UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jure Dokl
Mentor: redni profesor dr. Marjan Malešič
Somentor: asistent dr. Uroš Svete

INTERNET IN KONCEPT ČLOVEKOVE VARNOSTI

Diplomsko delo

Ljubljana, 2006

ZAHVALA

Iskrena hvala staršem za tople besede in izkazano ljubezen ter bratu in sestrama za podporo in razumevanje. Hvala tudi vsem prijateljem, ki so me spremljali na študijski poti in mi tako polepšali mladostne dni.

Hvala somentorju dr. Urošu Svetetu in mentorju dr. Marjanu Malešiču za vzpodbudne besede, podporo in usmeritve pri pisanju diplomske naloge.

KAZALO

ZAHVALA I
KAZALO 1
SEZNAM TABEL 2
SEZNAM SLIK 2
SEZNAM KRATIC IN SLOVARČEK 3
1. UVOD 6
2. METODOLOŠKI OKVIR 8
2.1. Namen in cilj preučevanja 8
2.2. Hipoteze 8
2.3. Pristop in temeljne uporabljene metode dela 8
2.4. Struktura analize 9
3. TEMELJNI POJMI IN KONCEPTI 10
3.1. Sodobna varnostna paradigma 10
3.2. Koncept človekove varnosti 12
3.3. Informacijska varnost 15
3.4. Informacijsko vojskovanje 18
4. INTERNET IN VARNOST POSAMEZNIKA 25
4.1. Nevarnosti in grožnje 25
4.1.1. Namerne grožnje 26
4.1.1.1. Zahrbtni programi 26
4.1.1.2. Prevare, sleparije 41
4.1.1.3. Lovljenje gesel 46
4.1.1.4. Elektronsko vohljanje 46
4.1.1.5. Zasipanje z neželeno pošto 50
4.1.1.6. Nepooblaščene spremembe in vdori 52
4.1.2. Nenamerne grožnje 53
4.1.3. Fizične grožnje 54
4.2. Zaščita in protiukrepi 54

5. ZAKLJUČEK 58
5.1. Preverjanje hipotez 58
5.2. Sklep 60
6. VIRI IN LITERATURA 62
6.1. Monografije 62
6.2. Članki v znanstvenih in strokovnih publikacijah 64
6.3. Poglavja iz zbornikov 64
6.4. Enciklopedije in leksikoni 64
6.5. Baze podatkov in raziskave 65
6.6. Internetne strani 65

SEZNAM TABEL

Tabela 1: Razširjeni koncepti obravnavanja varnosti 11
Tabela 2: Oblike ogrožanja informacijske varnosti 18
Tabela 3: Različne značilnosti zlonamernih programov 32

SEZNAM SLIK

Slika 1: Informacijsko vojskovanje 24
Slika 2: Prikaz porasta trojanskih konjev 32
Slika 3: Prikaz upada virusov in črvov 33
Slika 4: Prikaz porasta drugih zlonamernih programov 33
Slika 5: Primer poplave spyware-a 39
Slika 6: Porast poneverbe internetnih strani v zadnjem letu 45

SEZNAM KRATIC IN SLOVARČEK

- AFCERT – "**A**ir **F**orce **C**omputer **E**mergency **R**esponse **T**eam", odzivna skupina zračnih sil za računalniške nevarnosti
- ASCII – ang. **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange, akronim za kodo, ki predstavlja vse standardne angleške znake kot številke, kjer ima vsak znak določeno številko od 0 do 127. Tovrstno kodiranje je dobrodošlo predvsem zaradi lažje izmenjave tekstov med različnimi računalniki.
- BIT – ang. **BI**nary digi**T** - osnovna enota za merjenje informacij, bit je tista informacija, s katero dobimo odgovor na vprašanje, na katerega sta mogoča dva enako verjetna odgovora (DA=1 / NE = 0), seveda v binarnem matematičnem sistemu
- BitTorrent – ime protokola, ki omogoča izmenjavo datotek preko interneta avtorja Bram Cohena, namen tega protokola je široka distribucija velikih količin podatkov brez nepotrebne porabe dragocenih pasovnih širin in serverjevih zmogljivosti; lahko tudi program za prenašanje *.torrent* datotek
- BLOG – ang. we**B LOG** – spletni dnevnik
- Byte – 8 BITov
- C2W – ang. **C**ommand-and-**C**ontrol **W**arfare, akronim za bojevanje na poveljniško-nadzornem področu
- C3I – ang. **C**ommand, **C**ontrol, **C**ommunications and **I**ntelligence, akronim za poveljevanje, nadzor, komunikacije in obveščevalno dejavnost
- C4I – ang. **C**ommand, **C**ontrol, **C**ommunications, **C**omputers and **I**ntelligence, akronim za poveljevanje, nadzor, komunikacije, računalnike in obveščevalno dejavnost
- C4ISR – ang. **C**ommand, **C**ontrol, **C**ommunications, **C**omputers, **I**ntelligence, Surveillance and Reconnaissance, akronim za poveljevanje, nadzor, komunikacije, računalnike, obveščevalno dejavnost, nadzorstvo in izvidništvo
- CERT – ang. **C**omputer **E**mergency **R**esponse **T**eam, odzivna skupina za računalniške nevarnosti
- Cookie - piškotek je poseben (enkraten) identifikator v računalniku, ki ga spletna aplikacija pošlje obiskovalcu. Piškotek omogoča spletni strani, da si zapomni informacije o obiskovalčevih prejšnjih aktivnostih. Tako zbrani podatki omogočajo urednikom spletnih aplikacij, da lahko oblikujejo ponudbo po obiskovalčevih željah. Piškotki se uporabljajo tudi za to, da obiskovalcu pri ponovnem obisku, naročilu ipd. ni potrebno znova posredovati osebnih podatkov.
- CPU – ang. **C**entral **P**rocessing **U**nit – glavna procesna enota, procesor

- CYBERSPACE – internet; kibernetski prostor; globalno omrežje med seboj povezanih računalnikov in komunikacijskih sistemov; imaginarno okolje v katerem se prenašajo digitalizirane informacije prek računalniških omrežij
- CYBERWAR – spopad v virtualni sferi: sinonim za informacijsko vojskovanje (RAND); lahko tudi sinonim za netwar
- DoS – "**D**enial **o**f **S**ervice", zatajitev delovanja, zavrnitev storitve; lahko tudi "**D**isk **O**perating **S**ystem" - DOS
- DSL – ang. **D**igital **S**ubscriber **L**ine, digitalni naročniški vod
- e.g. - lat. "exempli gratia", na primer
- etc. – lat. "et cetera", in tako dalje
- Freeware – ang. **FREE** soft**WARE**, brezplačni programi, ki jih je mogoče naložiti iz interneta; čeprav so brezplačni avtor ohrani avtorske pravice in uporabnik lahko program le uporablja, ne pa tudi (pre)prodaja
- GB – ang. **G**iga**B**yte, pomeni 1024 MB ali 1.073.741.824 Bytov, ali 2^{30} Bytov
- HTML – ang. **H**yper **T**ext **M**arkup **L**anguage, spletni jezik, ki se uporablja za izdelavo dokumentov za uporabo na internetu
- i.e. – lat. "id est", to je
- IASIW – "**I**nstitute for **A**dvanced **S**tudy of **I**nformation **W**arfare", inštitut za višje študije informacijskega vojskovanja
- IKT – **I**nformacijsko **K**omunikacijske **T**ehnologije
- INFOSEC – "**INFO**rmation **SEC**urity", akronim za informacijsko varnost; zaščita zaupnih podatkov, ki je shranjena na računalnikih ali prenesena preko kateregakoli medija
- INTERNET - svetovno računalniško omrežje v katerega so povezana manjša in večja lokalna omrežja; globalno omrežje med seboj povezanih vladnih, univerzitetnih, šolskih, komercialnih, zasebnih in drugih omrežij, kjer se med računalniki pretakajo podatki na enak način po posebej dogovorjenem protokolu, ki se imenuje TCP/IP
- IP številka – ang. **I**nternet **P**rotocol Number, identifikacijska številka računalnika ali usmerjevalnika priključenega v medmrežje, oba jo nujno potrebujeta za dostop na internet
- ISP – ang. **I**nternet **S**ervice **P**rovider, dobavitelj/ponudnik internetne povezave, lahko tudi IAP – **I**nternet **A**ccess **P**rovider
- IW – ang. **I**nformation **W**arfare, informacijsko vojskovanje (IV)
- JPG – ang. **J**oint **P**hotographic Expert **G**roup, združena fotografska skupina strokovnjakov, kratica se uporablja za tehniko stiskanja velikosti slikovnih datotek za hitrejšo spletno uporabo
- kB – ang. **k**ilo**B**yte, pomeni 1024 Bytov, ali 2^{10} Bytov

- LIC – ang. **L**ow **I**ntensity **C**onflict, spopad nizke intenzivnosti
- MALWARE – ang. **MAL**icious soft**WARE**, zlonamerni programi
- MB – ang. **M**ega**B**yte, pomeni 1024 kB ali 1.048.576 Bytov ali 2^{20} Bytov
- NETWAR – omrežno bojevanje, ki obsega socialno, politično, ekonomsko in vojaško obliko konflikta, predvsem LIC in OOTW
- NSA – ang. **N**ational **S**ecurity **A**gency, državna varnostna agencija, ki ima prednostne naloge za nadzorovanje vseh vrst komunikacij znotraj in izven ZDA; ustanovljena je bila v povojnem obdobju in je plod Trumanove administracije
- OOTW – ang. **O**perations **O**ther **T**han **W**ar, operacije drugačne od vojne
- P2P – ang. **P**eer to **P**eer - uporabnik do uporabnika; okrajšava, ki se pretežno uporablja za oznako računalniških programov, ki so namenjeni izmenjavi datotek preko interneta
- PSYOPS – ang. **PSY**hological **OP**eartion**S,** psihološke operacije, načrtovane aktivnosti, ki so v miru ali vojni usmerjene proti nasprotniku, domači ali tuji javnosti, z namenom vplivanja na njihov odnos in vedenje, ki vpliva na doseganje določenih vojaških ali političnih ciljev
- RAND – ameriška korporacija, ang. **R**esearch **an**d **D**evelopment
- Shareware – ang. **SHAR**ing soft**WARE**, brezplačni programi za določeno obdobje, ki jih je mogoče naložiti iz interneta, vendar jih je potrebno po nekem pretečenem obdobju registrirati ali kupiti, sicer prenehajo delovati; uporablja se tudi rek "try before you buy" – preizkusi preden kupiš
- TCP/IP – ang. **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol, način prenosa podatkov, ki se uporablja na internetu
- torrent – deroč tok, izliv; beseda se v P2P okolju uporablja kot sinonim za *.torrent* datoteko, ki omogoča s pomočjo določenih programov izredno hitro in učinkovito nalaganje vsebin z interneta (priljubljeni programi so BitComet, BitTorrent, BitLord)
- UNDP – "**U**nited **N**ations **D**evelopment **P**rogramme", Razvojni program OZN
- URL – ang. **U**niform **R**esorce **L**ocator, univerzalni naslov dokumentov in drugih strani
- USB – ang. **U**niversal **S**erial **B**us – univerzalno serijsko vodilo
- VS OZN – **V**arnostni **S**vet **O**rganizacije **Z**druženih **N**arodov
- WWW – ang. **W**orld **W**ide **W**eb, sistem internetnih serverjev, ki podpirajo dokumente posebnih formatov (HTML), ki omogočajo povezovanje do drugih dokumentov, lahko pa tudi slik, glasb ali drugih datotek.

1. UVOD

Pred več kot petnajstimi leti je ameriški Državni raziskovalni svet zapisal v svoji izjavi, da je država v nevarnosti. Odvisna je od računalnikov! Kakor vsaka druga oblika odvisnosti, je tudi ta nevarna za obstoj neke entitete in zato je njena prisotnost zaskrbljujoča. Na začetku enaindvajsetega stoletja to ne velja več le za ZDA, temveč za vso razvito družbo, še posebno pa za visoko razviti zahodni svet, kamor sodi tudi Slovenija.

Dandanes računalniki nadzirajo in obvladujejo tudi tako bistvena področja za človekov obstoj kot sta oskrba z vodo in energijo. Vendar je to šele začetek. Računalniki v veliki meri upravljajo tudi s komunikacijami, finančnimi storitvami, prevozom, zdravniškimi zapisi, kriminalnimi kartotekami, proizvodnjo dobrin in tako naprej do skoraj vsakega segmenta v naši družbi, kjer nam lahko računalnik pomaga. Čeprav nam je uporaba računalnika v vsakdanjiku na mnogih področjih olajšala življenje in ga naredila enostavnejšega pa se moramo zavedati, da je računalnik le skupek strojne in programske opreme, ki lahko zataji. Zataji pa lahko zaradi slabe izdelave, fizične okvare, programske napake ali pa kar pa je najbolj zaskrbljujoče – zaradi namernega napada. In tako se vse ugodnosti in vse poenostavitve, ki nam jih prinaša uporaba računalnikov, lahko v trenutku spremenijo v nerešljivo uganko in popolno zatajitev delovanja. Na videz manj nevarna, vendar hujša oblika kot zatajitev delovanja, pa je sprememba delovanja brez vednosti uporabnika, ki nič hudega sluteč in nevede normalno opravlja vse naloge, njegov računalnik pa je hkrati orodje v rokah neznanca. In ta neznanec, lahko mu rečemo tudi informacijski bojevnik, je ob primerni opremljenosti in primernemu znanju sposoben narediti več škode s tipkovnico kot z bombo. V dobi računalnikov je sposoben ukrasti več s pomočjo računalnika kot bi lahko kdajkoli ukradel s pištolo.

Tako varnost posameznika na internetu dobiva posebno dimenzijo, ki v preteklosti ni imela velikega pomena, dandanes pa se je to spremenilo. Tako je o varnosti posameznika na internetu, v obdobju ko ima računalnik in dostop do interneta že skoraj vsako gospodinjstvo, potrebno spregovoriti nekaj več besed. Zato sem se odločil, da to temo bolj podrobno preučim. Poleg bolj računalniško naravnanega

osrednjega dela naloge pa sem želel vključiti tudi varnostno misel, ki se dotika moje teme. Preko sodobne varnostne paradigme, kjer se posameznika že obravnava kot referenčni objekt varnosti, ter koncepta človekove varnosti, sem prišel do novega varnostnega koncepta. V tem konceptu je internetna varnost že posebej izpostavljena in grožnjam, ki smo jim izpostavljeni na spletu, se namenja posebna pozornost. Da pa bi bralec lažje našel povezavo med temo moje diplomske naloge in obramboslovjem, sem se odločil tudi za opredelitev konceptov informacijske varnosti in informacijskega vojskovanja, ki v zadnjem času pridobivata na pomenu tudi s klasičnega vidika vojskovanja. Tudi nekatere internetne grožnje lahko posredno ogrozijo delovanje prav vsakega informacijsko podprtega sistema v sodobnih oboroženih silah, zato najmodernejše oborožene sile namenjajo temu področju čedalje večjo pozornost. Sam pa sem se odločil, da te grožnje predstavim na najnižji ravni, t.j. ravni posameznika, ki mi je tudi osebno najbližje. V nalogi sem naredil pregled najpogostejših groženj, ki so prisotne v uporabnikovi vsakdanji izkušnji z internetom. Poskusil sem zajeti vse od popolnoma programskih groženj, do tistih bolj zahtevnih in bolj nevarnih, ki že vključujejo tudi socialni inženiring in s tem prevare, zavajanje in izsiljevanje. V zadnjem delu naloge sem podal tudi deset pravil internetne zaščite posameznika in njegove zasebnosti, ki bodo bralcu privarčevali marsikatero izgubljeno uro za računalnikom in v najboljšem primeru tudi morebitno izgubo finančnih sredstev.

Ko vsa ta tveganja postavimo ob bok današnji izpostavljenosti in ranljivosti družbe in dodamo še s sodobnimi informacijskimi tehnologijami opremljen terorizem, je skrb za tovrstne probleme in varnost posameznika na internetu več kot na mestu. Za lepšo predstavo o resnični ogroženosti vseh uporabnikov informacijsko – komunikacijske tehnologije velja omeniti le še podatek, da so tovrstna kazniva dejanja v računalniško najbolj razvitih državah, najhitreje rastoča oblika kriminala. Zaradi vseprisotne odvisnosti družbe in posameznika od računalnikov, sem si izbral to temo tudi za svojo diplomsko nalogo.

2. METODOLOŠKI OKVIR

2.1. Namen in cilj preučevanja

S to temo želim morebitnemu bralcu približati problem človekove varnosti na internetu. V nalogi želim narediti pregled groženj, ki posamezniku lahko predstavljajo resno nevarnost z vidika zasebnosti in varstva podatkov ter tudi zaščite njegove programske in strojne opreme. Te nevarnosti lahko preko medmrežja vstopijo v našo zasebnost in nas ogrozijo prav na mestu, kjer se počutimo povsem varne pred neznanci in nevarnostmi - v lastnem stanovanju, le to pa nas naredi še bolj ranljive. Hkrati pa želim prikazati tudi možne načine preventivnega delovanja pred napadi iz medmrežja in ukrepe za zaščito uporabnikove zasebnosti.

2.2. Hipoteze

1. Osebna varnost posameznika na internetu pridobiva na pomenu, vendar ji še vedno posvečamo premalo pozornosti glede na realno ogroženost.
2. Z razvojem tehnologij in različnih storitev preko interneta se lahko varnost posameznika navidezno (in tudi v resnici) poveča, vendar je vse to lahko zavajajoče, saj je vsak posameznik, ne glede na znanje in interes, odgovoren za lastno zaščito.
3. Internetne nevarnosti so zapletene oblike ogrožanja posameznika, ki se jih največkrat ne zavedamo, dokler ni že prepozno.

2.3. Pristop in temeljne uporabljene metode dela

V nalogi sem uporabil več metod dela, s pomočjo katerih sem prišel do končnih ugotovitev. Preden sem se naloge lotil, sem z metodo zbiranja virov predelal literaturo, ki je bila na voljo. Pri pisanju uvoda ter opredeljevanju ključnih pojmov in konceptov sem uporabil predvsem analizo vsebine, tako primarnih kot sekundarnih virov in literature. V nek celovit pregled sem z opisno metodo vključil glavne internetne nevarnosti, njihove značilnosti ter različne narave delovanja. Na nek način pa bo v nalogi uporabljena tudi metoda opazovanja z udeležbo, saj sem tudi sam reden uporabnik interneta in lahko iz lastnih izkušenj opišem določene nastale situacije, ki smo jim uporabniki podvrženi.

Svojo temo želim analizirati z obramboslovnega vidika, vendar se zavedam, da bo potreben širši pristop od striktno družboslovnega za preučitev koncepta posameznikove varnosti na internetu. Poleg tega bo potrebno pri določenih računalniško naravnanih vprašanjih uporabiti tudi tehnično znanje s področja varnosti na internetu. Zato bi lahko pristop dela označil kot interdisciplinaren, predvsem zaradi prepletanja tehničnega in družboslovnega pristopa.

2.4. Struktura naloge

Prvo poglavje v nalogi predstavlja uvod, v katerem sem predstavil moj splošen pogled na predstavljeno problematiko in nekatere zanimivosti, s katerimi želim bralcu približati vsebino naloge in vzbuditi željo po branju le te.

Uvodu sledi metodološki okvir v katerem opredeljujem namen in cilj preučevanja, postavim hipoteze ter naštejem temeljne uporabljene metode dela. V metodološkem okviru začrtam tudi pristop k nalogi in način dela za ugotovitev morebitne pravilnosti postavljenih tez.

Tretje poglavje predstavlja teoretični okvir raziskovanja varnosti ter temeljne pojme in koncepte. S temeljnimi koncepti bom najprej opredelil sodobno varnostno paradigmo, ki se že dotika konceptov človekove varnosti – s tem pa tudi posameznikove varnosti na internetu. Opredelil bom še informacijsko varnost in informacijsko vojskovanje; koncepta, ki mojo nalogo postavljata v nek širši okvir.

Četrto poglavje predstavlja osrednji del moje naloge. Razdelil ga bom na dva večja sklopa. V prvem bom predstavil nevarnosti in grožnje, ki grozijo posamezniku na

internetu. Ta del poglavja bo najobsežnejši zaradi množice raznolikih groženj in drugih oblik nevarnosti. V drugem, krajšem delu, pa bom strnil nasvete in priporočila za povečanje posameznikove varnosti na internetu.

V zadnjem poglavju bom preveril pravilnost mojih hipotez in postavil nek sklep in zapisal moja razmišljanja ob koncu naloge.

3. TEMELJNI POJMI IN KONCEPTI

3.1. Sodobna varnostna paradigma

Politične in družbene spremembe zahtevajo prilagoditev ali ustvarjanje novih teorij. V drugi polovici dvajsetega stoletja, v času hladne vojne, je vprašanje varnosti opredeljevala bipolarna struktura sveta in le ta je bila dolgo obdobje dokaj jasno določena, zato je razvoj varnostnih misli malo zastal. Po koncu hladne vojne pa se je svet in s tem varnostni prostor močno preoblikoval in tako je v sodobnem okolju vprašanje in preučevanje ogrožanja ponovno dobilo pomembnejše mesto. Varnostna misel pa kljub spremenjenim razmeram v družbi ni v zadostni meri prilagodila tipologije varnostnih groženj, prav tako pa ne obstaja nek konceptualni konsenz o vsebini varnostnih groženj (Kirchner v Svete, 2005: 55). Sodobna varnostna razprava se tako usmerja predvsem na tri varnostne referenčne objekte, ki so: na koga se varnost nanaša, kdo ali kaj to varnost ogroža in seveda na kakšen način se varnost zagotavlja – varnostne mehanizme (Liotta v Svete, 2005: 55). In prav okoli teh treh referenčnih objektov se vrti celotna sodobna varnostna razprava.

Tradicionalno se je pojem varnosti povezoval predvsem z vojaško obrambo ozemlja držav, delujočih v anarhičnem mednarodnem okolju, dandanes pa se varnost nagiba tudi v druga področja, tako nekateri avtorji (Coker, 2001: 13,14) pravijo, da je koncept vojaka proti vojaku preteklost ter da danes varnostna vprašanja izhajajo iz naslova kriminala, terorizma ter družbenih in ekonomskih neenakosti. Bilgin (2003: 203, 204) pa gre še dlje in pravi, da se danes področja človekovega delovanja, nanašajoča na varnost, širijo in da vključujejo celotne družbe ter da se spustijo tudi na najnižjo raven, raven posameznika.

