let.
- 26% zaposlenih ima vsaj univerzitetno izobrazbo.
- 51% zaposlenih je v zavarovalnici zaposlenih več kot 5 let.

6.3. Anketa med slovenskimi uporabniki elektronske pošte

V okviru praktičnega dela tega magistrskega dela sem imel namen izvesti tudi »vseslovensko« anketo s ciljem poskusiti pravi socialnegi inženiring. Zbranih sem imel že prek deset tisoč elektronskih naslovov posameznikov (privatne in službene), ki sem jih pridobil povsem legalno med elektronsko pošto na delovnem mestu. Konkretno mislim na raznorazna verižna pisma, šale, filme in podobno, kar si ljudje posredujejo med seboj. Zelo veliko elektronskih naslovov sem pridobil na spletnem brskalniku www.najdi.si in na drugih spletnih straneh. Na spletni strani mail.google.com sem imel pripravljen poštni predal z izmišljenim imenom, na katerem naj bi se zbirale rešene, vrnjene ankete. Pripravljen sem imel anketni vprašalnik z ne preveč vprašanji, med njimi tudi vprašanje, kakšno je anketirančevo uporabniško ime in geslo na delovnem mestu, v šoli oziroma na fakulteti. Predstaviti sem se nameraval kot študent ali dijak, ki dela seminarsko nalogo na temo »Kako si na najenostavnejši način zapomnim svoje geslo«.

Pred samo izvedbo ankete sem se povezal s kriminalistično policijo (g. Šavnik, g. Uranjek) in jih prosil za pomoč ter oceno legalnosti nameravane izvedbe ankete. Pripravljen sem bil izvesti to anketo tudi z njihovim sodelovanjem, z njihovim »soavtorstvom«, oziroma bi bil zame sprejemljiv kakršenkoli način sodelovanja z njimi, saj bi z izvedbo ankete skupaj lahko pridobili dober podatek, kako varnostno ozaveščeni smo Slovenci. Pripravljen sem bil pridobiti še več elektronskih naslovov. Kriminalistični policiji se je zdel predlog sicer izredno zanimiv, vendar niso bili pripravljeni sodelovati, ker bi po njihovem mnenju lahko bila početje in izvedba ankete zakonsko sporna. Prav tako so tudi meni odsvetovali nadaljevanje tega dela praktične izvedbe magistrskega dela. Izpostavili so več razlogov in nejasnosti, na primer, kako naj sami ravnajo, če dobijo prijavo s strani kakšnega prejemnika elektronske pošte.

Kriminalistični policiji sem omenil namen izvedbe podobne ankete znotraj zavarovalnice v kateri sem zaposlen, s pravo identiteto in obstoječim elektronskim naslovom, čemur pa niso nasprotovali.

7. Celovit pristop k varnosti

Banke in zavarovalnice, ki sodijo v finančni sektor, že dlje časa med drugim ponujajo uporabo storitev preko spletnega komuniciranja. Zelo dobro se zavedajo varnostnih informacijskih tveganj, zato s sodobnimi tehnologijami zagotavljajo visoko stopnjo varnosti pri elektronskih komunikacijah s komitenti. Uporabnikom svetujejo upoštevanje minimalnih standardov, ki zagotavljajo varnost spletnega načina poslovanja. Kljub temu pa zaradi uporabe osebnega računalnika za druge namene v delovnem ali domačem okolju lahko pride do zlorabe zaupnih podatkov, kot so gesla, PIN (osebna identifikacijska številka), digitalna potrdila, številke kreditnih kartic in podobno.

Finančne institucije sicer spremljajo delovanje svojih sistemov in redno uvajajo ustrezne varnostne ukrepe, vendar so ti učinkoviti samo, če tudi komitenti pri uporabi osebnega računalnika upoštevajo priporočila bank in zavarovalnic za zagotavljanje varnosti elektronskega poslovanja prek javnega omrežja. Ta priporočila je Združenje bank Slovenije nazadnje strnilo in posredovalo uporabnikom februarja 2007, vsebujejo pa dvanajst dokaj podrobnih, a navadnim uporabnikom še vedno razumljivih pravil za varno elektronsko komuniciranje, ki jih na kratko povzemam:

1. *Varujte podatke, ko jih pošiljate po odprtih komunikacijskih poteh (spletu)*. Splošno pravilo je, da se po odprtih komunikacijskih poteh občutljivi in zaupni podatki (geslo, digitalno potrdilo in podobno) ne pošiljajo. Ko je osebni računalnik (vsak ima svojo edinstveno, IP številko, ki ga enoznačno označuje) priključen na splet, lahko spreten zasledovalec prevzame nadzor nad njim, spremlja aktivnosti, ga okuži z virusom in podobno.
2. *Prepričajte se, s kom elektronsko komunicirate*. Spletne strani so lahko ponarejene, preko njih lahko neupravičene osebe zahtevajo vnos zaupnih podatkov, po katerih finančna institucija nikoli ne povpraša.
3. *Skrbno ravnajte z občutljivimi podatki in pazite na medije za pristop*. Hramba občutljivih podatkov ni varna, če uporabnik pušča disketo v disketni enoti, pametno kartico v čitalniku, generator gesel, spominski ključ USB ali drug prenosni medij v dosegu nepooblaščenih oseb. Hrambi prenosnih medijev je potrebno nameniti posebno pozornost, da ne pride do odtujitev. Prenosnih medijev z občutljivimi podatki, digitalnimi potrdili, se ne vstavlja v računalnik/čitalnik pred začetkom dela (na primer s spletno banko), da se prepreči vzpostavitev neželene komunikacije.
4. *Izberite varno geslo*. Za vstop v spletno banko se je potrebno najprej povezati v splet, identifikacija pa se opravi z digitalnim potrdilom, geslom ali s kombinacijo obeh. Dovolj zanesljivo geslo mora biti sestavljeno tako, da ga je težko uganiti, da je dolgo

vsaj šest znakov, da je kombinacija velikih in malih črk ter posebnih znakov, potrebno pa ga je tudi menjavati na določeno časovno obdobje.