Tabela 1: Razširjeni koncepti obravnavanja varnosti

Teoretična perspektiva	*Oblika varnosti*	*Oblika širitve*		
		Referenčni objekt	Ogrožene vrednote	Viri ogrožanja
Tradicionalna (realistična)	nacionalna varnost	država	suverenost, teritorialna celovitost	druge države
Netradicionalna + tradicionalna (liberalna in realistična)	družbena varnost	narodi, družbene skupine, interesne skupine, politične skupine	narodna enotnost, identiteta, kvaliteta življenja	države, narodi, migranti, tuje kulture
Netradicionalna (liberalna)	človekova varnost	posamezniki, človeštvo, človekove pravice, vladavina prava	preživetje, kvaliteta življenja, človekov razvoj	država, globalizacija, narava
Netradicionalna (radikalna)	okoljska varnost	ekosistem	trajnost, stabilnost	človeštvo (izraba naravnih virov, vojne, onesnaževanje)

Vir: Svete, 2005: 55

Kot je prikazano v tabeli se sodobne razprave glede varnosti zelo razlikujejo glede referenčnih objektov in njihovih medsebojnih odnosov, varnostnega instrumentarija (kako doseči stanje varnosti), delno pa tudi glede virov ogrožanja. V nečem pa so si blizu - vse razumevajo varnost kot celostni problem ("holistični" pristop), le to pa ne izključuje varnosti na nivoju posameznih entitet, oz. referenčnih objektov (Svete, 2004: 655). V tem okviru se sodobna varnostna paradigma navzven lahko obravnava v obliki štirih temeljnih konceptualnih okvirov, ki so: 1. individualna varnost, 2. nacionalna varnost, 3. mednarodna varnost in 4. globalna varnost (Grizold, 1999: 28).

Pojav koncepta individualne varnosti[1] pa naj bi po Newmanu (2001: 239) imel izvor v vplivu individualnih vrednot in norm na mednarodno okolje, kjer vrednost posameznika pridobiva na pomenu. Vključevanje človeških (nevojaških) problemov v nove koncepte varnosti pa nam na novo odpre razmišljanja o tem ali so to varnostni problemi per se (sami po sebi) ali so to le vzroki za druge bolj tradicionalne varnostne probleme, ki vključujejo tudi državo in smo jih le odkrili na novo. V pojasnitev lahko sprejmemo termin "sekuritizacija" (ang. securitisation). Ta označuje proces, pri katerem

[1] Koncept človekove varnosti naj bi bil po Newmanu obsežen in šele razvijajoč se koncept v množici drugih konceptov varnosti.

neka zainteresirana skupina ali državna elita določeno zadevo vzame iz vsakdanje politike in le to definira kot varnostni problem. Iz tega lahko sklepamo, da se nevarnost ne smatra kot direktna posledica določene grožnje, ampak kot rezultat politične interpretacije te grožnje. Tako se varnost analizira kot reakcija politične akcije glede določene grožnje ali zaznanega problema (Kirchner, 2003: 11). "Sekuritizacija" je torej proces, v katerem se viri ogrožanja varnostno problematizirajo ter vzpostavijo mehanizmi učinkovitega in aktivnega odgovora nanje (Grayson v Svete, 2005: 58).

Sodobni pogledi na varnost se tako ne izključujejo, izbirajo pa nove smernice in se spuščajo (dvigajo) na nove nivoje. Tako vidimo, da se sodobna varnostna paradigma odmika od klasične pozicije država proti državi (vendar je ne opušča in ji ni v nasprotju) in vključuje mnogo drugih referenčnih objektov, le ti pa se nanašajo tudi na temo moje diplomske naloge – posameznika in njegovo varnost na internetu.

3.2. Koncept človekove varnosti

V prejšnjem poglavju sem razdelil koncept sodobne varnosti in v njem je svoj prostor našel tudi koncept človekove varnosti. Razlogi za nastanek le tega tičijo v družbenem razvoju, ki vodi v čedalje večje neenakosti v ekonomskih zmožnosti, zmanjševanje neobnovljivih virov, naraščanje proti tujcem nastrojenega razpoloženja, kot odgovor na pritiske migracij iz nerazvitega v razviti svet ter širjenje znotrajdržavnih konfliktov in pobude po človekoljubnem posredovanju (Bilgin v Svete, 2005: 58). Razlogi pa seveda tičijo tudi v prenosu vrednot posameznika (kot so preživetje, kvaliteta življenja ter človekove pravice in svoboščine) v mednarodni sistem. To vse so izzivi, ki jih s pomočjo tradicionalne varnostne paradigme ni bilo mogoče razjasniti, zato je potrebno nekatere ideje razširiti. Svete (2005: 94) pravi, da je interes za človekovo varnost posledica zaznanega ogrožanja te varnosti[2], zato je za koncept človekove varnosti nujno potrebna osvoboditev od drugih struktur moči, pa naj bodo

[2]Kot glavni vir ogrožanja nekateri vidijo globalizacijo, ki naj bi zmanjševala moč šibkih skupin, ogrozila domače gospodarske panoge ter povzročila družbeno neenakost, medtem ko drugi kot grožnjo človekovi varnosti zaznavajo predvsem državo in njene institucije (Svete, 2005: 94).

globalne, nacionalne ali regionalne. Teh konceptov človekove varnosti je več, vsak pa izhaja iz določenih družbenih, kulturnih ali geostrateških usmeritev.

V Razvojnem programu Organizacije združenih narodov (UNDP, 1994: 22, 24) je bilo že pred več kot desetletjem zapisanih nekaj splošnih ugotovitev glede koncepta človekove varnosti, ki naj bi imel štiri poglavitne značilnosti. Prva ugotovitev je bila, da je človekova varnost občа skrb in je pomembna tako za bogate kot revne narode, ki so izpostavljeni podobnim grožnjam, kot so nezaposlenost, droge, kriminal, onesnaženost, itd. Sicer je izpostavljenost tem grožnjam po svetu različna, le ena značilnost pa je prisotna pri vseh – tovrstna ogrožanja so v porastu. Druga ugotovitev UNDP-ja je bila, da so posamezne komponente človekove varnosti medsebojno povezane in soodvisne. Kajti če je varnost ljudi ogrožena v nekem delu sveta je zelo verjetno, da se bo ta grožnja razširila drugam. Lakota, bolezni, onesnaženje, trgovina z drogami, terorizem, etnični konflikti in razpad družbenih ureditev niso več osamljeni in izolirani dogodki, zaščiteni z državnimi mejami. Njihove posledice imajo globalen vpliv. Tretja ugotovitev poudarja, da je človekovo varnost lažje zagotavljati z zgodnjim preprečevanjem (preventivo) kot pa kasnejšim posredovanjem (kurativo). Grožnje človekovi varnosti je lažje in ceneje ustavljati in preprečevati, ko so še v povojih ali v porastu, kot pa kasneje, ko se je grožnja že razvila in dobila ogromne in neobvladljive razsežnosti. Zadnja ugotovitev strokovnjakov pri UNDP pa je bila, da je koncept človekove varnosti usmerjen k posamezniku. Ukvarja se z oblikami človekovega življenja v družbi, njihovo svobodo pri odločitvah, njihovimi možnostmi pri vključevanju na trg dobrin ter ali živijo v konfliktu in stalnem strahu ali v miru.

Podobno kot z drugimi temeljnimi koncepti (kot je človekova svoboda), je tudi človekovo varnost lažje definirati ob njeni odsotnosti, vendar pa je dobro da imamo vsaj neko bolj definirano opredelitev. Tako lahko za človekovo varnost rečemo, da ima dva glavna vidika; prvi je varnost pred tako bistvenimi grožnjami kot so lakota, bolezni in represija, drugi vidik pa je varnost in zaščita pred nenadnimi in škodljivimi razdori v vsakdanjem življenju pa najsibo v domovih, službah ali skupnostih (UNDP, 1994: 24).

Newman (2001: 243) je poleg UNDP-jeve opredelitve človekove varnosti opredelil še tri najpomembnejše prepletajoče vidike, ki se bolj razlikujejo po poudarkih in osredotočenjih, kot po različnih zvrsteh. Med seboj se ne izključujejo, temveč so nekako različne veje iste misli. Dodajmo še, da bi se lahko nekatere koncepte človekove

varnosti definiralo kot "netradicionalna varnost", kjer bi referenčni objekt ostala država, izzivi pa bi bili nedržavni in nevojaški. Ti vidiki so:

⇒ vidik temeljnih človekovih dobrin (UNDP)
⇒ dogmatični vidik (intervencionistična smer)
⇒ vidik družbene blaginje (razvojna smer)
⇒ nov varnostni koncept (ang. new security concept).

Prvi vidik, ki se osredotoča na temeljne človekove dobrine izhaja iz Razvojnega programa OZN (UNDP), ki vsebuje temeljno ekonomsko, zdravstveno, prehrambeno, osebno, okoljsko, kulturno ter politično varnost. UNDP je zapisal, da dandanes za večino ljudi, občutek nevarnosti izhaja iz bolj vsakdanjih skrbi, kot pa katastrofalnih dogodkov kataklizmičnih razsežnosti. Zanesljiva zaposlitev, zanesljiv dohodek, zdravstvena oskrba, okoljska varnost ter zaščita pred kriminalom so pojavljajoče skrbi človekove varnosti povsod po svetu. (UNDP, 1994: 3; Newman, 2001: 243)

Drugi vidik je intervencionističen, kajti človekova varnost se mora nujno osredotočiti na posameznika, čeprav to povzroča napetosti do državne neodvisnosti. Ta pristop ugotavlja da tradicionalen pristop k varnosti države ne zagotavlja nujno tudi varnosti državljanov. Trendi v sodobnem konfliktu, ki odražajo visoko raven znotrajdržavnih konfliktov so pokazali, da je velika večina žrtev med civilnim prebivalstvom, še posebno med ženskami in otroki. Zatorej je izrednega pomena, da je potrebno zaščititi človekove pravice tudi, če to posega v pravice države. Nazoren primer prednosti človekovih pravic pred državnimi je posredovanje Nata v ZRJ leta 1999. Nato se je odločil posredovati v smislu človekoljubnega posredovanja (človekove pravice), medtem ko so nekateri opozarjali na pomanjkanje pravno-formalne podlage in kršitev temeljev mednarodnega miru, varnosti in stabilnosti. Tako je potrebno včasih uporabiti silo proti določeni državi za zaščito človekove varnosti, nevarno pa je da bi tovrstno početje postalo praksa reševanja konfliktov (Newman, 2001: 244; Svete, 2005: 95). Da pa je položaj uveljavljanja človekove varnosti še bolj zapleten pa poskrbijo mednarodne medijske korporacije, ki ne predstavljajo vseh konfliktov s tega vidika, oz. opozarjajo samo na določene konflikte, kar pa države spet lahko izkoristijo za uveljavljanje lastnih interesov in tako delujejo na račun človekove varnosti in ne z namenom zagotavljanja le te.

Tretji vidik, vidik družbene blaginje, opredeljuje kot temeljno vrednoto družbeni razvoj, iz katerega se lahko gradijo druge splošne dobrine in svobode. Tu gredo še dlje od prvega vidika, kajti menijo da osnovne človekove dobrine niso dovolj. Družbeni razvoj jim ne predstavlja končni cilj, ampak je le sredstvo, s katerim se končni cilj lahko doseže. Zato pripadniki razvojne smeri menijo, da se demokracija, mir in razvoj zaradi medsebojne povezanosti obravnavajo skupaj. Svete (2005: 96) pa še pravi da morajo biti koncept človekove varnosti in strategije za njegovo uresničevanje integralne in celovite.

Četrti koncept človekove varnosti pa je z vidika moje diplomske naloge najpomembnejši, saj obravnava človekovo varnost na nov, netradicionalen način. Usmerjen je na netradicionalno varnost in nehumano družbo in se nanaša predvsem na epidemiologijo, droge, terorizem, trgovino s strelnim orožjem, nehumanim orožjem (protipehotne mine), kibernetsko bojevanje, trgovanje z ljudmi, itd (Newman, 2001: 245). Politične, ekonomske in tehnološke spremembe, ki so omogočile globalizacijo in razvoj, so omogočile delovanje tudi drugi, hudobni strani, ki predstavlja resne grožnje varnosti, razvoju in demokraciji. V tem konceptu je referenčni objekt tako država kot posameznik, obravnava se tako temeljne človekove dobrine kot tudi družbeno blaginjo. V tem konceptu je varnost posameznika neodvisna od varnosti države, lahko pa izguba človekove varnosti predstavlja tudi izzive za varnost države.

V posameznih pristopih k preučevanju človekove varnosti je zaznati različno razumevanje varnosti kot tudi družbenega okolja. Tako da ne obstaja nek konsenz o definiciji človekove varnosti. Kljub različnim pogledom pa lahko sklenemo, da je koncept človekove varnosti še vedno v veliki meri v nasprotju s tradicionalnim konceptom varnosti in državno suverenostjo, ki je še vedno med najpomembnejšimi stebri zagotavljanja miru in varnosti. Problem pri uveljavljanju človekove varnosti pa ni v konceptu samem, temveč v nevarnosti da bi pod pretvezo zagotavljanja človekove varnosti v novem globalnem položaju nekateri akterji tako uveljavljali svoje varnostne instrumente, ki v bistvu služijo starim realističnim konceptom varnosti.

3.3. Informacijska varnost

Informacijska varnost obravnava več različnih področij nanašajočih se na informacije. Informacijska varnost ni omejena le na računalniške sisteme, prav tako pa ne le na informacije v elektronski obliki. Nanaša se na vse aspekte zaščite in varovanja informacij in podatkov v kakršnikoli obliki.

Naj omenim le nekatere definicije bolj znanih institucij. IBM-ov računalniški slovar informacijsko varnost opredeljuje kot koncepte, tehnike, tehnične in administrativne ukrepe, ki se jih uporablja za zaščito informacij pred namernimi ali nenamernimi nepooblaščenimi pridobitvami, povzročanjem škode, razkritjem informacij, spremembo informacij, manipuliranje z njimi ali izgubo in uporabo informacij (McDaniel, 1994: 94). Državni slovar informacijske sistemske varnosti pa informacijsko varnost sistemov (INFOSEC) opredeljuje kot zaščito informacijskih sistemov pred nepooblaščenimi dostopi ali modifikacijami informacij, najsibo v shranjeni obliki, v procesu ali prenosu ter zaščito pred zatajitvijo delovanja (DOS) pooblaščenim uporabnikom in zagotovitvijo delovanja nepooblaščenim uporabnikom, vključno z vsemi ukrepi za odkrivanje, dokumentiranje in zavračanje tovrstnih groženj (Hayden, 2004: 33). Isto definicijo navaja tudi US Army Field Manual (FM 100-6). Računalniški slovar AFCERT pa informacijsko varnost opredeljuje kot rezultat kakršnega koli sistema ukrepov in procesov za identifikacijo, nadzor in zaščito nepooblaščenih razkritij informacij, katerih zaščita je odobrena s direktnim ukazom ali zakonsko odredbo (Whitaker, 1998).

Večina opredelitev informacijske varnosti se osredotoča na specifično uporabo in/ali specifičen medij, e.g. "zaščititi elektronske podatke pred nepooblaščeno uporabo". V bistvu pa je to napačna predstava ali nesporazum, ker se informacijsko varnost enači z računalniško varnostjo, ki je ožji pojem. Tovrstne definicije glede prenosa informacij (komunikacijski vidik) in uporabniškega vidika informacijsko komunikacijske tehnologije (IKT) opredeljuje in obravnava omrežna varnost. Koncept informacijske varnosti pa je širši in kot cilj ogroženosti vključuje celotno IKT, vključno z zbiranjem in obdelavo podatkov in delovanje strojne opreme nasploh (Svete, 2005: 107). Tako informacijska varnost ne prekriva le informacije, temveč celotno infrastrukturo, ki omogoča uporabo informacij (procesi, sistemi, storitve, tehnologija) vključno z računalniki, omrežji, itd. Pomembna ugotovitev je, da je informacijska varnost nujno nedokončno opredeljena, kajti vedno obstaja verjetnost, da nekdo najde neko novo

obliko uporabe/izrabe kakršnekoli informacije. Temeljno vodilo pri iskanju stopnje informacijske varnosti v kakršnikoli situaciji pa mora biti sorazmernost z vrednostjo informacij, ki jih je potrebno zaščititi ter z izgubo (finančno ali drugo), ki bi nastala z nepravilno uporabo (pooblaščeno ali nepooblaščeno) teh informacij – razkritje, degradacija, zatajitev ali karkoli drugega (Wikipedia, 2006: http://en.wikipedia.org/wiki/Information_security, 6. april 2006).

Kot temeljne elemente, lastnosti oziroma aspekte informacijske varnosti bi lahko zapisali sledeče tri:

⇒ zaupnost,

⇒ integriteta,

⇒ dostopnost[3].

Te tri lahko povežemo tudi s konceptom "prava informacija, pravim ljudem, ob pravem času". *Zaupnost* je načelo, ki zagotavlja, da informacije ne bodo razkrite nepooblaščenim uporabnikom. *Integriteta* predstavlja trdno upanje, ki temelji na dveh delih. Integriteta podatkov zagotavlja, da so na voljo pravi podatki in da niso bili spremenjeni na kakršenkoli način med prenosom in sprejemom le teh. Integriteta vira pa predpostavlja zaupanje, da je pošiljatelj določenih informacij tisti, za katerega se predstavlja. Integriteta podatkov je lahko ogrožena kadar so bile informacije spremenjene, namerno ali nenamerno, še preden jih je prejemnik dobil. Integriteta vira pa je ogrožena, kadar se nekdo s prevaro izdaja za pravi vir in tako dovaja nepopolne ali celo napačne informacije k prejemniku. *Dostopnost* pa je označena kot zmožnost zagotovitve dostopa do informacij, ko se le te potrebuje.

Četrti splošno sprejeti element pa je sposobnost sistema za sledenje sprememb v sistemu (*ang. accountability*), ki zagotavlja da sistemski administratorji lahko spremljajo spremembe, ki so bili storjene v sistemu in imajo tako vsaj vpogled v storjene spremembe, če že niso sposobni v celoti nadzirati sistema[4]. Peti element, ki ga je dodal Državni inštitut za standarde in tehnologijo v ZDA, pa je *zagotovitev*. Ta naj bi bil najpomembnejši, ker brez njega tudi ostali štirje nimajo pravega pomena. Zagotovitev je temeljno zaupanje, da vsi varnostni ukrepi, tehnični in operativni

[3] Te tri v svetu uporabljajo še drugi: kibernetsko bojevanje informacijske varnosti opisujejo kot CIA triada, CIA pa izhaja iz začetnic treh besed (**C**onfidentiality, **I**ntegrity, **A**vailability).

[4] Problem pa nastane takrat, kadar je nek nepooblaščen uporabnik tako vešč in je tako dober poznavalec sistemov, da je sposoben obiti sistem za sledenje sprememb, oziroma celo prevzeti nadzor nad njim.

delujejo tako kot so bili zasnovani z namenom zaščititi sistem in informacije ter procese. Prav tako pa zagotovitev pomeni tudi, da so vsi ostali štirje elementi informacijske varnosti zagotovljeni. (Wikipedia, 2006: http://en.wikipedia.org/wiki/Information_security, 6. april 2006).

Da pa bi lažje razumeli vseobsežnost informacijske varnosti, si lahko pogledamo samo njene grožnje. Svete (2005: 107) je grožnje razdelil v dve skupini. Prva skupina groženj se nanaša na informacijsko zagotovitev oz. fizične oblike ogrožanja, druga skupina pa obsega uporabniški vidik ogrožanja informacijske varnosti. V spodnji tabeli so prikazane oblike ogrožanja informacijske varnosti.

Tabela 2: Oblike ogrožanja informacijske varnosti

Višja sila	*Pomanjkljivosti strojne in programske opreme*	*Človeški dejavnik (nenamernost)*	*Človeški dejavnik (namernost)*
• **potres** • **nevihte** • **poplave** • **strele** • **požar** • **visoka temperatura** • **visoka vlažnost** • **onesnaženost** • **radarsko sevanje** • **akustično sevanje** • **elektromagnetno sevanje** • **nestabilnost napajanja z električno energijo** • **izredne razmere** • **vojno stanje**	• **izpad sistema** • **tehnične napake na strežniku** • **tehnične napake na odjemalcih** • **logične napake v strežnih programih** • **logične napake v aplikativnih programih**	• **slaba organizacija** • **nedisciplina** • **nemarnost** • **nestrokovnost** • **monotonost** • **utrujenost**	• **kraje** • **prevare** • **poneverbe** • **izsiljevanje** • **grožnje** • **kršenje zasebnosti** • **sabotaže** • **sporočanje zaupnih podatkov** • **vohunjenje** • **pornografija** • **propaganda** • **vandalizem (cracking)** • **terorizem** • **umori** • **vdiranje v računalnike (hacking)** • **izdelava in širjenje virusov** • **piratstvo na področju programske opreme** • **napadi DOS**
INFORMACIJSKA ZAGOTOVITEV		DRUŽBENO IN KULTURNO OGROŽANJE UPORABA KOT OGROŽANJE	

Vir: Svete, 2005: 108

3.4. Informacijsko vojskovanje

Informacijsko vojskovanje[5] je izredno širok koncept[6], za katerega ne obstaja neka enovita definicija, ki bi objela celotno sfero in bi jo sprejemali vsi avtorji, ki se udejanjajo na tem področju. Obstaja pa jasno dejstvo, da smo ali bomo vsi uporabniki[7] IKT prej ali slej podvrženi neki obliki informacijskega vojskovanja. Zakaj? Zato ker je sodobna družba vse bolj prepletena z uporabo IKT, ki neizbežno vključuje elemente informacijskega vojskovanja. Vse to pa je jasna posledica dejstva, da so temelji moderne družbe med drugim postavljeni na razpoložljivosti in dostopnosti informacij. Schwartau (1996: 28) pravi da so današnje informacije nekakšen ekvivalent včerajšnjih tovarn, vendar da so le te "novodobne tovarne" mnogo bolj podvržene nevarnostim in mnogo bolj ranljive. Informacijsko vojskovanje je tako elektronski konflikt, v katerem je informacija strateška dobrina, ki je vredna agresivnega pristopa in je tudi podvržena tovrstnemu delovanju. Prav tako v tem konceptu ni prve linije bojevanja, saj je potencialno bojišče lahko povsod kjer imamo sisteme povezane v kibernetski prostor. V informacijskem bojevanju so bombe in izstrelki svoje naslednike dobili v informacijskih orožjih. Le ti pa niso več pod drobnogledom državnih ali mednarodnih institucij oz. omejeni na uporabo državnih in naddržavnih organizacij. Informacijsko orožje je dandanes na voljo vsem, lahko tudi brezplačno. To dejstvo pa drastično poveča število referenčnih objektov oz. elementov, ki jih je potrebno upoštevati, ko obravnavamo sodobno varnost, ki zagotovo vključuje informacijsko vojskovanje. Informacijsko vojskovanje[8] se vrti okoli informacij, nadzora in uporabe le teh. Upoštevajoč, da so temelji sodobne družbe postavljeni prav na informacijah, je jasno da je IV neizogibno in da je pravzaprav že tukaj.

Da bi karseda celovito zaobjel koncept informacijskega vojskovanja in njegove temeljne karakteristike, bom navedel nekaj ugotovitev različnih avtorjev, ki so v okviru

[5] Informacijsko vojskovanje (bojevanje) je le eden izmed družine pojmov, ki opisujejo tovrstno ravnanje. Poleg tega se uporabljajo še drugi: kibernetsko bojevanje (ang. cyber warfare), digitalno bojevanje (ang. digital warfare) in neubojno bojevanje (ang. soft warfare) (Arsić, 2004).

[6] Informacijsko vojskovanje lahko imenujemo tudi informacijsko bojevanje, kadar je omejeno le na onesposabljanje sposobnosti zbiranja, obdelave, shranjevanja, posredovanja in uporabe informacij pri nasprotniku z namenom doseganja informacijske premoči (Svete, 2002: 75).

[7] S prvim januarjem 2006 je svetovna populacija uporabnikov interneta presegla eno milijardo, kar predstavlja 15,7% svetovne populacije. (Internet World Stats, http://www.internetworldstats.com/blog.htm, 11.april 2006)

[8] V nadaljevanju "IV".

Delphi[9] metode (Thrasher, 1996; Schwartau, 1994: 579-587) prišli do sledečih ugotovitev glede informacijskega vojskovanja.

AL Campen[10] (Thrasher, 1996: 4) omejuje IV na bojevanje z informacijami v elektronski obliki, ter na strojno in programsko opremo, ki upravlja, ureja, shranjuje in obdeluje te informacije. Temeljne značilnosti IV pa sta odvisnost in ranljivost informacijskih sistemov.

Peter Cochrane[11] (Thrasher, 1996: 4) pa kot temeljne značilnosti IV opaža kakršnokoli oskrbo ali zaviranje dostopa do informacij v katerikoli obliki, z namenom povzročiti slabe odločitve ali zmesti/preobremeniti komunikacijske ali odločevalske procese na strani prejemnika informacij. Navaja pa sledeče primere: zmesti nasprotnika z napačnimi informacijami, poznati podatke, ki jih nasprotnik ne pozna, prestrezati nasprotnikove komunikacije, uporaba dezinformacij ter poškodovanje sposobnosti informiranja nasprotnika ali povzročiti zatajitev delovanja njegovih informacijskih sistemov.

Fred Cohen[12] (Thrasher, 1996: 4) definira IV kot konflikt v katerem je informacija ali informacijska tehnologija orožje, tarča, cilj ali metoda.

James Dunningan[13] (Thrasher, 1996: 4) označuje IV kot napadanje in branjenje sposobnosti za prenos informacije.

Martin Libicki[14] (Thrasher, 1996: 6) definira IV kot katerokoli aktivnost motivirano s potrebo po spreminjanju informacijskih tokov usmerjenih proti nasprotniku in zaščito lastnih proti tovrstnemu delovanju. To se razteza od fizičnih do radio-elektronskih napadov na sisteme in senzorje, do kriptografije, napadov na

[9] Delphi metoda je oblika raziskovanja skupine določenih geografsko razpršenih raziskovalcev, ki s pomočjo sistematičnega ukvarjanja z določenim problemom omogoča, da skupina posameznikov deluje kot celota z namenom rešiti določen kompleksen problem. (The Delphi method, www.iit.edu/~it/**delphi**.html, 7. april 2006) Bistvo in namen Delphi metode pa je izogniti se standardnim slabostim odločanja v odborih, kar pomeni izničiti vpliv medsebojnega vplivanja znotraj raziskovalne skupine (The Delphi Method – The Basics, http://www.iit.edu/~it/delphi.html , 7. april 2006; Rendulić, 1981: 29-31)

[10] Campen je urednik knjige *First Information War.*

[11] Cochrane je bil v času raziskave direktor British Telekoma.

[12] Cohen je avtor knjige *Protection and the Security on the Information Superhighway.*

[13] Dunningan je avtor knjige *Digital Soldiers.*

[14] Libicki je avtor knjige *What is Information Warfare.*

računalnike ter psiholoških operacij. Libicki še opredeli sedem oblik informacijskega bojevanja, ki imajo informacijo kot sredstvo, cilj in orožje:

- bojevanje na poveljniško-nadzornem področju (C2W),
- bojevanje temelječe na obveščevalni dejavnosti (ang.intelligence warfare),
- elektronsko bojevanje (ang. electronic warfare),
- psihološko bojevanje (ang. psyhological warfare),
- hekersko bojevanje (ang. "hacker" warfare),
- ekonomsko informacijsko bojevanje (ang. economic information warfare) in
- kibernetsko bojevanje (ang. cyberwarfare) (Dovč, 2005: 16; Libicki, 1995; Svete, 2002:77)

Winn Schwartau (1994: 584) opredeli pravo IV kot uporabo informacij in informacijskih sistemov kot orožij v boju proti ciljnim informacijam in informacijskim sistemom. Zavrača kakršnokoli uporabo bomb ali krogel v pravi informacijski vojni. IV lahko doleti posameznike, organizacije ali države skozi mnogo različnih tehnik[15] (Schwartau v Thrasher, 1996: 7). Zato se zelo razlikuje od klasičnih vojskovanj[16], kajti IV lahko zelo enostavno doseže civilno sfero in direktno vpliva nanjo. Poleg tega pa so še sredstva za izvajanje IV zelo razpršena in lahko dostopna vsem.

Schwartau (1994: 33) je tako strogo omejen le na elektronske napade na računalniške sisteme in omrežja, le te pa razdeli na tri nivoje:

- **napadi prvega razreda** (ang. Personal Information Warfare),
- **napadi drugega razreda** (ang. Corporate Information Warfare),
- **napadi tretjega razreda** (ang. Global Information Warfare)

(Schwartau, 1994: 33 ; Svete, 1999: 17).

[15] Te tehnike so: ogrožanje zaupnosti, napadi na integriteto vira, zatajitev delovanja (DOS), psihološke operacije (PSYOPS), zavajanje medijev, itd. (Schwartau, 1994: 584).

[16] Dandanes vojskovanje nikakor ne izključuje informacijskega vojskovanja. Tako na primer Corpus (2006) ugotavlja, da imata Rusija in Kitajska na stotine izbranih hekerjev, ki imajo v primeru klasičnega vojaškega napada delujejo izredno novodobno, saj je njihov edini namen preko medmrežja onemogočiti delovanje sovražnikovih C4ISR sistemov, oziroma onemogočiti njihovo delovanje le za kratek čas, ki bi šibkejšemu omogočil dostojno obrambo in možnost povračilnih udarcev agresorju (http://www.atimes.com/atimes/China/HD20Ad03.html, 20. april 2006)

Informacijsko vojskovanje v prvem razredu vključuje napade proti posameznikovi elektronski zasebnosti, njegovim digitalnim zapisom, datotekam ali drugimi oblikami osebnega elektronskega materiala. Na prvem nivoju, kjer obravnava varnost posameznika, Schwartau (1994:473) izpostavi tri ključna pravila:

1. Elektronska zasebnost ne obstaja!
2. V kibernetskem prostoru[17] ste krivi, dokler ne dokažete nedolžnosti.
3. Informacija je orožje!

Na drugem nivoju Schwartau opredeljuje napade, ki vključujejo korporacije in organizacijsko raven IV, ta del se ukvarja tudi z industrijskimi vohunjenji in krajami intelektualne lastnine podjetij in njihovih novih konceptov. Drugi nivo zavzema t.i. ekonomsko vojskovanje, ki dandanes dosega povsem druge dimenzije kot pred desetletji. Na tem nivoju nacionalne države niso več edini dejavnik, kajti nekatere multinacionalke se lahko po svoji ekonomski ali politični moči povsem primerjajo z njimi. Tretji nivo pa je odprt za globalno raven in se osredotoča predvsem na problematiko kibernetskega terorizma[18].

Schwartau (1994: 17) je informacijsko vojskovanje povezal z mnogimi pojmi, ki se prepletajo v vsakdanjiku. Povezal ga je s pridobivanjem bogastva za nas in odklanjanjem bogastva za naše nasprotnike. Povezal ga je z močjo ter preživetjem. Kajti kdor nadzoruje informacije ima v rokah neznansko moč in z njo lahko vpliva na (ne)preživetje drugih v današnjem visoko tekmovalnem svetu.

Inštitut za višje študije informacijskega bojevanja (IASIW) uporablja definicijo dr. Ivana Goldberga, ki opisuje informacijsko vojskovanje takole: "Informacijsko vojskovanje je ofenzivna in defenzivna uporaba informacij in informacijskih sistemov za zanikanje, izkoriščanje ali uničenje nasprotnikovih informacij, procesov temelječih na informacijah, informacijskih sistemov in računalniških omrežij, medtem ko zaščitimo lastne sisteme. Tovrstna dejanja so uporabna za dosego prednosti pred vojaškimi, političnimi ali poslovnimi nasprotniki." (Goldberg, 2004)

Dorothy E. Denning (v Svete, 2002: 76) razume koncept informacijskega vojskovanja precej širše in gre preko računalniških omrežij in računalniških sistemov. V informacijsko vojskovanje vključuje tudi druge medije po katerih se prenašajo

[17] kibernetski prostor - cyberspace
[18] ang. cyber-terrorism

informacije, tako vključuje tudi človeka kot medij. Prenos informacij tako poteka med ljudmi in njihovim vsakdanjim okoljem ter preko različnih komunikacijskih storitev na njihove računalnike ali računalniške sisteme. Informacijsko vojskovanje obsega tako operacije proti vsebini informacij in operacije proti podpornim sistemom, pri čemer je vključena tako strojna kot programska oprema ter človekova dejavnost. Vse te informacije pa imajo skupno eno lastnost, to je da je njihov namen izkoristiti informacije v svoj prid in le to onemogočati svojim nasprotnikom (Denning, 1998: 9-13).

Obstajajo pa tudi druge oblike definiranja IV, tako naprimer Arquilla in Ronfeldt (v Dovč, 2005: 14) opredeljujeta kibernetsko (ang. cyberwar) in omrežno vojskovanje. Omrežno bojevanje obsega socialne, politične, ekonomske in vojaške oblike konflikta, kjer se govori predvsem o konfliktih nizke intenzivnosti (LIC), operacijah drugačnih od vojne (OOTW) in drugih predvsem nevojaških oblikah konflikta in kriminala. Kibernetsko bojevanje pa se nanaša na vojaško sfero, konflikte visoke intenzivnosti (HIC) in konflikte srednje intenzivnosti (MIC).

Glede na zgoraj omenjene definicije in opise konceptov informacijskega vojskovanja lahko sklenem, da neke enovite opredelitve IV ni, večina pa vsebuje nekaj glavnih elementov in značilnosti IV. Vedno je prisotna uporaba informacijskih tehnologij, s pomočjo katerih lahko negativno vplivamo na nasprotnikove informacijske sisteme ali zavarujemo naše pred tovrstnim delovanjem. Od vseh definicij se temi moje diplomske naloge najbolj približa razdelitev po Schwartau, kjer napadi prvega razreda vključujejo posameznikov vidik informacijskega vojskovanja in njegovo prizadetost ob tem. Prav tako pa Libicki v dveh od svojih sedmih oblik IV direktno navaja hekersko bojevanje in kibernetsko bojevanje, ki se direktno nanašata na probleme na katere naleti posameznik ob stiku s kibernetskim okoljem - internetom.

Prav tako je na mestu razmislek o uporabi terminologije za mojo nalogo. Termin **informacijsko vojskovanje** je za temo moje naloge preobsežen, prav tako bi lahko kot preobsežnega označil termin **informacijsko bojevanje**. Zato menim, da je na nivoju posameznika, in s tem moje diplomske naloge, bolj primeren termin **informacijsko delovanje**.

Slika 1: Informacijsko vojskovanje

Vir: prirejeno po Report of the Defense Science Board Task Force on Information Warfare – Defense, http://www.iwar.org.uk/iwar/resources/us/dsb/iwdmain.htm, (7. april 2006)

Zgornja slika prikazuje več aspektov, ki informacijsko vojskovanje ločijo od klasičnega vojskovanja in ga naredijo mnogo bolj nepredvidljivega in vseprisotnega. Informacijsko vojskovanje ponuja mnogo zaščitnih tančic, ki si jih lahko nadene napadalec; lahko se **skrije v mrežo** s pomočjo že vnaprej osvojenega sistema in z njega sproži napad. **Pomanjkanje geografskih, prostorskih in političnih omejitev** v kibernetskem prostoru še poveča možnost anonimnosti. IV je relativno poceni v primerjavi s konvencionalnim vojskovanjem in omogoča visoko vrednost doseženih rezultatov kljub **nizkim stroškom** in **relativno preprosti opremi in tehnologiji**, ki je za to potrebna – potrebno pa je **vrhunsko znanje**. Poleg tega **nejasna mednarodna zakonodaja**, oziroma zakonodaja po nekaterih državah, tovrstnega delovanja sploh ne preganja in je potemtakem lahko povsem legalno. Bistvena razlika s konvencionalnim

vojskovanjem je tudi ta, da je nasprotnik pri IV **anonimen**. Pomembna razlika pa je tudi ta, da je **težko določiti odgovorne** znotraj napadene organizacije, ki so odgovorni za to, da je tovrsten napad lahko uspešen. Vseskozi je potrebno upoštevati, da IV ni omejeno na napade na računalnike. Potencialne tarče IV lahko postanejo informacije same, informacijski sistemi, ljudje, pripomočki za oskrbo bistvenih informacijsko-odvisnih funkcij. Oblike napada so lahko kibernetske ali fizične in nenazadnje, IV je izredno prilagodljivo in akterji se neprestano izpopolnjujejo in učijo iz pridobljenih izkušenj.

4. INTERNET IN VARNOST POSAMEZNIKA

V prejšnjem poglavju sem podrobneje preučil teoretično podlago za mojo diplomsko nalogo. Opredelil sem temeljne pojme in koncepte, ki so potrebni za lažje razumevanje poglavja, ki je pred mano. Dotaknil sem se vprašanja sodobne varnostne paradigme, ki že vključuje koncept človekove varnosti in s tem varnost posameznika. Nadalje sem opredelil koncepta informacijske varnosti in informacijskega vojskovanja. V informacijskem vojskovanju sem omenil razdelitev po Schwartau, kjer je prvi razred napadov predstavljalo ogrožanje posameznikove varnosti in zasebnosti. Moja diplomska naloga pa obravnava prav to temo, varnost posameznika na internetu in poglavje pred vami ima namen predstaviti nevarnosti, ki posamezniku grozijo preko medmrežja, hkrati pa tudi nekatere preventivne ukrepe (zaščitne) in previdnosti, ki se jih vsak posameznik lahko posluži kot uporabnik interneta.

4.1. Nevarnosti in grožnje

To poglavje bom razdelil na tri podpoglavja. V prvem podpoglavju bom opisal grožnje, ki so povzročene (zlo)namerno in predstavljajo največjo nevarnost za posameznika. Drugi dve, krajši podpoglavji, pa bosta opredelili nenamerne grožnje posamezniku ter fizične grožnje, ki lahko onemogočijo uporabniku dostop do interneta ali njegovo uporabo. Razdelitev groženj je torej sledeča:

- namerne grožnje,
- nenamerne grožnje,
- fizične grožnje.

4.1.1. Namerne grožnje

Pod namerne grožnje sem uvrstil zahrbtne programe, prevare, sleparije, lovljenje gesel, elektronsko vohljanje, zasipanje z neželeno pošto, nepooblaščene spremembe in vdore. Najbolj nevarni in uporabniku najtežje izsledljivi so zahrbtni programi, zato bom najprej pozornost posvetil prav njim.

4.1.1.1. Zahrbtni programi

Pod prve namerne grožnje sem uvrstil zahrbtne programe[19], ki so povprečnemu uporabniku interneta verjetno najbolj poznani. Malware[20] je tako programska oprema, ki je ustvarjena z namenom vtihotapljenja v računalniški sistem brez vednosti lastnika in je pogosto označena kot računalniški onesnaževalec. Mnogo uporabnikov tovrstnih programov ne razlikuje in je za njih vse virus, kar pa seveda ni dovolj točno. V malware[21] kategorijo spadajo "virusi", "črvi", "trojanski konji", "logične bombe", "zajci", "bakterije"[22] ter vohunski in oglaševalski programi. Pogosto prihaja tudi do zamenjav malware-a in programskih napak v programih, kar pa seveda ni pravilno, kajti programi imajo legitimen namen (bistvena razlika z malware-om), žal pa napake pri pisanju programov lahko tudi povzročijo podobne posledico kot pravi malware. Iz tovrstnih napak tudi izhajajo zahrbtni programi, kajti začetki segajo prav v prve

[19] Besedna zveza "zahrbtni programi" je moj poskus prevoda angleškega termina "malicious software". Lahko uporabimo tudi direktni prevod, ki bi se glasil zlonamerna programska oprema. V računalniškem slengu pa sta za tovrstne grožnje uporabljena tudi morfema obeh besed združena v eno - "malware".
[20] "Malware" – okrajšava besedne zveze "malicious software", slabšalno pa se lahko uporablja tudi "scumware", ki izhaja iz angleške besede scum (izmeček, izvržek) in software (programska oprema).
[21] SI-CERT je v letu 2004 odkril 65 novih različic zlonamernih kod, v letu 2005 pa le 16 novih (http://www.arnes.si/si-cert/, 2. junij 2006).
[22] Narekovaje sem uporabil z namenom da bralec ne bo mislil, da spadajo v to kategorijo pravi črvi, zajci in bakterije. Te besede so seveda vzdevki, ki jih imajo sodobne elektronske grožnje.

programske stavke, kjer so se tovrstne kode zapisovale kot hudomušne šale ali manjši poskusi prodorov v sistem.

Računalniški programi so posebni algoritmi, zapisani v obliki kod, ki računalniku dajejo navodila za opravljanje določenih nalog. Vsak pozna dobronamerne pisane programe, ki jih uporabljamo vsak dan, kot sta na primer operacijska sistema Windows ali Linux ter druge uporabne aplikacije kot so na primer kalkulator, urejevalniki besedil, igre, etc. Ko nekdo napiše program, ki ni dobronameren in ima namen z njim nekaj ukrasti, se okoristiti, povzročiti nevšečnosti, motnje ali celo uničiti delo nekoga drugega, takrat tak program imenujemo zlonameren program – malware. Zlonameren program lahko povzročijo mnogo različnih nevšečnosti:

- se skrivno in sam od sebe reproducira,
- se poskusi skriti pred običajnimi postopki odkrivanja (npr. spreminja svoje ime) in odstranitve (ugašanje proti-virusnih programov) zlonamernih programov,
- se razširja in razmnožuje po omrežju, preko elektronske pošte, po nezaščitenem razširjanju datotek, ali izkorišča varnostne luknje na drugih računalnikih,
- spreminja operacijski sistem ali druge legitimne programe,
- se kopira na gibke diske, USB hranilne enote, CD/DVD-/+R/W diske ter druge hranilne enote,
- pošlje osebne informacije zbrane z okuženega računalnika nazaj k avtorju malware-a ali njegovim pomočnikom, za namene kraje identitete ali zbiranje tržnih informacij,
- prikazuje neželjene oglasne pasice na spletnih straneh ali v "pop-up"[23] oknih,
- dovoli zlonamernim uporabnikom, da nadzirajo vaš računalnik preko mreže ter
- zbriše, spremeni ali poškoduje datoteke in dokumente.

(http://www.rice.edu/it/resources/security/mal_software.html, 10. maj 2006)

Zlonamerni programi imajo lahko neke posebne lastnosti, na podlagi katerih jih lahko razvrstimo po sklopih, kar bom naredil na naslednjih straneh.

VIRUSI

[23] "pop-up" – okence brskalnika, ki se odpre zunaj našega spletnega brskalnika in je ob množici le teh lahko izredno moteče

Virus je samoreprodukcijski program, ki kopira svojo lastno kodo tako, da se pripne na druge izvršljive datoteke; ko se ta z virusom okužena datoteka zažene (obvezna uporabnikova aktivnost), hkrati zažene tudi virus. Virus je tako računalniška koda, ki je napisana z izrecnim namenom samodejnega širjenja. Ime je ta grožnja dobila zaradi podobnosti z biološkim virusom, kajti le ta prav tako išče gostitelja v živih celicah in se v njih replicira. Analogija z biološkim virusom se prav tako nadaljuje tudi pri prenašanju računalniškega virusa, ker kadar želimo povedati, da je nek program opremljen z virusom rečemo, da je okužen. Pomembna lastnost virusa je ta, da lahko poškoduje le programsko opremo in ne strojne opreme. Očiten primer datoteke, ki je lahko okužena z virusom je lahko nek program (*.com* ali *.exe* datoteka), dandanes pa je z uporabo interneta in različnih programov nevarnost dobila še večje razsežnosti, kajti določeni programi, ki se uporabljajo na internetnih straneh lahko potencialno vsebujejo viruse, ki se ob ogledu take strani prenesejo na naš računalnik. (Introduction to Viruses, 2006: http://www.cknow.com/vtutor/Introductionto Viruses.html, 5. maj 2006)

Čeprav so virusi[24] lahko potencialno uničujoči (izguba podatkov lahko tudi uničenje strojne opreme), jih je večina bolj blage narave, ki so lahko le moteč dejavnik, vsakdanja nadloga ali pa imajo lahko še nežnejše učinke[25]. Lahko pa virusi naredijo tudi več škode, kajti spreminjanje za uporabnika pomembnih programov in onemogočanje delovanja le teh ima lahko daljnosežne učinke. Okuženi računalnik pa po nepotrebnem svoje zmogljivosti uporablja tudi za razširjanje virusa, kar je še dodaten negativen dejavnik.