5. *Vedno uporabljajte programsko opremo, ki ima uradno licenco*. S spletnega naslova naj se ne prenaša nobena programska oprema, če ni zagotovila, da sta prenos in njeno delovanje varna ter verodostojnost pošiljatelja neoporečna. Prenašanje neplačljivih programov s svetovnega spleta se šteje za veliko varnostno tveganje.
6. *Uporabljajte najnovejše različice programske opreme*. Izdelovalci programskih rešitev nenehno izboljšujejo svoje izdelke, zato je priporočljivo uporabljati samo najnovejše različice operacijskega sistema in programske opreme, zlasti protivirusnih programov.
7. *Ne zanemarjajte varnostnega preverjanja*. Pri uporabi elektronske pošte je pravilo, da se ne odpirajo pripete datoteke, če pošiljatelj sporočila ni znan, po možnosti naj se ne odpre niti sporočilo. Če se uporabnik vseeno odloči, da pregleda pripeto datoteko, jo je potrebno predhodno shraniti in preveriti z varnostnim programom. To velja še posebej za vse tipe datotek s končnicami .bat, .exe, .com pa tudi za zvočne zapise in slike, kjer se prav tako lahko skrivajo prevare.
8. *Vklopite varnostne nastavitve spletnega brskalnika*. Priporočljivo je, da se po končanem delu pobrišejo piškotki, to so datoteke, kamor spletni brskalnik pri brskanju po spletu zapisuje sporočila, s katerimi računalnik hitreje najde že obiskano spletno stran. Priporočljivo je izključiti samodejno shranjevanje nastavitev spletnega brskalnika. Ta funkcija namreč shranjuje nastavitve, lahko tudi imena in gesla, ki so se pred tem uporabljala.
9. *Namestite na računalnik lovce virusov in dodatno zaščitno programsko opremo*. Ker operacijski sistemi ne zagotavljajo vseh varnostnih postopkov, je potrebno imeti nameščeno dodatno zaščitno programsko opremo, kot so protivirusni programi, protivohunski programi in podobno. Pozoren je potrebno biti tudi na spletne strani, kajti povsod so lahko nameščeni programi za samodejno vohljanje in sporočanje ali druga zlonamerna programska koda. V kakovostno programsko opremo sodi tudi požarni zid, ki dovoli le znane in avtorizirane povezave.
10. *Redno arhivirajte pomembne podatke*. Izguba podatkov, ki jih ni več moč priklicati, je lahko zelo boleča izkušnja, zato je sprotno in dosledno arhiviranje izredno pomembno. Ni tako pomembno, za kateri medij se uporabnik odloči, pomembneje je, da podatke redno shranjuje, da preverja, kaj je shranjeno ter da se arhivski medij shrani na mesto, ki ni dostopno nepooblaščenim.
11. *Za varnost poskrbite tudi pri vzdrževanju računalniške opreme*. Ob okvari se je potrebno obrniti na preverjene in usposobljene servisne službe. Pred predajo zaupne osebne podatke po možnosti začasno shranite na prenosni medij, na računalniku pa jih zbrišite.
12. *Redno preverjajte stanje na vašem bančnem računu*. K hitremu odkrivanju morebitnih neskladij zelo pripomore tudi sprotno in dosledno preverjanje stanja in transakcij na bančnem računu.

V nadaljevanju podajam splošna pravila, ki bi se jih podjetja in organizacije morale držati, če želijo zagotavljati vsaj osnovno varnost svojih informacijskih sistemov:

Varnostno kopiranje (angl. Backup). Definirati je potrebno pravila (Norberg, 2001, str. 136–137), kdo je odgovoren za izvajanje varnostnega kopiranja podatkov, kako pogosto naj se varnostno kopiranje izvaja, kje naj bodo shranjeni mediji z varnostno kopirano vsebino ter kdo je pristojen za obnovo (angl. restore) podatkov v sistem ali bazo.

Vzdrževanje omrežja. Vzdrževanje omrežja oziroma informacijskega sistema je trdo delo. Zahteva strokovno znanje, ustrezne metodologije, napisana pravila in tudi hitrost (Norberg, 2001, str. 169-175). Priporoča se redno revidiranje sistemov s strani zunanjega izvajalca, priporoča se redno informiranje (liste elektronske pošte proizvajalcev (HP, Microsoft, Red Hat, IBM, Cisco,..) in izobraževanje o novih varnostnih rešitvah.

Zagotavljanje varnega dostopa od doma ali druge lokacije do omrežnih virov znotraj podjetja. Na spreminjanje načina poslovne uporabe računalnika najbolj vplivajo dostopnost širokopasovnih povezav, razmah mobilnih naprav, porast IP telefonije in povečanje dela od doma. Naloga sistemskih upraviteljev je, da tak dostop omogočijo, saj lahko organizacija tako ustvarja in ohranja konkurenčno prednost na trgu, obenem pa mora poskrbeti za zaščito virov in podatkov. Organizacije se v praksi največkrat odločajo za začetno uvedbo manjšega obsega (dostop do spletnih odjemalcev elektronske pošte, dokumentov v skupni rabi), rešitev pa nato nadgrajujejo na vse širši spekter poslovanja (dostop do spletnih aplikacij, kot so dokumentni sistem, aplikacija CRM, naročila, prijave napak in druge). Poglavitna razlika je v varnostni komponenti, preverjanju varnosti dostopne točke in mehanizmu za zaščito podatkov. Zaščita podatkov pokriva celotno področje, od varnosti povezave do zaščite podatkov na strani uporabnika in na strani virov (Justin, 2007, str. 12 – 13).

Organizacije morajo pri rednem pregledovanju in načrtovanju razvoja svojega omrežja upoštevati naslednja pravila (Norberg, 2001, str. 15), priporočljivo pa je, da jih kot osnovo pri gradnji omrežja upoštevajo tudi organizacije v nastajanju, ki svoj informacijski sistem šele načrtujejo:

- *Neprepustnost*. Ne dovoliti drugega prometa po mreži razen tistega, ki je nujno potreben.
- *Obramba v globino*. Ne zanašati se le na en varnostni mehanizem.
- *Enostavnost*. Zapletene tehnologije in pravila je težko implementirati in težko razumeti. Prednost uporabi že preizkušenih produktov.
- *Postopnost*. Priporoča se postopno, fazno uvajanje posameznih segmentov v varnosti.
- *Planiranje*. Pred vsakim posegom v delovanje informacijskih sistemov in s tem povezano varnostjo je potrebno vsak korak dobro načrtovati.

Varnostne politike predstavljajo temelj informacijske varnosti podjetja in določajo pričakovan način dela z informacijskimi sredstvi v podjetju. Na eni strani določajo uporabo informacijskih sredstev za običajne uporabnike, na drugi strani pa temeljito opisujejo načine uporabe varnostnih mehanizmov in sredstev v oddelku za podporo informacijski tehnologiji.

Informacijske varnostne politike morajo zajemati vsa področja informacijske varnosti, ki so predpisana s standardom ISO 17799. Zaradi lažjega upravljanja informacijske varnosti je priporočljivo varnostne politike razdeliti v zaokrožena področja:

- krovna varnostna politika (predpisuje zaščito informacijskega sistema in mora biti dokument, ki izraža namen oziroma zahtevo uprave po zagotavljanju varnosti, neoporečnosti in zaupnosti informacijskega sistema in s tem poslovanja),
- informacijska varnostna politika za zaposlene (izdelana je na temelju principov in deklaracij iz krovne varnostne politike, ureja varovanje informacij in opreme, določa koncept lastništva nad podatki in opremo, razmejuje nadzor in odgovornosti, postavlja pravila ravnanja s svetovnim spletom, elektronsko pošto in gesli, ureja dostop tretjih strank),
- varnostna politika za področje informacijske tehnologije (nanaša se na posamezna področja informacijske zaščite informacijskega sistema, dokument s stališča principov zaupnosti, neoporečnosti in razpoložljivosti opredeljuje področja identifikacija/overovitev/odobritev, zaščita/zaupnost informacij, razpoložljivost informacijskih storitev, nadzorni zapisi, usklajenost, obvladovanje varnostnih incidentov in fizičen nadzor dostopa).