Naj omenim le en bolj znan primer enostavnih a izredno učinkovitih virusov. Virus Melissa je leta 1999 povzročil tako močan DoS med programi za odjemanje pošte, da so morali pri Microsoftu in drugih večjih ponudnikih tovrstnih storitev popolnoma izklopiti delovanje le teh, dokler se virusa ni zadržalo. Virus sam je bil elektronsko sporočilo z okuženo priponko v obliki datoteke urejevalnika besedil. Njegova edina funkcija pa je bila, da se razpošlje prvim petdesetim vpisanim uporabnikom v imeniku okuženega računalnika in ta funkcija je popolnoma zaustavila

[24] Prvi računalniški virus, ki je zapustil svoj matični računalnik je nosil ime "Elk Cloner" in ga je napisal 15-letni dijak (leta 1982) Rich Skenda in njegova edina naloga je bila, da se razširi preko gibkih diskov. Imel pa je še tole zanimivo lastnost, da je okuženi računalnik ob vsakem 50-tem zagonu na zaslonu prikazal hudomušno pesem. Prvi virus, ki je nadlegoval PC-je pa je bil "Brain" (leta 1986), ki naj bi oglaševal računalniško trgovino v Pakistanu. Napisan pa je bil za program Microsoft DOS (BBC News, http://news.bbc.co.uk/1/hi/technology/4630910.stm, 3. maj 2006).

[25] Tak primer je sprememba miškinega kazalca iz puščice "↖" v recimo srček "♥".

razpošiljanje elektronske pošte vseh uporabnikov na določenih strežnikih, zaradi DoS. (Brain, 2006: http://www.howstuffworks.com/virus.htm, 9. maj 2006)

Virus je dandanes vseprisotna nadloga računalniške varnosti in tudi že varnosti mobilne telefonske tehnologije[26], ki je časih celo neizogibna kljub največjim naporom za obrambo pred njo. Vendar pa v dobi interneta in omrežij izgublja na pomenu napram drugim grožnjam, ki so danes bolj prisotne. Tak primer so računalniški črvi.

ČRVI

Računalniški črv[27] je nadgradnja računalniškega virusa. Črv je **samoreprodukcijski program**, ki izdeluje svoje kopije in se **razpošilja** naokoli. Za razliko od virusa ne potrebuje drugega programa, da bi se nanj navezal in se razmnoževal. Tako je črv na nek način samostojen virus ali podzvrst le tega (TechFaq, http://www.tech-faq.com/computer-worm-virus.shtml, 10. maj 2006).

Lahko izkorišča pomanjkljivosti na računalnikih, ki omogočajo prenosljivost datotek. S tem, ko se črv razmnožuje in razpošilja naokoli direktno škoduje mreži na katero je okuženi računalnik povezan, saj ji povzroča nepotrebno delo in zavzema prostor ter pasovno širino, ki bi bila drugače na voljo za prenos drugih datotek. Tako s svojim delovanjem ne jemlje računalniških zmogljivosti le računalniku, ki se je okužil, temveč z repliciranjem in razpošiljanjem tudi ovira in otežuje delovanje mreže. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, kar vpliva na odzivnost in hitrost brskanja po internetu in odpiranju novih strani. Zato so računalniški črvi največkrat narejeni z namenom onesposobiti delovanje določenih mrež ali strežnikov zaradi DoS. Ta lastnost pa znatno pridobi na pomenu ob dejstvu, da je vse več in več računalnikov povezanih v mrežo, internet. Tovrstni zlonamerni programi s pridom izkoriščajo današnje odjemalce spletne pošte, kjer se vsak dan

[26] Leta 2004 se je pojavil prvi virus, ki je deloval na operacijskih sistemih mobilnih telefonov. S pomočjo bluetooth komunikacije je okužil mobilne telefone z operacijskim sistemom Sybian (http://www.f-secure.si/2004/, 2. junij 2006). Stvar postane še bolj zanimiva, če dodam da se v najsodobnejši avtomobilski industriji bluetooth prav tako uporablja za komunikacijo telefona z avtomobilom. V primeru da bi se tak virus prenesel tudi na avtomobilov operacijski sistem in onemogočil delovanje določenih sistemov pa zadeva postane že resno zaskrbljujoča.

[27] Ime "črv" izhaja iz romana Johna Brunnerja, The Shockwave Rider, kjer je v tej znanstveni fikciji junak uporabil svoje računalniško znanje za skovanje računalniškega programa, ki ga je poimenoval "worm" (ang. črv).

odkrije kakšna nova pomanjkljivost v programu, ki jo nepridipravi izkoristijo še preden avtor programa izda popravek, ki odkrito napako popravi[28].

Zelo znan računalniški črv[29], SQL Slammer, se je leta 2003 v ZDA širil s tako hitrostjo, da je v nekaj urah upočasnil delovanje korporacijskih in vladnih sistemov do te mere, da so prenehali delovati. Čeprav črv sam direktno ni povzročil nobene škode, pa je bila posredno povzročena škoda velika. Na določenih bankomatih je bil onemogočen dvig denarja, letalske družbe so morale začasno zaustaviti določene linije, vse to zaradi datoteke velike nekaj kB. Strokovnjaki so ta napad označili kot najbolj škodljiv v zadnjih 18 mesecih, saj je imel učinek v obliki DoS na omrežja v Aziji, Evropi in Ameriki. (http://www.cnn.com/2003/TECH/internet/01/25 /internet.attack/, 10. maj 2006)

TROJANSKI KONJI

Trojanski konj[30] je zlonameren program, ki je skrit ali spretno vtkan v nek drug legitimen program. Tako se na prvi pogled zdi uporaben (ali vsaj neškodljiv), v resnici pa je lahko izredno škodljiv[31]. Pogosto se uporablja tudi skrajšano poimenovanje "trojan". Poznamo dve obliki trojanskih konjev. Prva je s posegom crackerja[32] spremenjen drugače uporaben program, ki po novem vsebuje zlonamerno kodo, ki se

[28] Za črva SQL Slammer, ki je izkoriščal določene pomanjkljivosti v Windowsih je Microsoft izdal popravek že šest mesecev preden je bil črv napisan, vendar velika večina uporabnikov ni namestila popravkov, kar je posledično vplivalo na veliko in hitro razširitev tega črva. To je lep primer kako lahko uporabnikovo neposodabljanje programske opreme in neažurnost z različnimi varnostnimi informacijami privede do problemov.

[29] Zelo znan je tudi LoveBug črv, ki je maja 2000 obkrožil svet in ga ustavil za trenutek. Virus je prispel do uporabnika preko odjemalca spletne pošte s posvetilom "I LOVE YOU" in je vseboval priponko, ki je ob odprtju le te razposlala svoje kopije vsem naslovom v imeniku uporabnika; poleg tega pa je zbrisal vse *.jpeg* in *.mp3* datoteke na trdem disku uporabnika, kar je bil seveda mnogo hujši udarec za lastnika okuženega računalnika. Virus se je širil izredno hitro in je v prvem dnevu dosegel 45 milijonov uporabnikov po svetu. (ILOVEYOU Virus, 2006: http://searchsecurity.techtarget.com/sDefinition /03.html , 8.maj 2006) Zanimiv pa je podatek, da so avtorja črva odkrili na Filipinih, vendar ga zaradi tamkajšnje zakonodaje, ki ni pripisovala kazni za tovrstna dejanja niso kazensko preganjali. (Silverman, 2003: http://www.pbs.org/ newshour/science/computer_worms/famous.html, 9. maj 2006)

[30] Termin "trojanski konj" izhaja iz Vergilovega epa Eneida ter domnevnega mita o Trojanski vojni. Mitološki trojanski konj je bil navidezno darilo v katerem so se skrivali grški vojaki, ki so s prevaro in ukano zavzeli Trojo.

[31] Primer trojana bi lahko izgledal kot program "prOn.jpg.exe", ki bi se izdajal za pornografsko sliko z določene spletne strani, ampak bi ob zagonu izvedel kakšno neželeno operacijo, na primer zbrisal vse *.jpg* datoteke na disku.

[32] Oseba, ki z modificiranjem programa odstrani zakodirano začito pred presnemavanjem, kopiranjem, itd. Danes tovrstno početje ni več le nelegalno, temveč že spada pod kriminal.

izvrši, ko uporabnik zažene program[33] - več o nepooblaščenih spremembah kasneje. Druga oblika pa je samostojen program, ki je zamaskiran kot nekaj drugega (npr. igra ali slika) z namenom prevarati uporabnika, da bi le ta zagnal program in s tem sprožil zlonamerno kodo (http://www.symantec.com/avcenter/venc/data/trojan.horse.html, 2. junij 2006). Trojanski konj ne more delovati sam od sebe, temveč potrebuje pomoč uporabnika (podobno kot so Grki potrebovali Trojansko pomoč za odpiranje vrat in vnos konja v trdnjavo). Tako mora tudi vsaka nova žrtev znova zagnati program, saj se trojanski konj sam od sebe ne razmnožuje in razpošilja (http://www.irchelp.org/irchelp/security/trojan.html, 2. junij 2006; http://en.wikipedia.org/wiki/Trojan_horse_(computing), 10. maj 2006).

Tukaj je bistvena razlika napram virusom in črvom, saj trojanski konj izkorišča koncept socialnega inženiringa[34] namesto napak v računalniških programih in pomanjkljivi računalniški varnosti. Dandanes pa so tovrstni škodljivi programi med sabo že tako pomešani in prilagojeni, da je težko potegniti ločnico med virusom, črvom in trojanskim konjem, saj ima lahko nek trojanski konj v sebi tudi črva ali podobno zlonamerno kodo. Za lažjo primerljivost in razlikovanje med različnimi zlonamernimi programi[35] sem naredil spodnjo tabelo.

[33] Med tovrstne potencialno okužene programe sodijo različni vremenski napovedovalci, programi za nastavljanje točnega datuma, programi za izmenjavo datotek (P2P) preko interneta, itd.

[34] Ang. "social engineering" – postopek in praksa pridobivanja zaupnih informacij s pomočjo manipulacije in zvijače od legitimnih uporabnikov določenih storitev.

[35] Zanimiva pa je novica, ki je v maju 2006 presenetila P2P uporabnike, saj so strokovnjaki informacijsko varnostnega podjetja Sophos na svetovnem spletu odkrili nenavadno škodljivo programsko kodo, ki iz trdega diska računalnika odstranjuje piratske vsebine. Gre za trojanskega konja Erazer-A, ki se izredno hitro širi preko P2P omrežij. Zlonamerna koda odstranjuje večpredstavnostne vsebine iz map, ki jih pirati uporabljajo za spletno izmenjavo bolj ali manj legalnih datotek. Trojanec Erazer-A pri delovanju zbira tudi podatke o okuženem računalniškem sistemu. Škodljiva koda seveda ne loči med piratskimi in legalnimi vsebinami, kar pomeni, da lahko iz trdega diska izbriše tudi vsebine, ki niso avtorsko zaščitene, kar lahko povzroči veliko škode uporabniku (http://www.racunalniske-novice.com/main/index.php?page=clanek&cmd, 22. maj 2006). Zanimivo bi bilo poiskati tudi avtorja tega trojanca, saj zagotovo to ni eden izmed nadebudnih uporabnikov P2P omrežij, temveč prej kakšno podjetje za trženje avtorskih pravic. Tovrstno početje pa seveda ni v skladu z zakonodajo, vendar ima ta program olajševalno okoliščino, kajti deluje v "dobrem duhu" proti ilegalni izmenjavi avtorsko zaščitenih vsebin.

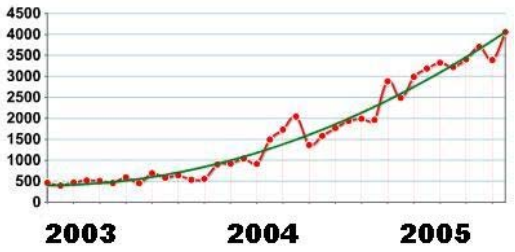
Tabela 3: Različne značilnosti zlonamernih programov

Značilnosti	Virus	Črv	Trojanski konj
Reprodukcija	reproducira se tako, da se pripne na druge programe, okužen program nato deluje kot prenašalec	reproducira se sam, tako da izdeluje svoje kopije	se ne reproducira
Prenos	okužen program se preko medija prenese na drug računalnik, kjer se ponovno začne proces reprodukcije	"mrežni črvi" sami najdejo možnosti širjenja preko mreže, drugi črvi se širijo preko okuženih medijev	prevarani uporabnik sam požene zlonameren program
Odvisnost	od drugih programov na katere se navežejo	le od mreže s pomočjo katere se širi	od uporabnikove nevednosti

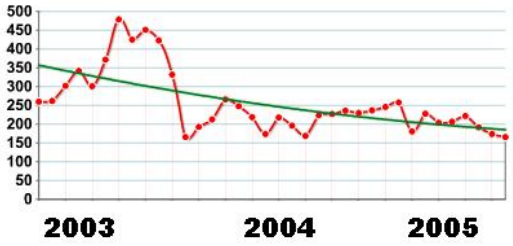
Trendi v lanskem letu (2005), se nagibajo k favoriziranju trojanskih konjev pred virusi in črvi. Razlogi za to tičijo v večji enostavnosti izdelave trojanskega konja in hitrem večanju števila neizkušeni uporabnikov, ki se ne zavedajo preteče nevarnosti. Računalniško podzemlje tako postaja čedalje bolj kriminalno in se osredotoča na dostop do podatkov, ki omogočajo hitre zaslužke. Med te pa sodijo bančni računi ter gesla za dostop, lastniške informacije in spletne igre na srečo z uporabniškimi imeni in gesli (Mashevsky, 2006: http://www.viruslist.com/en/analysis?pubid=178949694, 6. maj 2006).

Spodnje slike prikazujejo izjemen porast trojanskih konjev in zmeren porast drugih zlonamernih programov, ob tem pa število virusov in črvov upada.

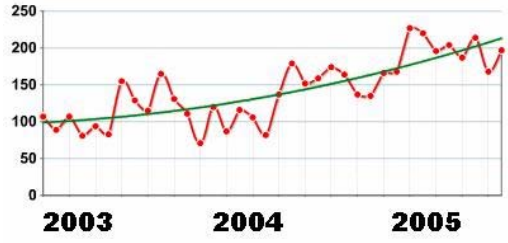
Slika 2: Prikaz porasta trojanskih konjev



Slika 3: Prikaz upada virusov in črvov



Slika 4: Prikaz porasta drugih zlonamernih programov



Slike prirejene po: Mashevsky, 2006: http://www.viruslist.com/en/analysis ?pubid=178949694, 6. maj 2006.

Vse tri slike prikazujejo število odkritih zlonamernih programov v enem mesecu s pomočjo komercialnega ponudnika protivirusne zaščite Kaspersky. Prav tako pa tudi drugi ponudniki varnostne zaščite opažajo podobne trende. Tako pri podjetju PandaLabs prav tako ugotavljajo da se je število trojanskih konjev dramatično povečalo od leta 2004 naprej, predvsem na račun črvov in virusov. Razlogi pa so podobni kot sem jih že sam zgoraj navedel, prednjači pa pridobitev finančnih prihodkov s pomočjo zlonamernih kod. Direktor podjetja PandaLabs Luis Corrons razlaga: "Trojanci so zelo prilagodljiva vrsta škodljivih programski kod, saj so lahko narejeni za izvajanje zelo različnih zlonamernih akcij, ne da bi jih uporabniki opazili. Na ta način lahko ustvarijo stranska vrata, ki jih lahko internetni prevaranti uporabijo za nadzor drugih računalnikov na daljavo, krajo podatkov, ki jih vpisuje uporabnik za dostop do spletnih storitev ali celo za spreminjanje sistema, da bi usmerili uporabnike, na lažne spletne strani, da bi posledično kradli osebne podatke. Druge vrste zlonamernih kod, kot so črvi, imajo običajno zelo vidno delovanje, ki privleče pozornost medijev kot tudi uporabnikov, ki jih hitro želijo odstraniti iz svojih sistemov. Zato tovrstni škodljivi programi niso primerni za današnje internetne prevarante, ki predvsem iščejo finančne

koristi" (http://www.racunalniske-novice.com/main/index.php?page=clanek2a915d2, 29. maj 2006).

Razvidno je, da se tudi vodilni v podjetjih za varnost na internetu zavedajo vseh groženj, ki jih omenjam v svoji diplomski nalogi. Nekaj od teh nevarnosti sledi v nadaljevanju, ki so prav tako ključnega pomena za uporabnikovo varnost.

LOGIČNE-ČASOVNE BOMBE

Logična bomba[36] je del programske kode, ki je namerno vnesen v določen programski sistem, ki bo sprožil svojo zlonamerno funkcijo, ko so izpolnjeni določeni pogoji (v primeru časovne opredelitve pogojev govorimo o časovni bombi[37]). Virusi in črvi pogosto vsebujejo logične bombe, ki zadržijo izvrševanje virusa. Le to pa ima izredno pomembno vlogo, kajti dokler se zlonamerna funkcija ne sproži, a se program kljub temu širi, se virusa/črva ne odkrije. Ko pa so določeni pogoji izpolnjeni, takrat logična bomba sproži delovanje zlonamernih kod in škoda, ki je povzročena, je mnogo večja, kot če bi se virus ali črv sprožil že takoj. Lahko rečemo tudi da so logične bombe virusi, ki imajo zakasnjeno delovanje (http://www.tech-faq.com/logic-bomb.shtml, 10. maj 2006).

Kot sem že omenili je najbolj pogost sprožilec logične bombe datum (časovna bomba). Taka časovna bomba spremlja sistemski datum in čas in ob prednastavljenem datumu in uri sproži svojo zlonamerno kodo. Lahko pa logična bomba sledi tudi različnim drugim dogodkom, spremembam v datoteki, spremembam v velikosti določenih podatkov, itd. Zelo pretkana pa je oblika logične bombe, ki se sproži, če se nekaj ne zgodi. Tako lahko računalniški programer v določenem podjetju nastavi logično bombo, ki se bo sprožila, če se na primer njegovo ime ne pojavi več na seznamu zaposlenih, ali se sam ne prijavi v sistem. Tovrstne zlorabe so seveda kaznive[38]. Logična bomba se sama po sebi ne razmnožuje in je v primerjavi z virusi in črvi "bolj

[36] Ang. "logic bomb" - primerjavo z resničnim svetom lahko naredimo s primerjanjem logične bombe s protipehotno mino. Le ta prav tako čaka in le ob primernem dogodku sproži svoje mehanizme in deluje zlonamerno.

[37] ang. "time bomb"

[38] Prvi tak primer je bil leta 1992, ko je računalniški programer moral plačati kazen v višini dveh svojih mesečnih prejemkov, zaradi tega, ker je v svojem podjetju General Motors nastavil logično bombo. Njegov namen je bil, da ga bodo v podjetju najeli za rešitev problema in mu seveda bogato poplačali. Na njegovo škodo se je sreča obrnila drugače. (Kabay, 2002: http://www.networkworld.com/newsletters /sec/2002/01514405.html, 9. maj 2006)

etična", saj je ponavadi usmerjena proti točno določenem uporabniku, kar za viruse in črve ne velja.

Ob tem lahko omenim, da nekakšne logične bombe uporabljajo podjetja za možnost preizkusa svojih programov s strani uporabnikov. Po določenem času uporabe, program zahteva registracijo ali pa se izbriše iz sistema. Tovrstni programi seveda ne sodijo v kategorijo zlonamernih programov, velja pa omeniti to posebnost.

ZAJCI

Zajec[39] je zlonameren program (podzvrst črva) , ki ima eno glavno nalogo; ta je da se razmnožuje do te mere, da porabi vsa sistemska sredstva. Lahko je to celoten prostor na trdem disku ali pa celotna računska sposobnost procesorja. Zajec je tako samostojen program, ki iz vsake originalne datoteke naredi dve identični kopiji, ti dve naprej naredita štiri identične kopije originala in tako naprej. Prej ali slej se porabi vsa procesorska moč ali pa zmanjka prostora na disku (Mateti, 2006: http://www.astalavista.com/index.php?section=docsys&cmd=details&id=25, 10. maj 2006).

Tako tudi ime tega malware-a izhaja iz narave, kjer sposobnost razmnoževanja nakazuje na naravno izredno plodne zajce.

BAKTERIJE

Bakterija[40] je zlonameren program (podzvrst virusa), ki se razmnožuje z namenom porabiti vsa sistemska sredstva, še posebno CPU moč. To počne tako, da se pripne k programom, še posebno k operacijskim sistemom.