Priporočljivo je, da organizacije razmislijo in v svoj dokument o varnostni politiki vključijo sklepe in določila o:

- uporabi svetovnega spleta (Overly, 1999, str. 107),
- prepovedanih aktivnostih (Overly, 1999, str. 100-101),
- definiranju privatnih opravil in prepovedi le teh (Overly, 1999, str. 100),
- smernicah zaposlenim za uporabo elektronske pošte (Overly, 1999, str. 71),
- lastništvu aplikacij (Information Security Policy Manual),
- razvoju aplikacij (Information Security Policy Manual),
- tehnični podpori (Information Security Policy Manual),
- glasovni komunikaciji (Information Security Policy Manual),
- izbiri, razvoju in implementaciji programske opreme ter ponudnikov le-te (Information Security Policy Manual),
- postopkih v primeru kršitve varnosti (Information Security Policy Manual),
- shranjevanju in uničenju podatkov (Information Security Policy Manual),
- tiskanju in distribuciji poročil (Information Security Policy Manual),

- magnetnih medijih (Information Security Policy Manual),
- izjemah v sprejetih pravilih in postopkih (Information Security Policy Manual),
- sprejemljivih metodah šifriranja podatkov (Information Security Policy Manual),
- elektronski izmenjavi podatkov (Information Security Policy Manual),
- lastništvu podatkov (Information Security Policy Manual),
- dostopu v strežniško sobo (Information Security Policy Manual),
- računalniških sistemih in okolju (Information Security Policy Manual).

Podjetja v celovitem dokumentu o varnostni politiki ne smejo pozabiti vključiti:

- analogne in ISDN linije, klicne dostope, oddaljene dostope drugih organizacij,
- varnostne preglede,
- ohranjanje sporočil elektronske pošte,
- etični kodeks podjetja,
- določanje občutljivosti informacij,
- ocenjevanje tveganj,
- varnostne nastavitve usmerjevalnikov in stikal,
- varnostne nastavitve strežnikov,
- brezžične komunikacije,
- uporabo prenosnih računalniških naprav,
- storitve in podporo za dlančnike, dogovor o skrbništvu mobilnih naprav.

V preteklosti je informatike zanimalo predvsem to, koliko časa potrebujejo, da spet vzpostavijo informacijsko infrastrukturo po resni prekinitvi. Sedaj, ko je informatika vpeta praktično v vse poslovne procese v podjetjih, je zanimivejše vprašanje, kako dolgo lahko podjetje posluje, če njegovi kritični poslovni procesi ne delujejo. To seveda pomeni, da se na morebitno katastrofo ne smejo pripravljati le informatiki, temveč je potrebno posebno pozornost nameniti procesom. Pri tem se je treba držati temeljnih pravil (Djurdjič, 2004, str. 15):

- *Ločevanje iniciative za načrtovanje neprekinjenega poslovanja od iniciative za okrevanje po katastrofi*. Cilj okrevanja po katastrofi je tehnično okrevanje, to je vnovična vzpostavitev pomnilniških in strežniških sistemov, omrežja in drugih sistemov, zato so zanj odgovorni računalniški strokovnjaki. Cilj nepretrganega poslovanja je stabilnost poslovnih procesov, zato so zanjo zadolžena različna poslovna področja.
- *Skrb, da so vsi postopki dobro definirani in dokumentirani*. Postopki morajo biti zapisani tako, da se jih da izvajati brez ključnih zaposlenih, ki so načrt za nepretrgano poslovanje pripravili. V primeru resne nesreče se lahko zgodi, da ti strokovnjaki ne bodo na voljo.

- *Pomembnost procesa se presoja s stališča ustvarjanja prihodka*. Vsak poslovni vodja oziroma tisti, ki je odgovoren za posamezen proces v podjetju, bo zahteval, da vsa informacijska podpora za njegov proces deluje takoj po nepričakovanem dogodku, vendar pa vsaka aplikacija ni ključna za prihodek in preživetje podjetja. Če mora poslovni vodja ocenjevati aplikacijo s stališča ustvarjanja prihodka, potem bo res premislil, kako hitro zares potrebuje aplikacijo. Prav ugotavljanje ključnih aplikacij, ki jih je nujno vzpostaviti, kakor hitro je mogoče, je glavni del pogajanj pri pripravi načrta za nepretrgano poslovanje.
- *Preizkus pripravljenih načrtov v praksi*. Skrbno periodično pregledovanje načrtov je sicer pomembno, vendar ne zadostno, ker se v praksi pogosto pokaže, da kakšna stvar ne deluje po pričakovanjih. Velike družbe naj bi do dvakrat na leto izvedle simulacijo katastrofe in pri tem preizkusile tehnologijo za povrnitev po katastrofi in načrte za neprekinjeno poslovanje.
- *Analiza, kaj je šlo pri preizkusu po načrtih in kje so potrebne spremembe*. Priprava načrtov za neprekinjeno poslovanje ni nikoli zaključeno delo, saj se procesi v podjetju spreminjajo. Zato je ključno, da se rezultati preizkusa analizirajo in da se posveti posebno pozornost tistim mestom, kjer so nastale težave. Če so spremembe potrebne, je treba načrt spremeniti ali dopolniti.

Na področju okrevanja po katastrofi se pojavljajo cenejše alternative, in sicer ponudniki, ki ponujajo rezervne lokacije v obliki zunanjega izvajanja storitev (angl. outsourcing), v obliki najema za mesečni ali letni pavšal, kar je lahko precej ceneje od lastne izgradnje sistema. Ti ponudniki lahko učinkoviteje nadzorujejo izkoristek uporabe rezervnih sistemov, kljub temu, da v vsakem trenutku ponujajo tudi dosegljivost v primeru napak. Prihranki so možni predvsem zaradi souporabe sistemov in storitev nadzora, pri katerih se stroški porazdelijo med več naročnikov. Takšni rezervni centri imajo tudi pomembno šibko točko. Če upravljajo rezervne kapacitete za eno regijo, lahko v primeru naravne nesreče, na primer potresa, udara strele ali poplave, več podjetij hkrati potrebuje svojo rezervno lokacijo, kar lahko tak center zelo obremeni.

Investicije v informatiko same po sebi ne prinašajo poslovne vrednosti (Groznik, 2005, str. 220), prav tako ne investicije v informacijsko varnost. Osnova za dolgoročen uspeh je strateško načrtovanje informatike, v sklopu katerega mora biti varnost informacijskih sistemov eden od temeljnih gradnikov. Ključni dejavniki strateškega načrtovanja informatike in tudi glavni nosilci vrednosti informatike so poslovni procesi, kadri in znanje, informacijska tehnologija ter povezave med njimi, vključno z vsemi posledicami potrebnih organizacijskih sprememb v smeri procesne organiziranosti in položaja informatike v podjetju (Groznik, 2005, str. 220). Če je katerikoli teh dejavnikov, še posebej pa informacijska tehnologija, na kakršenkoli način podvržen varnostnemu tveganju, je lahko ogroženo poslovanje in celo obstoj podjetja.

8. Sklep

Informacijska varnost ima vse večjo vlogo in pomen v poslovnem procesu družb. Številnim organizacijam z večjo informacijsko varnostjo uspeva zmanjševati tveganja. To dosegajo predvsem ob pomoči večjih vlaganj v informacijsko varnost in s tesnejšim sodelovanjem vodilnega osebja ter ob pozitivnem učinku zahtev nadzornih organov. Kljub temu sama dinamika tveganja zahteva nenehno dopolnjevanje in izboljševanje ukrepov informacijske varnosti.

Varovanje podatkov lahko pomeni oboje, varovanje pred krajo in varovanje pred izgubo. Zaščito pred izgubo podatkov povezujemo z izdelovanjem varnostnih kopij, kar predstavlja popolno podvojitev vseh podatkov na drug elektronski medij.

Varnost, zaupnost, neoporečnost in razpoložljivost poslovnega informacijskega sistema in podatkov je izjemnega pomena za vsakodnevno podporo poslovnim procesom. Nova potreba in izziv povečanja varnosti informacijskih sistemov je elektronsko poslovanje, ki izpostavlja informacijski sistem novim, zahtevnejšim in težko obvladljivim tveganjem. Elementi varnosti pomagajo vzdrževati konkurenčnost, dobre finančne tokove in ugled, skratka visok nivo finančne in poslovne uspešnosti.

Organizirano zlorabljanje svetovnega spleta in novih informacijskih tehnologij postaja gonilo kriminala in kovanja visokih dobičkov, ki jih ustvarjajo kriminalne združbe. Njihovo delovanje je tiho ter široki javnosti navidezno prikrito in ne glasno kot včasih, na primer pri izbruhih škodljivih virusov, ki so polnili stolpce časopisov in ostalih medijev.

Zagotavljanje tajnosti podatkov je ponovno postalo aktualno, ko so se po svetovnem spletu začela pošiljati zaupna sporočila. Vsako poslovanje prek svetovnega spleta zahteva tajnost, celovitost in avtentičnost sporočil. Svetovni splet omogoča zelo hiter prenos velikega števila sporočil, vendar tudi relativno enostavno prestrezanje sporočil. Kot odgovor na to težavo so se razvili šifrirni in dešifrirni sistemi (kriptografski sistemi), katerih osnovna naloga je zagotavljanje tajnosti prenašanega sporočila. Z dodatnimi postopki je mogoče zagotoviti celovitost in avtentičnost sporočil ter preprečitev utaje avtorstva in sprejema sporočila.

V organizacijah se pojavlja neobhodna potreba po vzpostavitvi sistema upravljanja informacijske varnosti. Pri tem se je priporočljivo opreti na dobre prakse in standarde, kot je standard BS 7799, ki določa vse potrebne korake in postopke za vzpostavitev, implementacijo, nadzor ter stalno izboljševanje sistema. Standard med drugim vpeljuje uporabo konsistentnih principov, ki omogočajo sistematičen in celovit pristop k vpeljavi sistema varovanja v podjetje. Bistvo vzpostavitve sistema varovanja ni certificiranje, temveč njegovo delovanje, redno vzdrževanje, spremljanje in izboljševanje.

Kljub dejstvu, da etika kot filozofska disciplina že dolgo obstaja, smo v razvitih delih sveta priča čedalje večjemu pomenu etike, tako na zasebnem kot na poslovnem področju. V primeru informacijske varnosti se etika nanaša na sistem moralnih principov, povezanih s prednostmi in slabostmi določenih dejanj, ter na poštenost in nezakonitost motivov in zaključkov teh dejanj. Zlato etično pravilo se glasi: *Ne stori drugim, kar ne želiš, da drugi storijo tebi*. Pomanjkljivo regulacijo novih, modernih tehnologij nadomeščajo kodeksi računalniške poklicne etike in netikete kot pravila obnašanja na svetovnem spletu. Etični kodeksi so uporabno in priljubljeno sredstvo za zagotavljanje etičnega ravnanja, vendar jih je potrebno uresničevati tudi v praksi, sicer ne uresničijo svojega namena.

Človek je najšibkejši člen v varnostni verigi informacijskega sistema, ni ga mogoče »skonfigurirati«, lahko se le izobražuje, z urjenjem se njegovo obnašanje spravi na neko raven, vendar to ne zagotavlja, da bo vedno ravnal ustrezno. Napadalec išče najšibkejši člen, to pa so v podjetjih običajno tisti ljudje, ki imajo stik s strankami. Navodila, ki jih dobijo zaposleni, so si nasprotujoča: ustreči stranki in z dejanji ne ogroziti varnosti.

Potrebno se je zavedati, da je varnost neprekinjena dejavnost, za katero morajo biti odgovorni vsi zaposleni. Pogosta napaka, ki jo delajo podjetja, je, da varnost podatkov prepuščajo zgolj oddelku informatike. Za varnost nikakor ne more biti odgovorna le določena tehnična funkcija ali oddelek, saj gre za sistematičen proces, ki zadeva celotno organizacijo. Vzroki za delegiranje tako pomembne naloge izvirajo iz prepričanja, da informacijska tehnologija lahko reši vse težave, zato se je potrebno zavedati, da je tehnologijo mogoče uporabiti le za podporo tem postopkom ter da tehnologija sama še ne pomeni varnosti informacij in ni primarni vir nadzora. V praksi se pogosto srečamo z ovirami, kot so nezadostna zavzetost vodstva, neformalni pristopi k organiziranju varovanja, razkorak med dodelitvijo virov in pričakovanji ter odsotnost funkcije neodvisnega preverjanja delovanja in urejanja varnosti v organizacijah.

V praktičnem delu magistrskega dela sem izvedel dve anketi in analiziral odgovore. Iz prve ankete, izvedene med vodji informatike v slovenskih finančnih institucijah, povzemam, da se vodje informatike zavedajo pomembnosti zagotavljanja varnosti informacijskih sistemov, največjo nevarnost pa jim predstavljajo notranji napadalci. Večina vodij informatike ne pripisuje posebnega pomena certificiranju, imajo pa v svojih organizacijah že napisan dokument o varnostni politiki. Vodje informatike ne posvečajo posebne pozornosti etiki, niti ne poznajo etičnega kodeksa Slovenskega društva INFORMATIKA.

Iz druge ankete, izvedene med sodelavci v zavarovalnici, povzemam, da je bil moj osnovni namen, izvedba socialnega inženiringa s ciljem pridobiti uporabniška gesla, uspešen, saj sem pridobil kar 42% uporabniških gesel izmed vseh, ki so anketo izpolnili in vrnili. Med drugim ugotavljam, da se je velik del zaposlenih naučil osnov računalništva na delovnem mestu, večina pa ima doma osebni računalnik ter dostop do svetovnega spleta.

Nameravano izvedbo tretje ankete, socialni inženiring med vseslovensko populacijo, ki uporablja za komuniciranje svoj privatni ali službeni elektronski naslov, sem po pridobitvi več kot deset tisoč elektronskih naslovov prekinil na predlog kriminalistične policije. Ta je sodelovanje pri izvedbi ankete odklonila zaradi več razlogov (eden izmed njih je bila nejasnost, kako naj ravnajo ob prijavi prejemnika elektronske pošte), obenem pa mi odsvetovala izvedbo v lastnem angažmaju.

Razumevanje namena in obsega varnostne politike je zelo različno, njen izgled, vsebina in struktura pa so prepuščeni posameznikom. Pomembno pa je, da je dokument o varnostni politiki zastavljen praktično in je zagotovljena njegova razumljivost.