VOHUNSKI PROGRAMI

Za vohunski program[41] bi lahko rekli, da je vsak program, ki prikrito zbira uporabnikove informacije preko uporabnikove internetne povezave, seveda brez vednosti uporabnika. Tovrstni vohunski programi, so pogosto spretno vprogramirani v freeware ali shareware[42] programe, ki jih je mogoče dobiti preko interneta. Vendar pa je potrebno omeniti, da originalni freeware in shareware ne vsebujeta vohunskih

[39] ang. rabbit – vzdevek za tovrstne programe
[40] ang. bacteria – vzdevek za tovrstne programe
[41] ang. spyware – spy software, vzdevek za vohunske programe; lahko tudi spybot – okrajšava za spy robot, vohunski robot; lahko tudi tracking software – sledilni program
[42] glej slovarček

programov. Vohunske programe vsebuje šele modificiran free(share)ware, ki je na voljo na določenih straneh. Zato je priporočljivo da brezplačne programe naložimo z interneta z njihovih uradnih strani, ne pa kakšnih drugih bolj "poslovno" orientiranih internetnih strani ali podjetij. Potem ko uporabnik nevede namesti vohunski program, le ta nadzira uporabnikovo delovanje, brskanje po internetu in v ozadju pošilja podatke o uporabnikovem početju avtorju vohunskega programa, ki lahko take podatke izkoristi v svoje namene. Tovrstni vohunski programi so sposobni pomnjenja elektronskih naslovov in celo določenih gesel ter številk bančnih kartic (http://www.webopedia.com /TERM/s/spyware.html, 15. maj 2006). Lahko pa nam tudi spremeni nastavitve na našem računalniku in tako onemogoča naše delo. Spyware je tako podoben trojanskim konjem, saj se z uporabnikovo pomočjo in v njegovi nevednosti namesti na računalnik in izvaja aktivnosti, ki niso uporabniku v korist. Spyware se najpogosteje nahaja v programih[43], ki so namenjeni za ilegalno izmenjavo datotek, v t.i. P2P omrežjih, vendar to večine mladih uporabnikov ne odvrne od uporabe le teh[44]. Pogosto pa se nahaja tudi v drugih programih, ki na prvi pogled delujejo povsem neškodljivo, kot so razni napovedovalci vremena, preproste računalniške igrice, aplikacije, ki naj bi pospešile delovanje vašega računalnika, emocionalne ikone ali druge oblike prikazovanja smeškotov ter drugi programi z na videz neškodljivo vsebino.

Poleg kršenja uporabnikove zasebnosti in etike pri distribuciji programov pa spyware tudi izrablja računalnikove zmogljivosti in pasovno širino njegove internetne povezave z obdelavo in pošiljanjem podatkov. Ker tovrstni programi, ki delujejo v ozadju, uporabljajo delovni spomin in procesorsko moč, lahko pretirana razširjenost le teh povzroči tudi nestabilnost celotnega sistema ali celo sesutje sistema. Vohunski programi so lahko tudi povsem samostojni in imajo tudi različne sposobnosti:

⇒ zmožnost nadziranja vsakega pritiska uporabnika na tipkovnico ali druge vnosne naprave (miška, igralna ploščica, igralna palica, itd.),

⇒ pregledovanje diska za določene datoteke,

[43] Tak primer je bil KaZaA (tudi eXeem), ki je kljub izredni razširjenosti z novimi verzijami prinesel tudi mnogo vohunskih programov, ki so raziskovali naše početje na internetu in o tem obveščali avtorje spyware-a. Tako se je večina P2P uporabnikov usmerila na druge oblike izmenjave datotek in druge tovrstne programe. Popularna sta predvsem eMule in programi za t.i. torrent izmenjavo datotek.

[44] Znani so že primeri posameznikov, ki so bili kazensko preganjani v ZDA zaradi ilegalne izmenjave datotek. Roka pravice pa se osredotoča predvsem na uporabnike, ki tovrstno izmenjavo omogočajo (http://news.bbc.co.uk/1/hi/technology/4875142.stm, 2. junij 2006).

⇒ pomnjenje obiska na določenih straneh,

⇒ zmanjšanje računalnikovih zmogljivosti ter sesutje sistema,

⇒ prikazovanje neželenih oglasov[45],

⇒ vohunjenje znotraj drugih programov (spletni pogovorni programi kot sta MSN Messenger in Windows Messenger ter urejevalniki besedil),

⇒ namestitev drugih neželenih programov,

⇒ branje piškotkov[46],

⇒ spreminjanje privzete domače strani na brskalniku ter

⇒ stalno pošiljanje informacij nazaj k avtorju spyware-a, ki lahko te podatke uporabi sam ali pa jih proda drugim zainteresiranim osebkom.

Iz zgornjih lastnosti vohunskih programov je zlahka razvidno da so lahko zelo škodljivi. V kombinaciji s socialnim inženiringom lahko s pomočjo spyware-a dobi nek posameznik kopico informacij, ki jih lahko zlorabi nam v škodo ter se v virtualni realnosti predstavlja celo z našo osebnostjo[47]. Tovrstno delovanje je izredno zahtevno in težavno za preprečiti, zato je preventivno delovanje prvotnega pomena in najboljša zaščita. Tako je potrebno nalaganje vsebin le s strani, ki jim zaupamo ter vedno prebirati izjave o zasebnosti[48], ki jih je potrebno potrditi pred namestitvijo programa. Te izjave pa so pogosto izredno dolgočasne in napisane v strokovnem pravnem jeziku ter povprečnemu uporabniku interneta manj razumljive, zato je po svoje razumljivo, da jih večina uporabnikov ne prebere (http://www.webopedia.com/TERM/s/spyware.html, 15. maj 2006).

Najbolj vsiljivi zlonamerni programi uporabljajo kopico trikov, ki uporabnika silijo v namestitev. Prva oblika je skrivanje znotraj drugih programov, kar sem že omenil. Druga, bolj moteča, pa je neprestano siljenje v uporabnika, ki ob vsakem obisku določene strani prikaže okno, ki mu ponuja določeno storitev. Čeprav uporabnik zavrne to storitev, pa se okno ponovno pojavi ob ponovnem obisku te strani. Tovrstno neprestano bombardiranje z vprašanjem marsikoga razjezi do te mere, da klikne na

[45] Glej naslednje podpoglavje → oglaševalski programi
[46] ang. "cookie"
[47] ang. identity theft – kraja osebnosti
[48] Na tak način se avtorji zlonamernih programov zaščitijo pred roko pravice, saj jim klik na "sprejemam pogoje delovanja programa" ob namestitvi, omogoča lahko pot za izmikanje in prelaganje krivde na uporabnika in njegovo strinjanje s početjem programa.

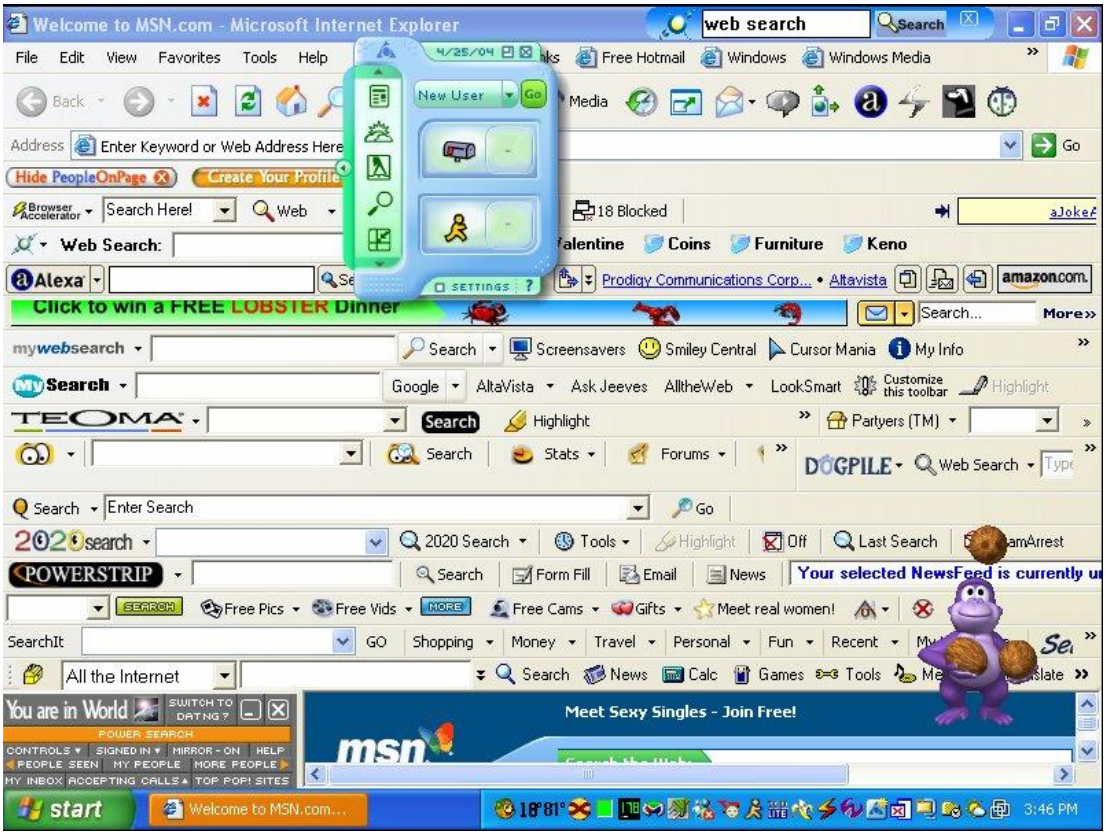
"sprejmem" ali "potrdi", čemur seveda sledi namestitev vohunskega programa. S pomočjo pop-up oken lahko celo vsilijo namestitev manj izkušenemu uporabniku, kljub "pravim klikom", saj lahko tudi s klikom na gumbe "prekini" ali "zapri okno" tovrsten program sproži namestitev na naš računalnik. Zato je zelo priporočljivo, da tovrstna okna zapiramo v opravilni vrstici ali pa kar v upravljalniku opravil[49], ter se tako izognemo neželeni namestitvi. Spletne varnostne nastavitve našega brskalnika ter zasebnost pa nastavimo na karseda visoko raven. Tretja oblika pretentanja uporabnika pa je pretveza, da uporabnik potrebuje nek program za ogled določene strani ali recimo voščilnice, ki mu jo je poslal prijatelj. Še ena izmed metod s pomočjo katerih se lahko ukani uporabnika pa je da vohunski program izgleda kot nek dodatek k že nameščenim programom znanih proizvajalcev. To se doseže tako, da program zveni kot neko znano ime, npr. "winstartup" in uporabnik seveda misli, da je to nek sistemski podprogram, ki mora delovati v ozadju.

Zanimivo je da je spyware povzročil tako velik odziv pri uporabnikih interneta, da so podjetja, ki se ukvarjajo z borbo proti spyware-u, akademiki, raziskovalci in drugi zainteresirani ustanovili celo organizacijo, ki se imenuje Anti-Spyware Coalition. Njihov glavni namen pa je graditi nek konsenz glede definicij spyware-a in deliti izkušnje glede problemov, ki jih povzročajo spyware in drugi zlonamerni programi ter neželene tehnologije (http://www.antispywarecoalition.org/about/, 15. maj 2006).

Slika v nadaljevanju izredno nazorno prikazuje, kako lahko vohunski programi popolnoma zasedejo okno brskalnika in nam onemogočijo delo z njim. V opravilni vrstici na dnu je prav tako vidna množica programov, ki tečejo v ozadju in tako porabljajo procesorsko moč in s tem oškodujejo uporabnika.

[49] ang. task manager, v operacijskem sistemu Windows

Slika 5: Primer poplave spyware-a



Vir: http://upload.wikimedia.org/wikipedia/en//Spyware_infestation.png, 15. maj 2006

Že med lastnostmi vohunskih programov sem omenil, da lahko le ti prikazujejo tudi neželene oglase. Tovrstne programe pa sem uvrstil v posebno kategorijo, ki ji je namenjen naslednji sestavek.

OGLAŠEVALSKI PROGRAMI

Oglaševalski program[50] je kakršenkoli program[51], ki ima sposobnost prikazovanja, predvajanja ali nalaganja oglasov na računalniku, medtem ko se uporablja določen program. Oglaševalski programi so izredno podobni vohunskim programom in so nekakšna podzvrst le teh. Prav tako se namestijo na naš računalnik s podobno tehniko kot trojanski konj. Oglaševalski programi spremljajo naše aktivnosti na internetu in tako si oblikujejo neko podobo o naših interesih, glede na obiskane strani. Njihova temeljna

[50] Ang. "adware" – advertising-supported software, programi podprti z oglaševanjem.
[51] Med bolj znanimi so 123 Messenger, 180 Solutions, Bonzi Buddy, PornDigger!, WINfixer, itd.

naloga je tako poizvedovati za našimi zanimanji in jih posredovati avtorju oglaševalskega programa. Avtor (lahko tudi program sam) pa glede na profil uporabnika prikazuje določene oglase (seveda proti plačilu naročnika oglasov), ki jih uporabnik sam ni želel videti, zato so lahko ob veliki množici le teh izredno moteči. V veliki večini so tovrstni oglaševalski programi zelo podobni vohunskim programom, saj imajo prav tako množico podobnih škodljivih stranskih efektov, ki so za uporabnika izredno neprijetni.

Poznamo pa tudi drugo obliko adware-a, ki je lahko povsem legitimna in legalna. To so programi, za katere uporabnik ne želi plačati nekega zneska. V zameno za uporabo določenega programa pa v ta legitimen program vgrajen adware prikazuje določene sponzorske pasice, ki oglašujejo določene izdelke. Uporabnik ima tako možnost uporabe njemu želenega programa, namesto plačila za ta program pa je izpostavljen prikazovanju oglasov med svojim brskanjem po internetu[52]. Tako je v mnogih primerih oglaševalski program lahko povsem legitimna oblika poplačila za avtorstvo, če uporabnik ne želi plačati za program[53]. Tovrstni oglaševalski program prav tako ne bo hranil naših navad brskanja po internetu, ter jih ne bo pošiljal ali celo prodajal tretjim osebam. Tak legitimen oglaševalski program ima le eno nalogo, prikazovanje oglasov v zameno za uporabo programa in ob nedelovanju programa tudi ne prikazuje oglasov. Takšni programi niso zlonamerni programi, čeprav delujejo povsem na istem principu. Razlika je le v tem, da nam uporabnikom ne povzročajo škode, saj je tovrstno oglaševanje le oblika našega plačila določene storitve ali programa. (http://www.techiwarehouse.com/cms/engine.php?page_id=41cc4355, 15. maj 2006)

S tem sem zaključil pregled zlonamernih programov, ki so po moji oceni med najbolj nevarnimi in najbolj prisotnimi oblikami nevarnosti, ki prežijo nad uporabnikom interneta. V nadaljevanju pa sledijo še druge oblike namernih groženj, ki so prav tako prisotne, vendar ne tako očitno kot v tem podpoglavju omenjeni zlonamerni programi.

---

[52] Najmodernejši adware pa ne deluje le ko brskamo po internetu, temveč je v delovanju ves čas, ko je računalnik vključen. Tako se nam oglasne pasice ali vrstice na ekranu prikazujejo tudi med recimo pisanjem teksta ali poslušanjem glasbe.

[53] Izredno lep primer tovrstnega sodelovanja oglaševalcev in avtorjem programa je odjemalec spletne pošte Eudora. Program lahko kupite ali pa ga naložite in zaženete v oglaševalski izvedbi. Kupljena izvedba je podobna drugim odjemalcem spletne pošte kot je na primer Outlook Express. Oglaševalska izvedba pa namesto plačila prikazuje oglase. Ko uporabnik požene Eudoro, bo ta najprej prikazala oglasno okence, v orodno vrstico pa bo dodala do tri ikone, ki bodo ob kliku nanje odprle novo okno s stranjo sponzorja.

4.1.1.2. Prevare, sleparije

V informacijski dobi je zlonamerno delovanje pogosto delo sleparjev ali pravih zlonamernežev skritih za neko prevleko, masko. Vse to pa ima za sabo nek skrit namen, ki je uporabniku neznan. Te napori pa imajo nekaj skupnega, njihov glavni namen je prevarati uporabnika, da sprejme napačne informacije oziroma naredi napačne poteze na podlagi napačnih informacij. Te napačne informacije pa pridobi iz vira za katerega misli da je avtentičen, vendar je ta vir lahko s pomočjo prevare ponarejen in tako informacije, ki so na voljo ne služijo prvotnemu namenu.

Prevara[54] v računalništvu predstavlja situacijo v kateri se neka oseba ali program uspešno zamaskira kot nekdo drug s ponarejanjem podatkov in tako dobi neko nelegitimno prednost ali korist. Tovrstna dejanja pa lahko razdelimo na več področij. Prvo in za posameznika verjetno najbolj ogrožajoča je kraja identitete, sledijo poneverbe elektronske pošte in spletnih strani.

KRAJA IDENTITETE

Kraja identitete je zlonamerna uporaba identitete neke druge osebe. Sem sodijo zloraba imena, davčne številke, enotne matične številke občana ali elektronskih naslovov oz. katerega drugega osebnega podatka, s pomočjo katerega je možno narediti pravi osebi neko škodo oziroma se okoristiti s tovrstnimi podatki. Najbolj poznana oblika je kraja številk kreditnih kartic, bančnih računov itd. V bolj razvitem zahodnem svetu, kjer pomembno vlogo igrajo tudi zdravniški ali plačilno sposobni podatki se tovrstne informacije lahko uporablja tudi za izsiljevanje. Razkritje tovrstnih podatkov lahko pripeljejo do tožb ali izgube službe ali celo ločitve. Zato je vsak posameznik močno zainteresiran, da določeni osebni podatki ostanejo intimni. Namen tovrstne kraje identitete pa je da se okoristimo z dejanji, ki so na voljo pravemu lastniku. Denningova (1998: 241) našteva kot možne zlorabe dvig sredstev z bančnega računa, prenosi denarja, plačilo nakupov, pridobitev dostopa do informacij zaupnega značaja ali izdajanje dokumentov ali izjav v imenu pravega lastnika identitete. Tat identitete tako s

[54] ang. "spoof" – tovrstno delovanje se v izvirniku imenuje "spoofing" ali "masquerade" - maškarada

pomočjo lažne identitete pridobi vpogled v denarna sredstva, zdravstveno stanje, ter zmožnost spreminjanja le teh, kar je največja grožnja. Tako so najbolj privlačne kraje številk kreditnih kartic, ki v kombinaciji z drugimi osebnimi podatki na določenih internetnih straneh omogočajo nakup. Seveda žrtev takega napada ne ve da se je nakup zgodil, dokler se ob izteku meseca ne izstavi račun, ki ga je seveda potrebno poravnati[55].

Tovrstne poneverbe so vedno posledica vdorov v zasebnost posameznika, le ta pa se lahko zgodi na treh ravneh. Prva raven je strankina zasebnost, saj določena podjetja zbirajo pomembne informacije o posamezniku in če so te informacije nenadoma na voljo (namerno ali nenamerno) se jih lahko spretni posamezniki polastijo in jih uporabijo v zle namene. Druga raven je potrošniška zasebnost v spletnih trgovinah. Le te hranijo podatke o kreditnih karticah in drugih oblikah plačila, hkrati z vsemi podatki, ki so potrebni za izvedbo takega plačila. Tovrstna podjetja so pogosto tarča elektronskih napadov na njihove serverje, saj so podatki v njih izredno "uporabni" za nadaljnje izkoriščanje, hkrati pa z eno potezo pridobimo izredno veliko bazo podatkov. Tretja in zadnja raven posameznikove zasebnosti pa je njegova intima oz. njegova politična prepričanja. Tovrstni podatki so izredno pomembni pri učinkovitem posnemanju neke osebe in torej izredno uporabni za krajo identitete, kajti z intimnimi in težko dostopnimi podatki postane tat identitete mnogo bolj prepričljiv pri predstavljanju svoje lažne identitete[56]. Med druge oblike pridobivanja tovrstnih informacij Federal Trade Commission v ZDA uvršča še krajo zapisov ali informacij iz podjetij ki hranijo te podatke[57] s strani zaposlenih, s podkupovanjem zaposlenih v teh podjetjih ter vdiranjem v njihov računalniški sistem (http://www.consumer.gov/idtheft/, 16. maj 2006).

Proti tovrstnim dejanjem so bili že pred desetletjem sproženi določeni ukrepi (npr. osebne izkaznice v Sloveniji), vendar zagotovila za popolnoma varno identiteto

[55] Danes določene banke omogočajo preverjanje vsakega bančnega nakupa in potrditev le tega preko telefona ali osebno. Tovrstno delovanje seveda povečuje varnost poslovanja s kreditno kartico, vendar vse na račun uporabnosti in enostavnosti nakupov.

[56] Morda se tovrstno delovanje res težje izvede v okolju kot je Slovenija, ki zaradi svoje majhnosti in poznavanju ljudi med sabo onemogoča enostavne prevare. V večjih državah in predvsem večjih podjetjih, kjer je nemogoče osebno poznati vse zaposlene, pa je tovrstno igranje z identitetami lažje izvedljivo. Tako je Združenje odvetnikov v Kaliforniji leta 1998 razglasilo krajo identitet za eno najhitreje rastočih kriminalnih dejanj v ZDA (Denning, 1998: 242). Leta 2003 se je ta rast umirila in ohranja isto raven. Tako je vsako leto 4,25% (9,3 milijona) vseh odraslih v ZDA podvrženim eni izmed oblik kraje identitete, kar je vsekakor veliko. (http://en.wikipedia.org/wiki/Identity_theft, 16. maj 2006)

[57] V ZDA so nekateri osebni podatki javnega značaja. V drugih državah je tovrstne podatke mnogo težje pridobiti, vendar imajo dostop do njih zaposleni in drugi delavci znotraj določenih institucij, tako da tudi ti podatki niso povsem varni.

seveda ne more nuditi nobena tehnologija. Verjetno najbližje je trenutno biometrija[58], ki bi s pomočjo branja šarenice, prstnih odtisov, obraznih potez in drugih bioloških značilnosti posameznika lahko zagotovila pravilno identifikacijo in istovetnost za določene potrebe uporabe identitete.

PONEVERBA ELEKTRONSKE POŠTE

Tovrstne poneverbe elektronske pošte[59] so del vsakdanjika, saj je to ena izmed lažjih oblik prevar, ki pa prav tako lahko povzroči veliko škode. Poneverba elektronske pošte se lahko pojavi v različnih oblikah, vendar imajo vse isti rezultat. Uporabnik dobi elektronsko pošto, ki se zdi kot da je prišla od določenega poznanega vira, vendar je bila poslana z drugega, ponarejenega. Tovrstne poneverbe se pogosto uporabljajo z namenom uporabnika pripraviti v škodljivo izjavo, ki jo nato uporabijo proti njemu v medijih ali drugi zainteresirani javnosti ali za izdajo zaupnih podatkov kot so gesla, številke kreditnih kartic in podobno. Primer ponarejenega elektronskega sporočila, ki bi škodoval vam, lahko vsebuje sledeča obvestila in/ali napotke:

- sistemski administrator vam sporoči, da morate spremeniti svoje geslo na določeno zaporedje črk in številk, ki vam ga navede; hkrati pa vam v istem sporočilu zagrozi, da vam bodo ukinili elektronski predal, če tega ne storite;
- elektronsko sporočilo, ki se predstavlja kot vaš nadrejeni oz. vaš skrbnik elektronskega predala in vas pod to pretvezo naproša da mu pošljete občutljive informacije ali podatke o geslih in uporabniških imenih (http://www.cert.org/tech_tips/email_spoofing.html, 16. maj 2006).