Z varnostjo se je potrebno spoprijeti na vseh ravneh poslovanja in se ji posvetiti na dnevni ravni. Ključnega pomena so stalni pregledi sistema in njegovo izboljševanje, saj lahko le na ta način zagotavljamo varnost informacijskega sistema v vsakem trenutku, ne glede na spremembe, ki nastajajo v procesih in sredstvih. Ključni dejavnik vpeljave sistema za upravljanje informacijske varnosti so zaposleni, vključno z upravo in vodstvom, ki morajo varnostno politiko sprejeti.

Kako ravnati, kako se obnašati v bodočnosti? Pazljivo, pazljivo in še enkrat pazljivo prav na vsakem koraku, v vsakem trenutku, v vsaki situaciji. Do svetovnega spleta (in obratno) je možno iz vsake slovenske vasi, mesta, skoraj iz vsakega kotička na naši Zemlji.

Nepridipravov, zlonamernežev, kriminalcev ali pa konec koncev zgolj naključnih radovednih računalniških zanesenjakov pa mrgoli in prav vsi imajo enkratno ter univerzalno znanje in orožje na dosegu miške.

Literatura

1. Arthurs Wendy: A Proactiv Defence to Social Engineering. SANS Institute. [URL:http://www.sans.org/infosecFAQ/social/defence.htm], 2.8.2001.
2. Bace Gurley Rebecca: Vulnerability Assessment and Intrusion Detection Systems. Bosworth Semour, Kabay M. E.: Computer Security Handbook, Fourth Edition. Canada: John Wiley & Sons, Inc, 2002, str. 37.1–37.16.
3. Baloh Peter, Indihar Štemberger Mojca, Vrečar Peter: Poslovna informatika – dodatno študijsko gradivo, naloge in vodnik po predmetu. Ljubljana: Ekonomska fakulteta, 2002. 121 str.
4. Bezlaj Peter: Vrednotenja finančnih institucij s poudarkom na posebnostih vrednotenja poslovnih bank. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 2006. 94 str.
5. Bosworth Semour, Jacobson V. Robert: Brief History and Mission of Information System Security. Bosworth Semour, Kabay M. E.: Computer Security Handbook, Fourth Edition. Canada: John Wiley & Sons, Inc, 2002, str. 1.1–1.13.
6. Bratuša Tomaž: Grožnje spletnemu bančništvu. Ljubljana: Moj Mikro, 22(2006), 4, str. 38–44.
7. Bratuša Tomaž: Napadi na omrežja WLAN. Ljubljana: Moj Mikro, 22(2006), 5, str. 38–41.
8. Bratuša Tomaž: Vdori v brezžično omrežje v praksi. Ljubljana: Moj Mikro, 22(2006), 5, str. 41–42.
9. Brenner Susan: The Psychology of Social Engineering. [URL:http://www.cybercrimes.net/property/Hacking/Social%20Engineering/PsychsocEng/PsySocEng.html], 5.7.1997.
10. Brezavšček Alenka, Zupan Lucija: Standardi in priporočila na področju informacijske varnosti. Portorož: Zbornik posvetovanja, Dnevi slovenske informatike 2006, 2006. 6 str.
11. Cuadra de la Fernardo: Socialni inženiring. [URL:http://www.386tele.com/sections.php?op=viewarticle&artid=60], 21.4.2006.
12. Damij Talib: Poslovna informatika. Ljubljana: Ekonomska fakulteta, 2004. 204 str.
13. Damodaran Aswath: Valuing financial Service Firms. [URL:http://www.stern.nyu.edu/~adamodar/pdfiles/papers/finfirm.pdf],2001. 44 str.
14. Djurdjič Vladimir: Izhod v sili. Ljubljana: Sistem, 12(2004), str. 13–15.
15. Donaldson John: Business Ethics: European Casebook. London: Academic Press Limited, 1992. 293. str.
16. Egan Mark, Mather Tim: Varnost informacij: grožnje, izzivi in rešitve: Vodnik za podjetja. Ljubljana: Pasadena, 2005. 269 str.
17. Frangež Zdenko: Škodljivci na pohodu. Ljubljana: Moj Mikro, 22(2006), 4, str. 48-52.
18. Fürst Maria, Halmer Nikolaus: Filozofija. Ljubljana: Državna založba Slovenije, 1990. 198 str.
19. Gradišar Miro: Uvod v informatiko. Ljubljana: Ekonomska fakulteta, 2003. 516 str.

20. Gradišar Miro, Resonovič Gortan: Informatika v poslovnem okolju. Ljubljana: Ekonomska fakulteta, 2001. 508 str.
21. Granger Sarah: Social Ingeneering Fundamentals, Part1: Hacker Tactics. [URL:http://www.securityfocus.com/infocus/1527], 18.12.2001, str. 1-7.
22. Gričar Jože: Elektronsko poslovanje: priložnost za gospodarske družbe, državno upravo in potrošnike. Ljubljana: Uporabna informatika 5(1997), 2, str. 7-12.
23. Groznik Aleš: Stanje poslovne informatike v Sloveniji. Ljubljana: Ekonomska fakulteta, Inštitut za poslovno informatiko, 2007.
24. Groznik Aleš, Lindič Jaka: Elektronsko poslovanje. Ljubljana: Ekonomska fakulteta, 2007. 85 str.
25. Groznik Aleš, Vičič Dejan: Vrednost in pomen informatike v podjetju. Zbornik posvetovanja DNEVI SLOVENSKE INFORMATIKE 2005. Ljubljana: Slovensko društvo INFORMATIKA, 2005, str. 218-224.
26. Harley David, Lee Andrew: The Root of All Evil? – Rootkits Revealed. U.S.A: Small Blue – Green World, 2006. 17 str.
27. Hunton James E. et al.: Core Concepts Of Information Technology Auditing. John Wiley & Sons, 2004. 496 str.
28. Jerman Blažič Borka et al.: Elektronsko poslovanje na internetu. Ljubljana: Gospodarski vestnik, 2001. 206 str.
29. Justin Tomaž: Varno od daleč. Ljubljana: Sistem, 3(2007), str. 12–13.
30. Ključevšek Rado, Vodopivec Tadej, Dolinar Peter: Obvladovanje varnosti informacij v skladu s standardom BS 7799. Ljubljana: SIQ, 2001. 45 str.
31. Krisper Marjan: Kodeks etike in strokovna odgovornost informatikov. Ljubljana: Uporabna informatika, 6(1998), 2, str. 5-10.
32. Kwok Lam-for, Longley Dennis: Information Security Management and Modeling. USA: MCB University Press: Information Management & Computer Security, 1999, str. 30-39.
33. Levine Diane E. et al.: Denial of Service Attacks. Bosworth Semour, Kabay M. E.: Computer Security Handbook, Fourth Edition. Canada: John Wiley & Sons, Inc, 2002, str. 11.1–11.26.
34. Linderman Landon James: Ethical Decision Making And High Tehnology. Bosworth Semour, Kabay M. E.: Computer Security Handbook, Fourth Edition. Canada: John Wiley & Sons, Inc, 2002, str. 30.1–30.8.
35. Lipovec Filip: Razvita teorija organizacije. Ljubljana: Univeza v Ljubljani. Ekonomska fakulteta, 1997. 355 str.
36. Mitnick Kevin D., Simon William L., Wozniak Steve: The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2002. 336 str.
37. Nash Laura: A Managers Guide to Resolving Ethical Problems. Boston: Harvard Business School Press, 1990. 259 str.
38. Norberg Stefan: Securing Windows NT/2000 Servers for the Internet. Sebastopol: O'Reilly & Associates, Inc., 2001. 199 str.

39. Overly Michael R.: E-policy: How to Develop Computer, E-mail, and Internet. Guidelines to Protect Your Company and Its Assets. USA: SciTech Publishing, Inc., 1999. 146 str.
40. Pahor David, Drobnič Matija: Leksikon računalništva in informatike. Ljubljana: Pasadena, 2002. 786 str.
41. Panian Željko: Kontrola i revizija informacijskih sustava. Zagreb : Sinergija nakladništvo d.o.o., 2001. 343 str.
42. Peltier Thomas R.: Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. USA: CRC Press LLC, 2002. 297 str.
43. Pivec Franci: Zasebnost in internet. Ljubljana: Uporabna informatika, 8(2000), 3, str. 137-145.
44. Pivec Franci: H konceptualizaciji informacijske etike. [URL:http://www.drustvo-informatika.si/dogodki/arhiv/dsi2001/sekcija-g/pivec.doc], 2001.
45. Pivec Franci: Revizija etičnega kodeksa informatikov. [URL:http://www.drustvo-informatika.si/dogodki//dsi2002/prispeliReferati/pivec.doc], 2002.
46. Preston Gralla: Zvijače za Windows XP. Ljubljana: Pasadena, 2004. 417 str.
47. Ribnikar Ivan: Denarni sistem in denarna teorija, I. del. Ljubljana: Ekonomska fakulteta, 1993. 336 str.
48. Ribnikar Ivan: Finančne institucije. Ljubljana: Bančni vestnik, 12(1996), str. 43-45.
49. Rogerson Simon: The Information Society. [URL:http://www.ccsr.cse.dmu.ac.uk/resources/general, ethicol/Ecv11no3.html], 2001.
50. Sanderson Ethan, Forcht Karen A.: Information Security in Business Environment. USA: MCB University Press: Information Management & Computer Security, 1996, str. 32-37.
51. Sandhu Ravi: Identification and Authentication. Bosworth Semour, Kabay M. E.: Computer Security Handbook, Fourth Edition. Canada: John Wiley & Sons, Inc, 2002, str. 16.1–16.16.
52. Saunders Anthony, Cornett Millon Marcia: Financial Institutions Management: A Risk Management Approach. Boston: McGraw-Hill Education, 2005. 856 str.
53. Savanović Damir: Pet nalog informacijske varnosti. Ljubljana: Sistem, 3(2007), str. 10–11.
54. Schlamberger Niko: Nadračunalništvo in varno poslovanje. Ljubljana: Uporabna informatika, 5(1997), 3, str. 38-39.
55. Sluga Marko: Varno po internetu. Ljubljana: ADD, IT Solutions, 2005. 42 str.
56. Sruk Vlado: Leksikon morala in etika. Ljubljana: Cankarjeva založba, 1986. 521 str.
57. Strosar Edi: Gospodarji prstana. Ljubljana: Monitor, 17(2007), 3, str. 100–103.
58. Sušnik Matjaž: Pravna odgovornost informatikov. Ljubljana: Sistem, 4(2006), str. 24-25.

59. Šinigoj Aleksander: Krizni management - upravljanje informacijsko – varnostnih nesreč. Zbornik posvetovanja DNEVI SLOVENSKE INFORMATIKE 2005. Ljubljana: Slovensko društvo INFORMATIKA, 2005, str. 411-416.
60. Tavčar Mitja: Management. Radovljica: Didakta, 1994. 1072 str.
61. Tulloch Mitch: Microsoft Encyclopedia of Security. Redmond, Washington: Microsoft Press, A Division of Microsoft Corporation, 2003. 449 str.
62. Tulloch Mitch: Zvijače za Windows server. Ljubljana: Pasadena, 2005. 403 str.
63. Wood Cresson Charles: A Secure Password Storage Policy. USA: MCB University Press: Information Management & Computer Security, 1997, str. 79-80.
64. Zimšek Andrej: Varno in učinkovito elektronsko poslovanje. Ljubljana: Uporabna informatika, 8(2000), 1, str. 47-51.
65. Zupan Lucija: Zahteve za uspešno vpeljavo standarda BS7799-2 za področje informacijske varnosti. Ljubljana: Uporabna informatika, 13(2005), 1, str. 37-50.
66. Žnidar Borut: Organizirajte napad. Ljubljana: Sistem, 5(2006), str. 18–19.
67. Žurman Darko: Premajhna zavest o informacijski varnosti. Ljubljana: Sistem, 1(2005), str. 6-7.

Viri

1. 2006 Global Security Survey. [URL:http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf], junij 2006.
2. British Standard BS ISO/IEC 17799:2005: Slovenski prevod standarda, Information Tehnology, Security Techniques, Code of Practise for Information Security Management. Nova Gorica: Palsit, junij 2005. 299 str.
3. British Standard BS ISO/IEC 17799:2000: Information Tehnology, Code of Practise for Information Security Management. Geneva: ISO Copyright Office, 2000. 71 str.
4. Information Security Policy Manual. Connecticut, USA: Rohstein Associates Inc., 2000.
5. Kazenski zakonik Republike Slovenije. [URL:http://www.ius-software.si/Baze/REGI/Zakoni/B/Z94877BZ.htm], 26.9.2007.
6. Priporočila za varno uporabo storitev spletne banke. Ljubljana: Združenje bank Slovenije, 2007. 12 str.
7. Računalniške novice. Ljubljana: 3/XII (2007). str. 17.
8. Računalniške novice. Ljubljana: 3/XII (2007). str. 32.
9. SirRoss: A Guide to Social Engineering. [URL:http://www.altavista.com/index.php?section=directory&cmd=detail&id=3487) A_Guide_to_Social_Engineering], 20.1.2005.
10. SKB banka d.d., Sektor IBT: Varen elektronski prenos podatkov med podjetji in SKB banko, delovno navodilo. Ljubljana, januar 2005. 20 str.

11. Slovenski standard PSIST BS 7799: Kodeks varovanja informacij(identičen BS 7799:1995). Ljubljana: Urad Republike Slovenije za standardizacijo in meroslovje pri Ministrstvu za znanost in tehnologijo, 2006. 135 str.
12. Spletna stran Governmentsecurity. [URL:http://www.governmentsecurity.org/arhive/t10264.html], 14.2.2007.
13. Spletna stran Snoopstick. [URL:http://www.snoopstick.com.htm], 23.2.2007.
14. Zalaznik Janez: Uporabnik NLB Klika: Pobrali so mi 770 tisočakov. Ljubljana: Dnevnik, 10.11.2006.