Tovrstne prevare se pogosto predmet delovanja pošiljateljev množičnih elektronskih sporočil oziroma tekmovalnih podjetij, ki želijo očrniti pravega izvirnika, ter tako pridobiti stranke na svojo stran.

[58] Mednarodna biometrična družba ima svojo spletno stran na naslovu: http://tibs.org/biometrics/ (16. maj 2006)
[59] To je moj poizkus prevoda, izvirnik je v ang. E-Mail Forgeries ali Spoofed/Forged E-Mail

PONEVERBA INTERNETNIH STRANI

Poneverba internetnih strani[60] pridobiva na pomenu. Vzrok temu je čedalje večja prisotnost spletnih prenosov denarja, plačil in drugih oblik bančnega poslovanja. Tovrstne prevare[61] se uporabljajo kot zvijača s pomočjo katere se pridobi uporabniška imena in gesla, številke kreditnih kartic in druge pomembne informacije. Postopek pa je lahko sledeč. Najprej s poneverbo elektronskega sporočila povabimo uporabnika na uporabo določene njemu že poznane storitve, seveda pod pretvezo uradne elektronske komunikacije podjetja z uporabnikom (http://www.arnes.si/si-cert/obvestila/2004-06.html, 2. junij 2006). V elektronskem sporočilu uporabnik dobi povezavo na določeno internetno stran, ki samo izgleda tako kot izvirna stran. Uporabnik tako verjame, da je na uradni spletni strani podjetja, kjer opravlja svoje poslovanje (http://en.wikipedia. org/wiki/Phishing, 19. maj 2006).

Tako uporabnik v dobri veri vpiše uporabniško ime in geslo v za to namenjena okenca. Ker pa ponarejena internetna stran nima točno določenih ključev za pristop v sistem, uporabniku sporoči, da je bilo geslo napačno vpisano in ga preusmeri na uradno stran. Uporabnik misli, da se je zatipkal in normalno ponovno vpiše uporabniško ime in geslo ter se normalno prijavi v sistem, brez da bi sploh pomislil na morebitno zlorabo, saj postopek izgleda povsem normalno. Zlonamerneži v ozadju pa so pridobili njegove zasebne podatke potrebne za pristop v določeno aplikacijo.

SI-CERT pa je na svoji spletni strani[62] objavil krajši seznam navodil, ki nas lahko obvarujejo pred tovrstnimi zlorabami. Svetujejo, da:

- nikoli ne odgovarjajte na elektronska pisma, ki od vas zahtevajo osebne in finančne podatke,
- sami nikoli ne pošiljajte osebne podatke preko elektronske pošte,
- ne sledite povezavam do takšnih spletnih strani,

[60] Izvirnik v ang. phishing (lahko tudi webpage spoofing), nanaša se na internetno pogovorno obliko zapisa besede "fishing", ki pomeni ribarjenje. To je značilen zapis v hekerskem okolju, kjer se pogosto uporablja napačno črkovanje, namesto "f" uporablja "ph", namesto "i" se uporablja "1", namesto "s" vedno "z" (i.e. codes – codez), menjava se tudi "0" z "o" (i.e. l00zer) (http://www.outpost9.com /reference/jargon/jargon_10.html#SEC17, 19. maj 2006).

[61] SI-CERT je v letu 2004 odkril 4 tovrstne prevare, v letu 2005 pa kar 12 (http://www.arnes.si/si-cert/, 2. junij 2006). Trend napram drugim grožnjam je tako več kot očiten. Tovrstne zlorabe so v izrednem porastu, kajti omogočajo hitre zaslužke malopridnim uporabnikom.

[62] http://www.arnes.si/si-cert/, 2. junij 2006

- kadar se prijavite v spletne strani, ki imajo karkoli opraviti z denarjem, vedno vtipkajte naslov (URL) direktno v naslovno vrstico, saj se tako izognete preusmeritvam ter
- redno preverjajte izpiske bančnih računov in kreditnih kartic (http://www.arnes.si/si-cert/obvestila/2004-06.html, 2. junij 2006).

V zadnjem poglavju moje naloge pa bom še naknadno naredil seznam najnujnejši preventivnih ukrepov, ki nas lahko obvarujejo pred zlorabami in zlonamernimi programi.

Slika 6: Porast poneverbe internetnih strani v zadnjem letu

Prirejeno po: http://www.ciphertrust.com/files/forms/landing_template.php?sp=spam_overture, 19. maj 2006

Delovanje proti tovrstnim zlorabam je mogoče predvsem s strani uporabnika in njegove previdnosti, kajti nobena zakonodaja in noben predpis ni sposoben zaščititi uporabnika pred njegovo naivnostjo. Tako ima vrsta tovrstnih zlorab že v naslovni vrstici brskalnika, ki ga uporabnik uporablja, očitno napačno zapisan naslov kjer se nahajamo iz katerega je moč razbrati, da gre za prevaro. Seveda pa je to za povprečnega uporabnika že precej zahtevno, vendar ob dejstvu da gre za naš denar in našo zasebnost, dodaten trud ni odveč. Najnovejše različice brskalnikov Explorer in Firefox pa že vsebujeta popravke, ki tovrstne zavajajoče naslove v naslovni vrstici onemogočata. Problem pa nastane, ko zlonamerneži uporabijo bolj prefinjene metode poneverbe internetnih strani, v teh primerih pa uporabnikova previdnost ni dovolj. Za podrobnejši opis le tega pa je moja diplomska naloga premalo obsežna.

4.1.1.3. Lovljenje gesel

Lovljenje gesel[63] je oblika iskanja uporabniških imen in gesel za dostop do določene aplikacije. Poznamo dve bolj razširjeni obliki. Prva je sekvenčno lovljenje in se uporablja pri bolj zahtevnih iskanjih gesel, ko je potrebno združiti moč večih računalnikov. Vsak računalnik tako dobi poseben odsek možnih gesel, ki ga mora pregledati. Skupina večih računalnikov tako pregleda celoten spekter gesel in dobi rešitev. Druga oblika pa je lovljenje gesel s pomočjo slovarja pogosto uporabljenih gesel. Tovrstno lovljenje se uporablja pri manj zahtevnih iskanjih, kot so različna vdiranja v elektronske predale in druge brezplačne oblike, ki so na voljo uporabnikom interneta (http://www.caci.com/ia/threats.html, 19. maj 2006).

Osnovna zaščita pred takšnim delovanjem, ki je precej pogosto[64], pa je izbiranje karseda zapletenih gesel v kombinaciji z različnimi znaki ASCII[65], ne samo številkami in besedami.

4.1.1.4. Elektronsko vohljanje

Elektronsko vohljanje[66] je nadzorovanje pretoka informacij s strani ISP-jev[67] ali drugih administratorjev, ki upravljajo s prenosom podatkov k nam in od nas. Druga oblika vohljanja pa je bolj enostavna in v bistvu vključuje gledanje čez ramo uporabniku[68]. Tovrstna nevarnost preti predvsem kadar uporabnik uporablja javni dostop do interneta in nima nadzora nad dogajanjem za njim. Tako lahko nekdo podrobno spremlja in opazuje tipkovnico in si tako pridobi uporabniško ime in geslo za dostop. Seveda pa je mnogo bolj zahtevna in za uporabnika vprašljiva prva oblika, t.j. nadzorovanje s strani ISP-jev in različnih vladnih služb.

[63] V izvirniku ang. "sequential scanning" in ang. "dictionary scanning".
[64] SI-CERT je v letu 2004 odkril 415, v letu 2005 pa 252 tovrstnih iskanj gesel (http://www.arnes.si/si-cert/, 2. junij 2006).
[65] glej slovarček
[66] ang. "digital snooping"
[67] glej slovarček
[68] ang. "shoulder surfing"

Evropska direktiva o "elektronskem vohljanju"

V zadnjem letu je problematika v EU na tem področju dobila tudi novo direktivo Evropskega parlamenta in Evropskega sveta. Direktiva 2006/24/ES o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij je bila sprejeta 15. marca 2006. Direktiva zagovarja tovrstno hrambo podatkov kot potrebno, primerno in ustrezno znotraj demokratične družbe z vidika posebnih namenov javnega reda, t.j. za zaščito nacionalne varnosti (t.j. državne varnosti), obrambe, javne varnosti ali preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskih komunikacijskih sistemov. Direktiva v svojem šestnajstem odstavku predgovora nalaga nacionalnim zakonodajnim telesom, da sprejmejo zakonodajne ukrepe za zagotovitev hranjenja podatkov v skladu s to direktivo. Hkrati pa nalaga, da so ti podatki dostopni samo pristojnim nacionalnim organom v skladu z nacionalno zakonodajo ob polnem spoštovanju temeljnih pravic oseb, ki se jih te omejitve dotikajo (Direktiva EU 2006/24/ES, 2006).

Direktiva je sestavljena iz sedemnajstih členov, ki opredeljujejo različna področja. Za mojo diplomsko nalogo so pomembni predvsem tretji do sedmi člen te Direktive. Tretji člen opredeljuje obveznost hranjenja podatkov pri ponudnikih javno dostopnih elektronsko komunikacijskih storitev ali javnega komunikacijskega omrežja v njihovi pristojnosti. Tako se Direktiva neposredno dotika posameznika, ki je povezan z internetom preko takega komercialnega ponudnika. Četrti člen določa pravico dostopa do teh podatkov brez nepotrebnega odlašanja (8. člen), ki je omejena izključno na pristojne nacionalne organe, le ti pa morajo pristopiti k podatkom za vsak primer posebej in v skladu z nacionalnim pravom. Vsaka država članica sama določi pogoje in postopke za dostop do teh podatkov. Naslednji, peti člen pa določa kategorije podatkov, ki se hranijo. To so podatki potrebni za sledenje in prepoznavanje vira komunikacije, cilja komunikacije, podatki potrebni za ugotovitev datuma, časa in trajanja komunikacije, podatki potrebni za ugotovitev vrste komunikacije, podatki potrebni za razpoznavo komunikacijske opreme uporabnikov ali njihove dozdevne opreme ter podatki potrebni za ugotovitev lokacije opreme za mobilno komunikacijo. Za mojo nalogo pa so pomembni predvsem podatki pri dostopu do interneta, elektronske pošte in internetne telefonije. Direktiva kot podatke, ki se hranijo, našteva:

- dodeljeno uporabniško ime,
- telefonsko številko dodeljeno za vsako komunikacijo dostopa v javno omrežje,
- ime in naslov naročnika ali registriranega uporabnika, ki mu je bil v času komunikacije dodeljen naslov internetnega protokola (IP),
- datum in čas prijave ter odjave z internetnega dostopa,
- tip internetne storitve,
- klicoča telefonska številka za klicni dostop ali digitalni naročniški vod (DSL) ali druga končna točka začetnika komunikacije (Direktiva EU 2006/24/ES, 2006).

Šesti člen opredeljuje obdobje hrambe, ki znaša najmanj šest mesecev in ne več kot dve leti od datuma komunikacije. Sedmi člen pa je za temo moje diplomske naloge najpomembnejši, saj opredeljuje varovanje in varnost podatkov pridobljenih v skladu s to Direktivo. Spoštovati je potrebno naslednja načela varovanja podatkov:

- shranjeni podatki so enake kakovosti in zanje veljajo enaka določila o varnosti in zaščiti kot za podatke na omrežju;
- sprejmejo se primerni tehnični in organizacijski ukrepi s katerimi se jih zaščiti pred nezakonitim uničenjem, izgubo in spremembami nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkrivanja;
- sprejmejo se primerni tehnični in organizacijski ukrepi s katerimi se zagotovi, da so podatki dostopni samo posebej pooblaščenemu osebju ter
- ob koncu obdobja hranjenja se uničijo vsi podatki, razen tistih, do katerih se je dostopalo in se jih shranilo (Direktiva EU 2006/24/ES, 2006).

Tovrstna navodila seveda puščajo kar precej prostora nacionalnim zakonodajalcem, kar lahko za sabo povleče različne končne oblike nadzora. To pa seveda ni v prid posamezniku. Prav tako tovrstno hranjenje enormnih količin podatkov predstavlja velik strošek, ki ga bodo ISP-ji zagotovo prenesli na uporabnike, kar je še ena negativna stran te direktive. Poleg tega je tudi vzrok, ki je bil podlaga za pisanje tovrstnih direktiv na rahlo majavih nogah, saj je pisan v duhu "vojne proti terorizmu" in tako postavlja varnost pred svobodo[69]. Kar pa je seveda sporno z vidika posameznika,

[69] Direktiva tako sledi ameriškim zgledom, kjer NSA že več let skrbno beleži vso elektronsko pošto in vse komunikacije, ki vsebujejo določene besede ali besedne zveze (http://www.nsawatch.org/resources.html, 28. maj 2006).

saj mu bosta omejena svoboda in zasebnost na račun premočno prikazane grožnje terorizma. Saj terorizem v primerjavi z drugimi grožnjami, ki so bolj prisotne realno ne predstavlja tako velike grožnje. Resda je EU sprejela že pred tem sklep o obsodbi terorističnih napadov na London ter potrebo po čimprejšnjem sprejetju skupnih ukrepov za hrambo telekomunikacijskih podatkov. Lahko pa le upamo, da se tovrsten nadzor ne bo sprevrgel v zlorabo in bo omogočal nadzorovanje posameznikov in izkoriščanje pridobljenih podatkov v druge namene (izsiljevanje, itd.). Direktiva v svojem devetnajstem odstavku predgovora hkrati dopušča tudi pravico do odškodnine, ki jo ima katerakoli oseba, ki je (bo) utrpela škodo kot posledico nezakonitega postopka obdelave ali kateregakoli dejanja, ki je (bo) nezdružljivo z nacionalnimi določbami, sprejetimi v skladu z navedeno direktivo. Ta pravica do odškodnin se nanaša tudi na vsak nezakonit postopek obdelave kakršnih koli osebnih podatkov, kar uporabniku dopušča vsaj občutek zavarovanosti pred zlorabami in pravice do zasebnosti. Direktiva nacionalnim zakonodajalcem pušča tudi proste roke pri oblikovanju nadzornega organa, ki naj bi zagotavljal delovanje vseh naštetih elementov v skladu z Direktivo.

Na tem mestu velja omeniti še druge evropske predpise, ki se prav tako nanašajo na elektronski kriminal.

Konvencija o kibernetski kriminaliteti

Pomembnejša med njimi je Konvencija Sveta Evrope o kibernetski kriminaliteti. Slovenija je k tej konvenciji pristopila 24. 7. 2002 in jo ratificirala 8. 9. 2004. Slovenija je tudi ena izmed redkih držav podpisnic, v kateri ta Konvencija že velja v obliki Zakona o ratifikaciji Konvencije o kibernetskih kriminaliteti, v veljavo je stopila s 1. 1. 2005. Temeljni namen Konvencije pa je vzpostaviti neko predhodno podlago o zaščiti družbe pred kibernetskim kriminalom, z namenom kasnejše vzpostavitve primerne državne zakonodaje (http://conventions.coe.int/Treaty/en /Summaries /Html/185.htm, 30. maj2006). Direktiva EU, ki sem jo omenil zgoraj je tako ena izmed posledic te Konvencije.

Strategija za varno informacijsko družbo

Evropska komisija[70] je izdala tudi Strategijo za varno informacijsko družbo[71] v obliki krajšega dokumenta, ki naj bi ponovno oživila in nadaljevala strategijo Evropske komisije za Mrežno in informacijsko varnost iz leta 2001. V novi strategiji se omenja trenutno stanje groženj informacijski varnosti in ukrepe, ki so potrebni za izboljšanje le te. V strategiji se omenja tudi posameznike in njihov del prispevka k skupni informacijski varnostni verigi, saj brez varnih računalnikov navadnega uporabnika ni varnega medmrežja. Kot temeljni kamen zaščite vseh uporabnikov IKT pa Komisija navaja izboljšanje poznavanja problemov, ki jih prinaša internet. Evropska komisija za rešitev teh problemov predlaga dinamičen in povezan pristop vseh akterjev, ta strategija pa naj temelji na dialogu, partnerstvu in odgovornosti (http://ec.europa.eu /information_society/doc/com2006251.pdf, 2. junij 2006).

Moja diplomska naloga je lahko tako uporabna tudi v tej luči.

4.1.1.5. Zasipanje z neželeno pošto

Zasipanje z neželeno pošto[72] je zagotovo poznano prav vsakemu uporabniku spletne pošte. V splošnem lahko za SPAM označimo vsako sporočilo, ki je hkrati poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki je naslovniki sami ne želijo prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov (http://www.infosys.si/, 22. maj 2006). Ti izdelki so pogosto dvomljive kvalitete. SPAM je tako vsaka elektronska pošta[73], ki ste jo dobili, ne da bi jo želeli ali zahtevali in vključuje enega ali več naslednjih elementov:

- neželena oglasna in reklamna sporočila,
- denarne ponudbe, piramidne sheme, verižna pisma,
- zlonamerne programe, ki se širijo prek elektronske pošte,
- poceni zdravila ali pripomočke za rast osebnih organov[74].

[70] Evropska komisija je politično neodvisna institucija, ki zastopa in podpira interese Evropske unije kot celote.
[71] Dostopno na: http://ec.europa.eu/information_society/doc/com2006251.pdf, 2. junij 2006.
[72] Original se glasi v ang. "spamming", SPAM, lahko tudi "Junk E-Mail", odpadna elektronska pošta.
[73] SI-CERT je v letu 2004 odkril 6, v letu 2005 pa 15 novih oblik tovrstnih neželenih elektronskih sporočil (http://www.arnes.si/si-cert/, 2. junij 2006).
[74] V zadnjem času je tovrsten SPAM v ospredju, saj moškim uporabnikom lažno obljubljajo povečanje spolnega uda ob neki čudežni formuli, ki je pomagala že mnogim. Poleg tega pa pomemben delež SPAM-a pripada tudi zdravilom, ki so na voljo preko plačila v internetnih trgovina.

Glavni namen SPAM-a je neželeno oglaševanje stvari in izdelkov, ki nas zvabijo v nakup teh "dobrin", seveda je večina teh poslov prevara ali goljufija, ki na račun človeškega pohlepa služi in se okorišča. SPAM, ki vključuje še zlonamerne kode pa lahko še upočasni delovanje vašega računalnika, vaše povezave v splet ter vam vzame dragocen čas, ki bi ga lahko namenili za druge, bolj pomembne stvari. Poleg tega pa večina uporabnikov teh sporočil ne bere, saj je njihov izvor razpoznaven že od daleč. Ob vsem tem se vprašamo, kaj je sploh namen SPAM-a in zakaj ga nekateri sploh razpošiljajo? Odgovor je preprost in jasen, zaradi nizkih stroškov oglaševanja in izrednih razsežnosti populacije, ki nam je na voljo. Stroški pa nastanejo na drugi strani, pri ISP-jih, kajti le ti morajo zagotoviti zaščito pred tovrstno neželeno pošto (lahko tudi brezplačno za končnega uporabnika) ter dodaten prostor, ki je potreben, da nam neželena pošta ne prepreči dostopa do druge želene pošte, ki jo pošiljatelju zavrne, če imamo predal poln. Zasipanje z neželeno pošto je zelo razširjeno in izredno nezaželeno med uporabniki[75]. Poznamo pa še mnogo drugih vrst SPAM-a, kar pa je za obseg moje naloge preobširna tema.

Vprašanje je, če se tovrstno oglaševanje sploh splača[76], glede na dejstvo da je SPAM osovražen. Nekateri manj resni oglaševalci se na to sploh ne ozirajo, kajti vedno se najde kakšen odstotek uporabnikov, ki verjamejo tovrstnim ponudbam in svoj denar zapravljajo tudi za nesmiselne stvari. Medijsko bolj prepoznavne družbe in podjetja se tovrstnega oglaševanja ne poslužujejo, temveč svoje oglaševanje nudijo le ob izrecnem soglasju uporabnika, ter tako pokažejo spoštovanje do uporabnikove/strankine zasebnosti in s tem svoj korekten odnos do kupcev. Na njihova oglasna sporočila se je enostavno naročiti in tudi odjaviti, ta oblika oglaševanja pa se mi zdi sprejemljiva.

---

[75] Problematiko pa povečuje tudi spretnost pošiljalcev SPAM-a, kajti le ti dobro poznajo priljubljene odjemalce pošte kot so Microsoft Outlook, Eudora in Opera. V le teh se lahko z nekaj ukazi nastavi, da odjemalec elektronske pošte avtomatično prepozna SPAM po določenih besedah, avtorju ali temi sporočila. Taki primeri besed so "sensational", "medical offer", "extraordinary", "enlargement" in podobne besede ali besedne zveze, ki oglašujejo nekaj izrednega in neponovljivega. Odjemalec pošte zazna tovrstne besede in tovrstno elektronsko pošto posebej označi ali premakne v ta namen določeno mapo. Vendar pa pošiljatelji poznajo tovrstno zaščito in svoje oglase prilagodijo tako, da jih odjemalci ne zaznajo kot SPAM, to pa naredijo s pomočjo enostavnih ukan. Lahko vedno odprejo nov elektronski predal in z njega razpošiljajo naprej, lahko pa z ASCII znaki spremenijo besede tako da so še vedno berljive, vendar jih odjemalci ne zaznajo. Taki primeri bi bili "E*nlarg*ment", "e-Xtra-Ordinary", "M-E-D-I-C-A-L", "besT$eLLers" etc. In ves trud za zaščito pred SPAM-om postane neploden.

[76] V maju se je končal kazenski pregon kralja SPAM-a z obsodbo! Sodišče je pošiljatelju neželenih sporočil naložilo kazen povračilo stroškov – štiri milijone ameriških dolarjev (James, 2006: http://www.vnunet.com/vnunet/news/2155507/spam-king-loses-court-battl, 2. junij 2006) To je zanimiv presedan, ki bi lahko v prihodnosti zmanjšal tovrstne zlorabe.