Priloga 1: Slovarček slovenskih prevodov tujih izrazov

Accounting - vodenje računov
Administrator - skrbnik, upravljalec računov
Advancement - napredovanje
Adwertising Software (Adware) - reklamni programi
Aplication Programming Interface (API) - vmesnik uporabniškega programa
Attachment - priponka
Authentication - preverjanje pristnosti
Authorisation - pooblaščanje
Back Door - zadnja vrata
Backup - varnostno kopiranje
Bandwith Consumption - zasedanje pasovne širine
Basic Input-Output System (BIOS) - temeljni vhodno-izodni sistem
Blended - mešan
Blind test - slepo testiranje
Blog - novičarstvo
Bona Fide - v dobri veri, odkritosrčno
Bot - skupina
British Standard (BS) - britanski standard
Buffer Owerflow - prekoračitev pomnilnika
Business to Business (B2B) - med podjetji
Business to Consumer (B2C) - med podjetji in potrošniki
Business to Government (B2G) - med podjetji in javno oziroma državno upravo
Chief Information Officer (CIO) - vodja informatike
Cleanup - čiščenje
Compact Disc (CD) - kompaktna plošča
Conformity - podobnost
Consumer to Consumer (C2C) - med potrošniki
Consumer to Government (C2G) - med državljani in javno oziroma državno upravo
Cookie - piškotek
Core Wars - jedro vojn
Customer Relationship Management (CRM) - upravljanje odnosov s strankami
Cyber - kibernetični
Data Mining - podatkovno rudarjenje
Database Administrator - skrbnik baze podatkov
Destructive Devices - uničevanje naprav
Dialer - klicalec
Distributed Denial of Dervices Attack (DDoS attack) - distribuiran napad za zavrnitev storitve
Domain - skupina računalnikov v omrežju z enakimi varnostnimi ukrepi
Downloader - prenešenec
DRM - Sonyjev protikopirni zaščitni sistem

Dumpster Diving (Trashing) - brskanje po smeteh
E-mail Bombing - bombandiranje z elektronsko pošto
Enterprice Resources Planning (ERP) - celovite programske rešitve
Firewall - požarni zid
Gaining a Toehold - noga med vrati
Government to Government (G2G) - znotraj javne oziroma državne uprave
Hacker - heker
Help Desks - službe servisne pomoči
HEX - šestnajstiški zapis števila
Hoax: potegavščina
Impersonate - izdajati se za koga drugega
Information Security - celovitost informacije
Information Security Officer - varnostni inženir
Information Technology (IT) - informacijska tehnologija
Internet - svetovni splet
Internet Protokol (IP) - internetni protokol za prenos podatkovnih paketov
Internet Relay Chat (IRC) - klepetanje po internetu
Intrusion Detection Systems - sistemi za zaznavanje vdorov
Kernel Level Rootkit - raven jedra operacijskega sistema
Library Rootkits - knjižnični korenski kompleti
Listening Phase: faza prisluškovanja
Malicious Software (Malware) - škodljivi programi
Man In The Middle Attack (MITM Attack) - napadalec med žrtvijo in žrtvino tarčo
My Login - moje uporabniško ime
My Password - moje geslo
Netiquette - etika spletnega obnašanja
Online - v živo
Outsourcing: zunanje izvajanje
Penetration Test: penetracijski test
Phishing - spletno ribarjenje
Ping-of-Death - napad smrti
Plan-Do-Check-Act - načrtuj-izvedi-preveri-ukrepaj
Policy - pravilnik
Port - vrata
Probe and Attack - preizkus in napad
Proxy Server - namestniški strežnik
Rabbits - zajčki
Reconnaissance - analiza okolja
Reset - vnovična nastavitev
Resource Starvation - zasedanje vseh vrst virov
Restore - obnova
Rootkit - korenski komplet

Router - usmerjevalnik
Router Attacks - napadi na usmerjevalnike
Routing and Domain Name System Attacks - sistemski napadi na domenske strežnike
Secure Sockets Layer (SSL) - plast varnih vtičnic (protokol za varno izmenjavo dokumentov)
Social Engineering - družbeni ali socialni inženiring
Spam - e-slama, nezaželena elektronska pošta
Spying Software (Spyware) - vohunski programi
Statefull Inspection - nadzor suverenosti
Stealth Phase - faza prikrivanja
SYN Flooding - poplavljanje sinhronizacij
Takeover - prevzem
The Christmass Tree Worm - črv Božično drevo
Uniform Resource Locator (URL) - enolični krajevnik vira
Universal Serial Bus (USB) - vsestransko zaporedno vodilo
Virtual Private Network (VPN) - navidezno zasebno omrežje
VoIP (Voice over IP) - internetna telefonija
Vulnerability Scanning - preverjanje ranljivosti
What you are - kaj si
What you do - kaj delaš
What you have - kaj imaš
What you know - kaj znaš
Windows Explorer - raziskovalec Oken
Zombie - zombi, računalnik, nad katerim je bil prevzet oddaljen nadzor, brez vednosti lastnika

Priloga 2: Anketni vprašalnik za vodje informatike

ANKETNI VPRAŠALNIK za vodje informatike

1. **Imate v podjetju napisano varnostno politiko za informacijski sistem?**

DA	NE	je v pripravi	ne želim odgovarjati
□	□	□	□

2. **Če imate v podjetju napisano varnostno politiko za informacijski sistem, ali jo tudi izvajate?**

DA	NE	je v pripravi	ne želim odgovarjati
□	□	□	□

3. **Lahko na kratko opišete, kako poteka nadzor nad izvajanjem varnostne politike, če jo izvajate?**

4. **Kdo menite, so za varnost IS v organizaciji na splošno najbolj nevarni?**

□	zunanji napadalci(hackerji, crackerji,…)
□	notranji napadalci(zaposleni, študentje,…)
□	drugo:
□	ne želim odgovarjati

5. **Ste se v podjetju že srečali s hujšo težavo oz. poskusom vdora ali vdora v IS?**

DA	NE	ne želim odgovarjati	drugo:
□	□	□	□

6. **V podjetju vam težave pri varovanju IS povzročajo**

	malo težav	srednje težav	veliko težav
virusi, črvi, tempirane bombe	□	□	□
spam, phishing	□	□	□
rootkits	□	□	□
aktivni napadi z interneta(hackerji,..)	□	□	□
poskusi notranjih napadov	□	□	□
kraja podatkov s strani zaposlenih	□	□	□
drugo	□	□	□

7. **Ste v podjetju preventivno že izvajali simuliran vdor (penetracijski test)?**

da, izvajamo ga redno	□
da, izvajamo ga občasno, po potrebi	□
ne, nismo ga še izvedli	□

smo v pripravi na izvedbo	□
drugo	□
ne želim odgovarjati	□

8. Če ste penetracijski test izvedli, kdo je bil izvajalec?

□	zunanji neodvisni izvajalec
□	podjetje, ki nam vzdržuje, svetuje pri izgradnji in varnosti IS
□	sami, zaposleni administratorji, inženirji,..
□	drugo:
□	ne želim odgovarjati

9. V podjetju imate pridobljenega enega od certifikatov (BS 7799, ISO/IEC 17799 ,…)?

DA □ NE □ je v pripravi □ ne želim odgovarjati □ drugo: □

10. Ocenite prosim pomembnost certificiranja (1-nepomembno, 5-zelo pomembno).

1	2	3	4	5
□	□	□	□	□

11. Lahko na kratko napišete, zakaj ste se oz. zakaj bi se odločili za certificiranje?

12. Ali imate v podjetju izdelan načrt neprekinjenega poslovanja?

DA □ NE □ je v pripravi □ da, a ga ne izvajamo □ ne želim odgovarjati □

13. V podjetju imate vsaj enega zaposlenega, ki se ukvarja izključno samo z varnostjo (IS)?

DA □ NE □ ne želim odgovarjati □ drugo: □

14. So vsi zaposleni v podjetju seznanjeni z varnostnimi mehanizmi za varovanje IS?

DA □ NE □ ne želim odgovarjati □ drugo: □

15. So vsi zaposleni v podjetju podpisali izjavo za kazensko odgovornost v primeru kršitve pravilnika za varovanje informacij?