4.1.1.6. Nepooblaščene spremembe in vdori

Med namerne grožnje sem uvrstil tudi nepooblaščene spremembe[77], saj lahko uporabniku prav tako naredijo veliko škode. Prav tako pa velja omeniti tudi vdore[78], ki so prav tako lahko razlog za veliko škodo povzročeno uporabniku.

Nepooblaščene spremembe se največkrat nanašajo na spremembo programske opreme z namenom odstranitve zaščite pred kopiranjem. Tovrstno početje ni več le nelegalno, temveč po večini razvitih državah[79] tudi kaznivo. Bistvo tovrstnih sprememb je odstraniti zaščito s reprogramiranjem programa na tistem mestu, kjer se pojavlja zaščita. Digitalno zaščito[80] se lahko obide ali pa popolnoma ukine, tako da program sam izgubi svoj "obrambni" mehanizem. To se naredi s posebnimi programi za iskanje napak v programih, ki omogočajo naknadno spremembo znotraj programov, lahko pa tudi le z datoteko[81], ki odstrani določene ukrepe za preverjanje pristnosti, kar je še posebej enostavno za končnega uporabnika. Na internetu je množica strani, ki omogočajo nalaganje tovrstnih datotek, vendar je izredno velika verjetnost, da bo ob taki datoteki pripeta še kakšna druga zlonamerna koda.

Vdori v računalniške sisteme so posledica delovanja hekerjev[82]. Heker je posameznik, ki je izredno podkovan z znanjem na računalniškem področju in iz ima sposobnost izkoriščanja pomanjkljivosti programov. Hekerji uporabljajo svoje znanje za vdore v informacijska omrežja in računalnike iz različnih vzgibov. Prvi izmed razlogov za vdiranje v sisteme pa je intelektualni izziv. Poznamo pa več vrst hekerjev. Sekači (white hat hacker) spoštujejo etnična pravila in ne povzročajo škode, njihov namen pri delovanju je odkrivanje napak in varnostnih pomanjkljivosti ter popravljane le teh.

---

[77] ang. cracking
[78] ang. hacking
[79] V ZDA je tovrstne spremembe označil za kaznive t.i. DMCA (Digital Millennium Copyright Act), zakon o digitalnih avtorskih pravicah, v EU pa so leto kasneje (2001) sprejeli EU Copyright Directive, Direktivo EU o avtorskih pravicah (http://en.wikipedia.org/wiki/Software_cracking, 28. maj 2006).
[80] SI-CERT je v letu 2004 odkril 2, v letu 2005 pa 7 nepooblaščenih sprememb programske opreme (http://www.arnes.si/si-cert/, 2. junij 2006).
[81] Tovrstne datoteke ("cracki") so izredno razširjeni po P2P omrežjih in lahko dostopni kljub svoji nelegalni naravi. Večina avtorjev, piscev tovrstnih crackov, pa hkrati z razširjanjem teh datotek ponudi tudi obvestilo, v katerem se nekako operejo krivde in omenjajo tovrstno početje kot intelektualni izziv in omenijo, da so sami kupili legalen izdelek in ga malce priredili. Na koncu dodajo še stavek v smislu: "Podpirajte programska podjetja!" ali "Če boste igro igrali, jo kupite!", kar pa v veliki večini primerov naleti na neposlušnost. Vsi pa se seveda predstavljajo pod različnimi vzdevki, med bolj poznanimi pa so skupine RELOADED, DEViANCE, FairLIGHT in Razor1911.
[82] ang. hacker – direkten prevod bi se glasil, da je heker oseba, ki s sekiro oblikuje pohištvo; v slovenščini pa imamo zaradi navezave na originalen izvor besede tudi različen prevod za dobronamerne hekerje – sekači in zlonamerne hekerje – lomači (http://sl.wikipedia.org/wiki/Heker, 28. maj 2006).

Lomači (black hat hacker) pa so hekerji, ki svoje znanje uporabljajo za krajo podatkov, vdiranje v sisteme in povzročanje škode. To so zlonamerni posamezniki, ki besedi heker dajejo slab prizvok in tako zavračanje večine slabše podučenih uporabnikov. Tretja oblika hekerjev pa so t.i. "grey hats", to so hekerji, ki ne spadajo v nobeno od zgornjih kategorij in se vedejo glede na trenutno situacijo in odziv napadenega (Parker, www.windowsecurity.com/articles/Different-Shades-Hackers.html, 28. maj 2006).

Z vdorom v računalnik[83] se lahko nad njim pridobi popolna oblast ali pa le spremlja delovanje. V obeh primerih je to za uporabnika škodljivo saj ne ve, da je podvržen nadzoru in s tem lahko tudi manipulaciji. V primeru popolnega prevzema nadzora pa lahko uporabnik kaj kmalu ostane brez svojih datotek, programske opreme ali celo strojne opreme, ki jo je mogoče z določenimi operacijami tudi fizično poškodovati.

4.1.2. Nenamerne grožnje

Nenamerne grožnje so lahko prav tako nevarne kot namerne grožnje, vendar je njihova pogostost veliko nižja od namernih. Pod nenamerne grožnje sem uvrstil motnje v delovanje in človeške napake.

MOTNJE V DELOVANJU

V ta sklop napak sodijo napake strojne opreme in napake programske opreme. Bolj pogoste so napake programske opreme, ki zaradi svoje neizdelanosti ali morebitnih varnostnih pomanjkljivosti lahko povzročijo škodo uporabniku ali druge oblike neprijetnosti, kot je nenadna izguba podatkov zaradi napake v programu. Napake strojne opreme pa so težje odpravljive, saj strojna napaka zahteva tehničen poseg ali zamenjavo dobavljenega kosa opreme. Grožnjo pa predstavlja izguba podatkov (okvara trdih diskov) zaradi nenadnih prekinitev dela.

[83] V Sloveniji je GPU v letu 2005 odkrila tovrstne kršitve. Kategorizirala jih je kot neupravičen vstop v informacijski sistem z uporabo računalniških programov in drugih sredstev in omrežja (omenjena sta dva primera, po drugih kategorizacijah bi lahko našli še kakšnega). Drugih podatkov o tovrstnih kršitvah v statistiki Slovenske policije ni (http://www.policija.si /si/, 2.junij 2006). SI-CERT pa ima drugačne podatke, v letu 2004 naj bi bilo 27 vdorov v sistem, v letu 2005 pa 34 (http://www.arnes.si/si-cert/, 2. junij 2006).

ČLOVEŠKE NAPAKE

Sem sodijo napake programerjev ali uporabniške napake. Programerske napake lahko označimo kot namerne ali nenamerne. Bolj nevarne so namerne "napake", saj programerji lahko izkoriščajo pomanjkljivost v slabe namene in lastno okoriščaje na račun uporabnika. Lahko si omogočijo dostop do podatkov na uporabnikovem računalniku tudi po nakupu programske opreme s pomočjo t.i. zadnjih vrat[84]. Zadnja vrata pa lahko pusti odprta tudi uporabnik sam – uporabniška napaka, z namenom uporabe določenih aplikacij, ki za svoje delovanje potrebujejo odprte določene kanale za povezovanje z internetom. Tovrstne varnostne luknje pa lahko omogočijo vstop različnim zlonamernim programom, ki so sposobni narediti veliko škode uporabniku.

4.1.3. Fizične grožnje

Zadnja oblika groženj je fizične narave. Na seznam groženj sem jih uvrstil predvsem z vidika prekinitve dostopa do interneta in s tem uporabnikove nezmožnosti delovanja in nedostopa do podatkov. Najpomembnejša je prekinitev električne energije, ki je vitalnega pomena za uporabo IKT, brez nje se dobesedno vrnemo v prejšnje stoletje, saj nam je onemogočeno uporabljati kakršnekoli električne naprave. Druga nevarnost sta poplava in požar, ki lahko poškodujeta ali celo uničita našo strojno opremo in s tem vse podatke, ki so na njej ter nam onemogočita dostop do interneta.

Naj je razlog za prekinitev delovanja še tako trivialen in v naravi povsem običajen pojav, je njegov učinek na naše delovanje lahko izjemen. Tako nas lahko udar strele v računalnik popolnoma odreže od virtualnega sveta in je lahko kratkoročno nevarnejši od vseh zlonamernih programov ali drugih oblik namernih groženj.

4.2. Zaščita in protiukrepi

Večino zaščitnih ukrepov in protiukrepov proti različnim nevarnostim, ki pretijo uporabniku interneta, sem navajal že sproti ob grožnjah. Vendar je potreben nek

[84] Ang. "back door", "trap door" – je izraz za odprte povezave, ki se izognejo nadzoru požarnega zidu, največkrat z uporabnikovo privolitvijo v upanju, da je odprtost določenih vrat potrebna za normalno delovanje programa.

povzetek vsega zapisanega za lažji pregled in uporabo zapisanih informacij. Poleg tega bom navedel še druge zaščitne ukrepe, ki so potrebni za zagotavljanje minimalne varnosti pri uporabi interneta. Velja pa si zapomniti eno pravilo, popolne varnosti na internetu ni! Omeniti velja, da zaščita pred mnogimi nevarnostmi ni enostavna, vendar z zahtevnostjo protiukrepov raste tudi stopnja varnosti, ki si jo zagotovimo. Tako morebitnemu napadalcu ostane na izbiro napasti zaščiten računalnik in ob tem izgubiti ure in ure časa ali se polastiti drugega uporabnika, ki le te zaščite sploh nima. Tako je izbira jasna s strani napadalca, naša naloga pa je da morebitnemu napadalcu karseda otežimo delo in ga s tem odvrnemo od njegovih namenov. Še enkrat pa moram poudariti, da neprebojni sistemi in popolna zaščita ne obstajata!

Pri pisanju zaščite in protiukrepov sem se naslonil na različne organizacije[85], ki ponujajo internetno zaščito in se bojujejo proti internetnemu kriminalu. Na podlagi večih različnih predlogov pa sem sestavil seznam potrebnih protiukrepov in dejanj, ki naj bi nam zagotovili karseda močno varnost. Seznam ukrepov po pomembnosti in krajša razlaga sledita v nadaljevanju.

1. NAMESTITEV IN UPORABA PROTIVIRUSNIH PROGRAMOV

   Prvi in najpomembnejši ukrep pri zaščiti vašega računalnika. Protivirusni[86] program mora vsebovati redno (večkrat dnevno) posodabljanje podatkovne baze in omogoča sproten pregled prihajajoče in odhajajoče elektronske pošte. Omogočati mora celotno pregledovanje računalnika in načrtovanje pregledov sistema. Poleg protivirusnega programa pa je priporočljiv tudi protivohunski[87] program, ki odkriva druge možne oblike ogrožanja vaše varnosti.

[85] Upošteval sem naslednje organizacije: CERT, uradna spletna stran: http://www.cert.org/, 29. maj 2006; SI-CERT, uradna spletna stran: http://www.arnes.si/si-cert/, 2. junij 2006; Computer Security Institute– uradna spletna stran: http://www.gocsi.com/, 29. maj 2006; Computer Security Training, Certification and Research – Sans, uradna spletna stran: http://www.sans.org/, 29. maj 2006; Computer, Internet and Information Security, ITSecurity.com, uradna spletna stran: http://www.itsecurity.com/, 29. maj 2006; A Division of Cybertrust ICSA Labs, uradna spletna stran: http://www.icsalabs.com/icsa/icsahome.php, 29. maj 2006.

[86] ang. "antivirus"

[87] ang. "antispyware"

2. NEPRESTANO NALAGANJE POPRAVKOV

Redno nalaganje popravkov in varnostnih dodatkov za vaš operacijski sistem lahko stori mnogo in prepreči veliko morebitnih nevšečnosti. Takoj ko se odkrije neka varnostna pomanjkljivost, je potrebno naložiti potreben popravek.

3. PREVIDNOST PRI BRANJU ELEKTRONSKE POŠTE S PRIPONKAMI

Vsako elektronsko sporočilo, ki vsebuje priponko je potencialno nevarno za vaš računalnik. Zato je pomembno da poznamo pošiljatelja sporočila, kaj nam pošilja, ter da protivirusni program pregleduje našo pošto še preden jo naložimo na računalnik. Ta nasvet se nanaša tudi na uporabo pogovornih programov in nalaganje vsebin z njihovo pomočjo.

4. NAMESTITEV IN UPORABA POŽARNEGA ZIDU

Požarni zid predstavlja vratarja za dostop do vašega računalnika. Nadzoruje ves promet med vami in drugimi računalniki, preko lokalnega omrežja ali interneta. Njegova naloga je da nadzoruje vse možne izhode in vhode v vaš računalnik in vas obvešča o morebitnem prenosu podatkov. Z njegovo pomočjo lahko računalnik dodatno zaščitimo pred neželenimi dogodki.

5. IZDELAVA VARNOSTNIH KOPIJ POMEMBNIH DATOTEK

Vedno modra odločitev. Kljub vsem naporom se lahko zgodi, da naša zaščita ne bo zadostovala in bomo izgubili podatke. Zato je izrednega pomena, da naše podatke shranimo na mesto, ki ni podvrženo vplivom z interneta, kar pomeni na nek varnostni medij.

6. UPORABA ZAHTEVNIH GESEL

Pogosto spregledan korak v varnosti računalnika. Izbira ne preveč enostavnega gesla in njihova raznovrstnost je lahko pomemben dodatek k vaši varnosti. Geslo naj izkoristi vse možnosti, ki jih aplikacija ponuja, od njegove dolžine do različnih kombinacij ASCII znakov. Gesla naj se ne ponavljajo! Pomembna aktivnost pa je tudi spreminjanje gesla po določenem obdobju in izbira gesel, ki nam jih ni treba zapisati.

7. PREVIDNOST PRI NALAGANJU VSEBIN Z INTERNETA

Ta korak je verjetno najbolj podvržen uporabnikovi "zdravi pameti", saj nas nobena programska oprema in nikakršni nasveti ne morejo zadržati pred tem da sami storimo napako in dovolimo dostop ali nalaganje škodljivih vsebin. Pomagamo si lahko s tremi kratkimi pravili. Program, ki ga nameščamo, moramo poznati in vedeti njegovo funkcijo na računalniku. Vedeti moramo kam smo ga namestili, kaj program spremeni in kako se ga odstrani z računalnika. Na koncu pa je pomembna tudi izkušnja drugih uporabnikov, kako deluje pri njih in ali so z njim zadovoljni.

8. UPORABA STROJNEGA POŽARNEGA ZIDU

Strojni požarni zid omogoča zaščito celega domačega omrežja, česar programski požarni zid ne omogoča. Strojni požarni zid tako ločuje domače omrežje od interneta in deli omrežje na varni del in nevarni del. Kombinirana uporaba obeh požarnih zidov je najboljša rešitev[88].

9. UPORABA PROGRAMOV ZA KODIRANJE

Tovrstna zaščita naših podatkov je posebej pomembna pri prenosu zaupnih informacij preko medmrežja. Na voljo je mnogo dobrih kodirnih[89] programov - tudi brezplačno. Tako si pomembne podatke lahko zaščitimo s posebnimi ključi, ki so znani le nam, morebitnemu nepooblaščenemu iskalcu teh podatkov pa izredno otežimo razkritje le teh.

10. VAROVANJE VAŠIH ZAUPNIH PODATKOV

Nikoli ne izdajajte zaupnih podatkov kot so gesla, uporabniška imena, številke kreditnih kartic in drugih zasebnih podatkov preko interneta!

[88] Na tem mestu velja omeniti še varnost brezžičnih domačih internetnih omrežij, ki ob vse večji razširjenosti le teh pridobiva na pomenu. Poleg kodiranja signala internetne točke je potrebno ob namestitvi razdelilnika, vsakemu odvzemniku nameniti še svojo IP številko, ga povezati z razdelilnikom internetne povezave in nato skriti signal razdelilnika pred drugimi nepovabljenimi gosti.

[89] Tak primer je Pretty Good Privacy, njihovo spletno stran pa najdete na naslovu: http://www.pgp.com/, 2. junij 2006.

5. ZAKLJUČEK

5.1. Preverjanje hipotez

V svoji prvi hipotezi sem zapisal, da *osebna varnost posameznika na internetu pridobiva na pomenu, vendar ji še vedno posvečamo premalo pozornosti glede na realno ogroženost*. Ugotavljanje pravilnosti te hipoteze bom moral razdeliti na dva dela. Prvi del glede pridobivanja pomena posameznikove varnosti lahko vsekakor potrdim, saj se v mednarodnih krogih posameznik kot pomemben varnostni referenčni objekt vse pogosteje pojavlja. Varnost posameznika tako pridobiva na pomenu, verjetno tudi na račun pomena nacionalne varnosti, ki zaenkrat še nosi ključno vlogo. Izpostavil bi le en vidik koncepta človekove varnosti, t.i. nov varnostni koncept (ang. new security concept), ki neposredno vključuje tudi varnost na internetu, t.i. kibernetsko varnost. Pridobivanje varnosti posameznika na internetu se lahko potrdi tudi s sprejetjem precej strogih zakonodaj na tem področju. Tako Konvencije Sveta Evrope kot Direktive Evropske unije poudarjajo posameznikovo varnost in kriminalizirajo dejanja, ki so usmerjena proti njej. Vendar na tem mestu lahko izrazim potrditev s pomislekom, saj se je na račun državne varnosti zmanjšala raven zasebnosti, ki jo ima posameznik pri svoji uporabi interneta. Drugi del prve hipoteze pa moram zavrniti. Zapisal sem, da se internetni varnosti premalo posvečamo, vendar to vsekakor ne drži. Ob poplavi vseh oglasov, internetnih strani, spletnih klepetalnic, brezplačnih zaščitnih programov in celo člankov v tiskanih medijih o varnosti računalnika, ne moremo govoriti o pomanjkanju pozornosti za varnost posameznika na internetu. Za zainteresiranega posameznika je informacij vsekakor dovolj, morda celo preveč za izbiro pravih, pomembno je le da se uporabnik sam odloči in zaščiti svoj računalnik in s tem sebe. Pozornost uporabnikov in javnosti je vsekakor usmerjena tudi k varnosti na internetu in zaščiti računalnikov pred grožnjami. Varnosti posameznika in spoštovanju etičnih pravil tudi v kibernetskem okolju pa se posveča tudi država, ne samo s kurativo v obliki kazni, temveč tudi s preventivo[90] pri najbolj občutljivi skupini – mladoletnikih in otrocih.

[90] Moj komentar se nanaša na brošuro o nevarnostih in pasteh piratstva, ki jo je izdalo nekdanje Ministrstvo za informacijsko družbo, z naslovom Peter proti piratom. Brošura je dostopna na naslovu: http://mid.gov.si/mid/mid.nsf/f1?OpenFrameSet&Frame=main&Src=/mid/mid.nsf/0/634D1B941FFDB8EFC1256F09004071EE?OpenDocument, 30. maj 2006)

Moja druga hipoteza je predpostavljala, da se *z razvojem tehnologij in različnih storitev preko interneta lahko varnost posameznika navidezno (in tudi v resnici) poveča, vendar je vse to lahko zavajajoče, saj je vsak posameznik, ne glede na znanje in interes, odgovoren za lastno zaščito.* To hipotezo lahko sprejmem v celoti, vendar je potreben ob sprejetju le te kratek razmislek. Razvoj zmogljivosti računalnika, odkritje novih tehnologij, novih oblik kodiranja, varnostnih programov in požarnih zidov je zagotovo prineslo povsem novo dimenzijo varnosti, ki jo lahko tehnologija ponudi posamezniku. Vendar sta na mestu dva pomisleka. Prvi je, da je povsem enaka tehnologija, včasih lahko tudi boljša, na voljo zlonamernim uporabnikom interneta. Posameznikom, ki prav to tehnologijo lahko izkoristijo v našo škodo in proti nam. Drugi pomislek pa se nanaša na drugi del te hipoteze, da nam nobena sodobna tehnologija ne more pomagati, če je ne uporabljamo, oziroma je ne izkoristimo v celoti. Najhujša oblika bi bila, da bi celo napačno uporabljali določen program (npr. požarni zid) in sami napravili še dodatne varnostne pomanjkljivosti. Tako je lahko na voljo kopica varnostnih popravkov in najmodernejši protivirusni programi, vendar če uporabnik sam ne zagotovi namestitve le teh, je ves trud strokovnjakov zaman. Zato je lahko zagotovitev varnosti z moderno tehnologijo tudi zavajajoča, ker je v prvi vrsti odvisna tudi od interesa in znanja uporabnika in posledično je moja druga hipoteza pravilna.

Varnost na internetu je varljive narave. Ni popolnega zagotovila, da je naš računalnik zaščiten in da smo pri brskanju po spletu ali opravljanju določenih opravil varni. Obstaja pa kopica kazalcev, ki nam povedo, kako varni smo in v katerih primerih smo zaščiteni pred neželenimi dogodki. Problem nastane pri na novo odkritih varnostnih pomanjkljivostih in luknjah v naši zaščiti, ker smo tistih nekaj ur prepuščeni na milost in nemilost zlonamernih neznancev. Najbolj ogroženi so posamezniki, ki se ne zavedajo nevarnosti, ki jim grozijo preko interneta. Tako je za nepoučenost in neznanje tudi v tem primeru kazen lahko precej huda. Taki uporabniki so podvrženi veliki verjetnosti, da bo njihov računalnik postal tarča zlonamernih programov, nezaželene pošte, elektronskega vohljanja, itd. Sami pa bodo prve tarče sleparij in prevar, ki jih spretni avtorji izdelujejo prav za take uporabnike – nepoučene. Sami pa v svoji nevednosti verjetno ne bodo spoznali, da so bili prevarani, dokler ne bodo soočenimi z neprijetnimi posledicami. Tako lahko v celoti sprejmem tudi mojo tretjo hipotezo, ki opredeljuje *internetne nevarnosti kot zapletene oblike ogrožanja posameznika, ki se jih največkrat ne zavedamo, dokler ni že prepozno.* Ta ugotovitev lepo povzema trenutno

najbolj popularno grožnjo – t.i. phishing. S to vrsto prevare uporabniku povzročimo škodo, ne da bi se uporabnik zavedal, da je bilo karkoli narobe ali da je žrtev prevare.

5.2. Sklep

V diplomski nalogi sem želel predstaviti najpogostejše nevarnosti, ki grozijo uporabnikom interneta. Probleme, s katerimi se uporabniki interneta srečujemo vsak dan, sem želel prikazati v neki novi luči. Želel sem vključiti te varnostne probleme in skrb za zasebnost internetnih uporabnikov tudi v neke širše koncepte varnostne in tudi mednarodne politike.