DA □ NE □ ne želim odgovarjati □ nimamo pravilnika □ drugo: □

16. V podjetju redno oz. po potrebi seznanjate, obveščate ali izobražujete zaposlene o nevarnostih, ki pretijo IS?

DA NE ne želim odgovarjati drugo:
□ □ □ □

17. Ste se v podjetju že srečali s poskusom socialnega inženiringa?

DA NE ne želim odgovarjati drugo:
□ □ □ □

18. Ste kot vodja službe za informatiko v vašem podjetju tudi član uprave?

DA NE ne želim odgovarjati
□ □ □

19. Vam je kdorkoli od zaposlenih že kdaj zaupal svoje geslo?

DA NE ne želim odgovarjati
□ □ □

20. Vam je kdorkoli od članov uprave že kdaj zaupal svoje geslo?

DA NE ne želim odgovarjati
□ □ □

21. Poznate Kodeks etike Slovenskega društva informatike?

DA NE ne želim odgovarjati drugo:
□ □ □ □

22. Ali ima vaše podjetje pisno opredeljen etični kodeks?

DA NE je v pripravi ne želim odgovarjati drugo:
□ □ □ □ □

23. Če ima vaše podjetje pisno opredeljen etični kodeks, ali zajema tudi informatiko?

DA NE je v pripravi ne želim odgovarjati drugo:
□ □ □ □ □

24. Komu bi sporočili primer neetičnega ravnanja in kako bi ravnali v takem primeru?

25. Ste v spletni trgovini že kadarkoli karkoli kupili ?

DA NE ne želim odgovarjati drugo:
□ □ □ □

Osebni podatki:

26. Spol

M Ž
□ □

27. Starost

20-29	30-39	40-49	50-59	60+
□	□	□	□	□

28. Dosežena stopnja vaše izobrazbe

□	srednja šola (V)
□	višja šola (VI)
□	visokošolska izobrazba
□	univerzitetna izobrazba
□	magisterij, doktorat

29. V podjetju ste zaposleni

□	manj kot eno leto
□	več kot 1 leto in manj kot 3 leta
□	več kot 3 leta in manj kot 5 let
□	več kot 5 let

30. Vaše mnenje, pripombe, če želite karkoli dodati, pojasniti,…

Spoštovani, za izpolnjen in vrnjen anketni vprašalnik se vam najlepše zahvaljujem ter vam želim uspešno in predvsem varno poslovanje.

Jernej Pečnik

Priloga 3: Anketni vprašalnik za zaposlene v zavarovalnici

ANKETNI VPRAŠALNIK za zaposlene v zavarovalnici

1. **Udeležil sem se že vsaj enega tečaja ali seminarja na kakršnokoli temo iz računalništva (v sklopu šole, službe, privat,…).**

DA	NE
□	□

2. **Dela z računalniškim orodjem oz. programom sem se naučil**

	doma	**v šoli**	**v službi**	**drugje**	**ne poznam**
MS Windows	□	□	□	□	□
MS Word	□	□	□	□	□
MS Excel	□	□	□	□	□
MS PowerPoint	□	□	□	□	□
MS Outlook	□	□	□	□	□
Internet Explorer	□	□	□	□	□
NLB Proklik	□	□	□	□	□
TIS	□	□	□	□	□
Symass	□	□	□	□	□
Acrobat Reader	□	□	□	□	□
AdAware	□	□	□	□	□
VNC	□	□	□	□	□
ZIP	□	□	□	□	□
RAR	□	□	□	□	□

3. **Uporaba računalniških orodij in programov mi je bila ob prihodu na delovno mesto razložena in prikazana v skladu z mojimi potrebami.**

se strinjam	se ne strinjam	drugo
□	□	□

4. **Ob zaposlitvi mi je bila nazorno prikazana in razložena tudi**

	se strinjam	se ne strinjam	drugo
organizacija informacijskega sistema	□	□	□
varnost informacijskega sistema	□	□	□
delovanje informacijskega sistema	□	□	□

5. **Ob zaposlitvi (ali naknadno) sem bil seznanjen s sankcijami neupoštevanja pravil.**

se strinjam	se ne strinjam	drugo
□	□	□

6. **V podjetju oz. oddelku imamo sestanke (redno/občasno), ki so namenjeni informiranju zaposlenih.**

se strinjam	se ne strinjam	drugo
□	□	□

7. **Tudi v prostem času se zanimam za računalništvo.**

sploh ne	malo	srednje	zelo se zanimam
□	□	□	□

8. **Doma imam svoj računalnik.**

DA □ NE □ vsi domači uporabljamo en računalnik □

9. **Redno ali občasno doma zračunalnikom dokončam službeno zadevo (izdelava wordovega dokumenta, exelove tabele, PP prezentacije, ipd.)**

DA □ NE □ drugo □

10. **Doma imam dostop do interneta.**

DA □ NE □

11. **Znanje računalništva, ki sem ga pridobil na delovnem mestu, mi koristijo tudi v privatnem življenju.**

sploh ne	malo	srednje	povsem se strinjam
□	□	□	□

12. **Ime domene, v katero se prijavljam na delovnem mestu:**

13. **Uporabniško ime, ki ga uporabljam za prijavo v sistem na delovnem mestu:**

14. **Geslo, ki ga uporabljam za prijavo v sistem na delovnem mestu:**

15. **Na delovnem mestu imam dostop do interneta.**

DA □ NE □

16. **Vsaj enkrat (v službi ali doma) sem obiskal spletno trgovino in tudi nekaj kupil.**

DA □ NE □ spletno trgovino sem samo obiskal □

17. **Položnice plačujem preko interneta.**

redno □ nikoli □ občasno □

18. **Slišal sem že za naslednje pojme**

	da	ne
Moj Mikro	□	□
Trend Micro	□	□
Bil Gates	□	□

SAP	□	□
DNS	□	□
WINS	□	□
IP	□	□
konsolidacija	□	□
virtualizacija	□	□
CISCO	□	□
rooter	□	□
rootkits	□	□
script kiddies	□	□
procesni inženiring	□	□
socialni inženiring	□	□
CIO	□	□
CIA	□	□
MITM attack	□	□
MITY attachment	□	□

Moji osebni podatki:

19. Spol

M	Ž
□	□

20. Starost

20-29	30-39	40-49	50-59	60+
□	□	□	□	□

21. Dosežena stopnja izobrazbe

□	srednja šola (V)
□	višja šola (VI)
□	visokošolska izobrazba
□	univerzitetna izobrazba
□	magisterij

22. V tej zavarovalnici sem zaposlen

□	manj kot eno leto
□	več kot 1 leto in manj kot 3 let
□	več kot 3 leta in manj kot 5 let
□	več kot 5 let

23. Morebitne pripombe, mnenja, komentar na anketni vprašalnik, drugo …

Za izpolnjen in vrnjen anketni vprašalnik se vam najlepše zahvaljujem.
Jernej Pečnik