Zato sem v prvem delu diplome iskal povezave s teoretično podlago in varnostno mislijo na najvišjem nivoju. Pri sodobni varnostni misli in njenih treh referenčnih objektih pa sem lahko prvič našel povezavo z varnostjo posameznika – tudi v njegovi zasebnosti, internetu. S konceptom človekove varnosti (nov varnostni koncept) pa sem dobil potrditev, da varnost posameznika (in s tem tudi njegova varnost na internetu) danes ima nek prostor v mednarodni politiki in varnostni misli. Nadaljeval sem z opredeljevanjem konceptov informacijske varnosti in informacijskega vojskovanja. Pri nekaterih avtorjih je bil tudi v okviru informacijskega vojskovanja izpostavljen posameznik – omenim naj le Schwartau-a in njegov razred osebnega informacijskega vojskovanja.

Osrednji del naloge je bil namenjen predstavitvi najpogostejših groženj na internetu. Grožnje sem razdelil na namerne, nenamerne in fizične. Najpogostejše in najnevarnejše so namerne grožnje, med njimi pa si zaslužijo največjo pozornost zahrbtni programi, ki sem jih v nalogi tudi podrobneje opisal in razdelil. Ostalim sem pozornost namenil glede na stopnjo grožnje, ki jo predstavljajo. Dotaknil sem se tudi evropske zakonodaje, ki opredeljuje delovanje posameznika in omejitve, ki jim je podvržen na internetu. Tako sta Direktiva Evropske unije o hrambi podatkov in Konvencija Sveta Evrope o kibernetski kriminaliteti prva mednarodna dokumenta, ki opredeljujeta to področje. Slovenija kot članica EU in kot podpisnica konvencije spada v sam vrh držav sveta glede ureditve tega področja. Glede na starost države, je to področje zgledno urejeno.

V zadnjem delu naloge pa sem se posvetil še zaščiti in protiukrepom, ki so posameznemu uporabniku interneta na voljo za povečanje svoje varnosti. Vse nasvete in priporočila sem strnil v deset pravil, ki uporabniku olajšujejo vzpostavitev minimalnega standarda varnosti in varovanja zasebnosti. Tako lahko sklenem, da je cilj mojega dela dosežen.

6. VIRI IN LITERATURA

6.1. Monografije

1. *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*. (2006) Brussels: European Commission (Dostopno na: http://ec.europa.eu/information_society/doc/com2006251.pdf, 2. junij 2006).
2. Barkham, Jason (2001): *Information Warfare and International Law on the use of Force*. New York: Harward Law School.
3. Coker, Christopher (2001): *Globalisation and insecurity in the twenty-first century: NATO and the management of risk*. New York: Oxford University Press, The international institute for strategic studies (Dostopno na: http://www.amazon.com /gp/reader/0198516711/ref=sib_dp_pt/102-9178780-1488968#reader-page; 30. marec 2006).
4. Denning, Dorothy Elizabeth Robling (1998): *Information warfare and security*. Massachusetts: ADDISON-WESLEY .
5. De la Cuadra, Fernando (2006): *Kako ukrasti denar z virusom?*. Dnevnik, 4. maj: 27.
6. Dovč, Danica (2005): *Uporaba oblik informacijskega bojevanja v sodobnem terorizmu: primer teroristične organizacije PKK*. Diplomsko delo, Ljubljana: Fakulteta za družbene vede.
7. Forno, Richard, Baklarz Ronald u.r. (1999): *The Art of Information Warfare-Insight into the Knowledge Warrior Philosophy*. Dunkirk: Universal Publishers (Dostopno na: http://www.taoiw.org, 5. marec 2006).
8. Grizold, Anton (1999): *Obrambni sistem Republike Slovenije*. Ljubljana: Visoka policijsko-varnostna šola.
9. Haeni, Reto (1997): *Information Warfare – An Introduction*, The George Washington University, Washington: Cyberspace Policy Institute.
10. Kirchner, Emil J. (2003): *European security trends*. Miami: University of Miami (Dostopno na http://www.miami.edu/eucenter/kirchner_1.pdf , 29.marec 2006).

11. Libicki, Martin (1995): *What is Information Warfare?*. Washington D.C.: Institute for national Strategic Studies (Dostopno na: http://www.iwar.org.uk/iwar/resources / ndu/infowar/a003cont.html, 7.april 2006).
12. Molander, Roger C. (1996): *Strategic Information Warfare: A New Face of War*. National Defense Research Institute, Santa Monica: RAND.
13. Rendulić, Zlatko (1981); *Naučno-tehnički progres i naoružanje,* Beograd: Vojnoizdavački zavod.
14. Schwartau, Winn (1994): *Information warfare, Cyberterrorism: Your personal security in the electronic age*. New York: Thunder's mouth press.
15. Schwartau, Winn (1996): *Information warfar: Chaos on the electronic superhighway*. New York: Thunder's mouth press.
16. Sinchak, Steve (2004): *Hacking Windows XP*. Wiley Publishing, Indianapolis.
17. Sutton, Michael (2002): *Hacking the Invisible Network.* iDEFENSE Labs, Chantilly.
18. Svete, Uroš (1999): *Informacijsko bojevanje – opredelitev in koncept.* Diplomsko delo, Ljubljana: Fakulteta za družbene vede.
19. Svete, Uroš (2002): *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju.* Magistrsko delo, Ljubljana: Fakulteta za družbene vede.
20. Svete, Uroš (2005): *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede, 2005.
21. Svete, Uroš (2005): *Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije.* Doktorska disertacija, Ljubljana: Fakulteta za družbene vede.
22. *The National Strategy to Secure Cyberspace* (2003). Washington: White House (Dostopno na http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, 4. april 2006).
23. *US Army Field Manual 100-6, Information operations* (1996). Washington DC: Headquarters - Department of the army (Dostopno na: http://www.fas.org/ irp/doddir/army/fm100-6/index.html, 4. april 2006).
24. Waltz, Edvard (1998): *Information Warfare Principles and Operations*. London – Boston: Artech House.

6.2. Članki v znanstvenih in strokovnih publikacijah

25. Arsić, Stanislav (2004): Nevidni sovražnik: Informacijsko bojevanje. *Revija Obramba*, 12/2004, 23-25.
26. Svete, Uroš (2004): Novi izzivi za obramboslovje – Obrambne in varnostne razsežnosti uporabe informacijske tehnologije. *V: Društvo mladih raziskovalcev Slovenije – združenje podiplomskih študentov: Znanstveno delo podiplomskih študentov v Sloveniji*, Ljubljana (Dostopno na http://www.drustvo-dmrs.si/e_zbornik_drugi/Prispevki/62_Svete_Uros.pdf , 29. marec 2006).
27. UNDP - United Nations Development programme (1994): *Human development report*, New York (Dostopno na: http://hdr.undp.org/reports/global /1994/en/pdf/ hdr_1994_ch2.pdf , 3. april 2006).
28. Uradni list Evropske unije, Direktiva 2006/24/ES Evropskega parlamenta in Sveta, Strasbourg (Dostopno na: http://www.ispai.ie/DR%20as%20published%20OJ% 2013-04-06.pdf, 15. maj 2006).

6.3. Poglavja iz zbornikov

29. Bilgin, Pinar (2003) Individual and societal dimensions of security. *International studies review 5(2)*: 203-222 (Dostopno na: http://www.bilkent.edu.tr/~pbilgin /Bilgin-isr2003.pdf; 29. marec 2006).
30. Newman, Edward (2001): Human security and constructivism. *International studies perspectives 2 (3)*: 239-251 (Dostopno na: http://people.cas.sc.edu/coate/ Readings/Newman.pdf; 29. marec 2006).

6.4. Enciklopedije in leksikoni

31. Hayden, Michael (ed.) (2003): *National information assurance glossary*, Committee on national Security Systems, NSA, 2003 (Dostopno na: http://www.cnss.gov/ Assets/pdf/cnssi_4009.pdf, 5. april 2006).
32. McDaniel, George (ed.) (1994): *IBM Dictionary of computing*, New York.

33. Whitaker, Randall (ed.) (1998): *Information Warfare Glossary*, US Department of Defense, Pentagon (Dostopno na: http://www.enolagaia.com/IWGlossary.html, 6. marec 2006).

6.5. Baze podatkov in raziskave

34. Europe's Information Society Newsroom, http://europa.eu.int/information_society /newsroom/cf/menu.cfm (2. junij 2006).
35. Raba interneta v Sloveniji, http://www.ris.org/ (30. maj 2006).
36. *Report of the Defense Science Board Task Force on Information Warfare* – Defense, http://www.iwar.org.uk/iwar/resources/us/dsb/iwdmain.htm (7. april 2006).
37. Thrasher, Roger Dean (ed.) (1996): *Information Warfare Delphi*, US NAVY Naval Postgraduate School, Monterey California (Dostopno na: http://www.iwar.org.uk/iwar/resources/usnavy/delphi.pdf, 6. april 2006).
38. Wikipedia, http://en.wikipedia.org/ (6. april 2006).

6.6. Internetne strani

39. A Division of Cybertrust - ICSA Labs, http://www.icsalabs.com/icsa/icsahome. php (29. maj 2006).
40. Anti-Phishing Working Group, http://www.antiphishing.org/ (5. junij 2006)
41. Agencija za pošto in elektronske komunikacije - APEK, http://www.apek.si/ (30. maj 2006).
42. Akademska in raziskovalna mreža Slovenija – ARNES, http://www.arnes.si/ (30. maj 2006).
43. Anti-Spyware Coalition, http://www.antispywarecoalition.org/ (15. maj 2006).
44. Avast! Antivirus Software, http://www.avast.com/ (21. maj 2006).
45. BitTorrent, http://en.wikipedia.org/wiki/Bittorrent (15. maj 2006).
46. Black Hat Homepage, http://www.blackhat.com/main.html (28. maj 2006).
47. Brain, Marshal (2006): *How Computer viruses work?* http://www.howstuff works.com/virus.htm (9. maj 2006).

48. Bullguard, http://www.bullguard.com/ (21. maj 2006).
49. Carnegie Corporation of New York, http://www.carnegie.org/sub/pubs/deadly/cpdvprg.html (3. april 2006).
50. Computer Crime Research Center,http://www.crime-research.org/ (29. maj 2006).
51. Computer Security Institute, http://www.gocsi.com/ (29. maj 2006).
52. Computer security threats, http://www.caci.com/business/ia/threats.html#Unintentional%20Threats (19. maj 2006)
53. Computer Security Training, Certification and Research – SANS, http://www.sans.org/ (29. maj 2006).
54. Computer virus, Wikipedia, http://en.wikipedia.org/wiki/Computer_virus (5.maj 2006).
55. *Computer worm grounds flights, blocks ATMs*, CNN: http://www.cnn.com/2003/TECH/internet/01/25 /internet.attack/ (10. maj 2006)
56. Computer, Internet and Information Security, ITSecurity.com, http://www.itsecurity .com/ (29. maj 2006).
57. Corpus, Victor (2006): *If it comes to a shooting war...* Asia Times Online http://www.atimes.com/atimes/China/HD20Ad03.html (20. april 2006).
58. Cracking Clans, http://transcriptions.english.ucsb.edu/curriculum/lci/magazine/s_02/eric/Cracking_final.htm (28. maj 2006).
59. Cyber Security Policy & Research Institute: http://www.cpi.seas.gwu.edu/ (25. marec 2006).
60. Cybercrime – High Tech Crime, http://www.jisclegal.ac.uk/cybercrime/cybercrime.htm/ (27. maj 2006).
61. Cybercrimes, http://cybercrimes.net/ (21. maj 2006).
62. CipherTrust, http://www.ciphertrust.com/ (17. maj 2006).
63. Delo, http://www.delo.si/ (30. maj 2006).
64. Department od Defense, Dictionary of military Terms, http://www.dtic.mil/doctrine/jel/doddict/ (18. marec 2006).
65. Diffrence between Adware & Spyware, http://www.techiwarehouse.com/cms/engine.php?page_id=41cc4355 (15. maj 2006)
66. Dirty spyware tricks, http://www.pcpitstop.com/spycheck/tricks.asp, 15. maj 2006
67. Dnevnik, http://www.dnevnik.si/si/ (30. maj 2006).
68. ESET – We Protect Digital Worlds, http://www.eset.com/index.php, 26. maj 2006

69. Evropska komisija, http://ec.europa.eu/index_en.htm (2. junij 2006).
70. Evropske institucije, http://evropa.gov.si/evropomocnik/question/623-156/ (2. junij 2006)
71. Federal Bureau of Investigation - Cyber Investigations, http://www.fbi.gov/ cyberinvest/cyberhome.htm (27. maj 2006).
72. Federal Trade Commission, http://www.consumer.gov/idtheft/ (16. maj 2006).
73. Federation of American Scientists, http://www.fas.org/main/home.jsp (4. april 2006).
74. *File-sharerers face legal onslaught*, BBC News, http://news.bbc.co.uk /1/hi/technology/4875142.stm (2. junij 2006).
75. Free Security Software that Really Works, http://www.geocities.com /freeantistuff/ (29. maj 2006).
76. Freeware, http://www.pcwebopaedia.com/TERM/F/freeware.htm (15. maj 2006).
77. Goldberg, Ivan (2004) Institute for Advanced Studies od Information Warfare, http://www.psycom.net/iwar.1.html (8. april 2006).
78. Google.com, http://www.google.com (30. maj 2006).
79. How stuff works, http://www.howstuffworks.com (9. maj 2006).
80. HTML, http://www.webopedia.com/TERM/H/HTML.html (2. junij 2006).
81. Human development reports, http://hdr.undp.org/ (3. april 2006).
82. Identity theft, http://en.wikipedia.org/wiki/Identity_theft (16. maj 2006).
83. ILOVEYOU Virus, 2006: http://searchsecurity.techtarget.com/sDefinition /03.html (8.maj 2006).
84. Information and Internet Security Portal, http://www.astalavista.com (30. maj 2006).
85. Information Warfare Glossary, http://www.enolagaia.com/IWGlossary.html (2. april 2006).
86. Infosys, Računalniški inženiring, http://www.infosys.si/ (22. maj 2006).
87. International Biometric Society, http://tibs.org/biometrics/ (16. maj 2006).
88. Internet Privacy and You, http://neworder.box.sk/news/14956 (28. maj 2006).
89. Internet Service Provider, http://en.wikipedia.org/wiki/Internet_service_ provider (19. maj 2006).
90. Internet Terms and Definitions, http://www.rbcwebdesign.com/Terms.htm (29. maj 2006).

91. Internet World Stats, http://www.internetworldstats.com/blog.htm (7. april 2006).
92. *Introduction to Viruses*, Computer Knowledge, http://www.cknow.com/vtutor/ IntroductiontoViruses.html (5.maj 2006).
93. James, Clement (2006): *Spam King Wallace loses court battle*, http://www. vnunet.com/vnunet/news/2155507/spam-king-loses-court-battl (2. junij 2006).
94. Kabay, M.E. (2002): *Logic bombs*, Network World, http://www.networkworld. com/newsletters/sec/2002/01514405.html (9. maj 2006).
95. Kaj je internet?, http://www.telprom.si/faq.htm#Kaj_je_Internet (20. marec 2006).
96. Kaj je IP številka?, http://www.impresija.com/default.asp?id=18 (16. maj 2006).
97. Kaj je piškotek (cookie)?, Mladinska knjiga, http://www.mladinska.com/ emag.aspx?docid=121496&nodeid=1176&day=&month=&year=&selectedmonth= (15. maj 2006).
98. KaZaA, http://www.kazaa.com/us/index.htm, (14. maj 2006).
99. Lavasoft – Protect your privacy, http://www.lavasoft.com/ (26. maj 2006).
100. Legion of Ethical Hacking, http://www.hackerslegion.com/home/news.php (27. maj 2006).
101. Magoo's Wise Words – Guide to Eliminating Spyware, http://guides. radified.com /magoo/guides/spyware/remove_spyware_01.htm (30. maj 2006).
102. *Malicious software: Worms, Viruses and Spyware Fact Sheet,* Rice University, http://www.rice.edu/it/resources/security/mal_software.html (10. maj 2006).
103. Malicuous software, Wikipedia, http://en.wikipedia.org/wiki/Malware (5.maj 2006).
104. Mashevsky, Yury (2006): *Malware Evolution 2005*, Kaspersky Lab http://www.viruslist.com /en/analysis?pubid=178949694 (6. maj 2006).
105. Mateti, Prabhaker (2006): *Viruses, Worms and Trojans*, http://www.astalavista. com/index.php?section=docsys&cmd=details&id=25 (10. maj 2006).
106. Ministrstvo za informacijsko družbo, http://mid.gov.si/mid/mid.nsf (30. maj 2006).
107. National Institute of Standards and Technology, http://www.nist.gov/ (5. april 2006).
108. NSAWatch, http://www.nsawatch.org/resources.html (28. maj 2006).
109. Pacchiano, Ronald (2003): *Firewall Debate: Hardware vs. Software*, http://www.smallbusinesscomputing.com/webmaster/article.php/3103431 (29. maj 2006).

110. Parker, Don: The Different Shades of Hackers (2006), http://www.windows security.com/articles/Different-Shades-Hackers.html (28. maj 2006).
111. *PC viruses hit 20 year milestone*, BBC News, http://news.bbc.co.uk /1/hi/technology/ 4630910.stm (3.maj 2006).
112. PCreVieW – Computer News and Reviews, http://www.pcreview.co.uk/ articles/Windows/Protection_against_Adware_and_Spyware/ (15. maj 2006).
113. *Phishing – nova oblika spletne prevare (kraje)*, SI-CERT, ARNES, http://www. arnes.si/si-cert/obvestila/2004-06.html (2. junij 2006).
114. Policija, http://www.policija.si/si/ (2. junij 2006).
115. *Poročilo podjetja F-Secure o informacijski varnosti v letu 2004*, http://www.f-secure.si/2004/ (2. junij 2006).
116. Predstavitev virusov, črvov in trojanskih konjev, http://www.microsoft.com /slovenija/doma/varnost/virusi/predstavitev_virusov.mspx (10. maj 2006).
117. Preety Good Privacy, http://www.pgp.com/ (2. junij 2006).
118. Protipiratski trojanski konj, http://www.racunalniske-novice.com/main/index.php? page=clanek&cmd=clanek (22. maj 2006).
119. Republika Slovenija – Državni zbor, sprejeti zakoni in akti, http://www.dz-rs.si/ index.php?id =kriminal&mandate=-1&unid=SZ0B41 (30. maj 2006).
120. Ronald B. Standler (2002): Examples of Malicious Computer programs, http://www.rbs2.com/cvirus.htm (7.maj 2006).
121. RTV Slovenija, http://www.rtvslo.si/ (30. maj 2006).
122. SAFE.SI, www.safe.si, (22. maj 2006).
123. Security Definitions – Spyware, http://searchsecurity.techtarget.com/sDefinition /0,,sid14_gci214518,00.html (15. maj 2006).
124. Security Glossary by Lynn Wheeler, http://www.garlic.com/~lynn/secgloss.htm (28. marec 2006).
125. SecurityFocus, http://www.securityfocus.com/ (2. junij 2006).
126. SI-CERT, http://www.arnes.si/si-cert/ (30. maj 2006).
127. Silverman, Sheryl (2003): *Famous Worms and Viruses*: http://www.pbs.org/ newshour/science/computer_worms /famous.html (9. maj 2006).
128. SiOL, http://www.siol.net/ (30. maj 2006).
129. SLO-TECH, http://www.slo-tech.com/ (7. april 2006).
130. Software Engineering Institute, CERT, http://www.cert.org/ (29. maj 2006).

131. Software technology roadmap, Glossary, http://www.sei.cmu.edu/str/indexes/glossary/ (5. april 2006).
132. Spoofed/Forged Email, http://www.cert.org/tech_tips/email_spoofing.html (16. maj 2006).
133. SpyBot Search&Destroy, http://www.safer-networking.org/en/home/index.html (29. maj 2006).
134. Spyware Education Center, http://www.webroot.com/resources/spywareinfo/adware.html (15. maj 2006).
135. Spyware, http://www.webopedia.com/TERM/s/spyware.html (15. maj 2006).
136. The Beginner's Guide to Surfing the Internet Safely, http://www.internet-beginners-guide.com/safe-surfing/ (29. maj 2006).
137. The Delphi Method – The Basics, http://www.iit.edu/it/delphi.html (7. april 2006).
138. The Delphi Method, www.iit.edu/~it/delphi.html (7. april 2006).
139. The Free Dictionary, http://www.thefreedictionary.com/ (5. april 2006).
140. The Hacker Quarterly 2600, http://www.2600.com/ (28. maj 2006).
141. The History Channel, http://www.historychannel.com/exhibits/science_war/iwar.html (6. april 2006).
142. The New Hacker's Dictionary, http://www.outpost9.com/reference/jargon /jargon_toc.html, (15. marec 2006).
143. The New Hacker's Dictionary, http://www.outpost9.com/reference/jargon/jargon_10.html#SEC17/ (19. maj 2006).
144. Trojan horse (computing), http://en.wikipedia.org/wiki/Trojan_horse_ (computing) (10. maj 2006).
145. Trojan Horse Attacks, http://www.irchelp.org/irchelp/security/trojan.html (2. junij 2006).
146. Trojan Horse, http://www.symantec.com/avcenter/venc/data/trojan.horse.html (2. junij 2006).
147. Trojan horse, Webopedia Computer Dictionary, http://www.webopedia.com /TERM/T/Trojan_horse.html (10. maj 2006).
148. Trojanci v porastu, število črvov upada, http://www.racunalniske-novice.com /main/index.php?page=clanek2a915d2 (29. maj 2006).
149. URL, http://www.webopedia.com/TERM/U/URL.html (2. junij 2006).

150. *Virus information*, National Institute of Standards and Technology, Computer Security Division, http://csrc.nist.gov/virus/ (5.maj 2006).
151. Vlada RS, http://www.vlada.si/ (30. maj 2006).
152. Webopedia, http://www.webopedia.com/ (10. maj 2006).
153. What is a computer worm?, TechFaq, http://www.tech-faq.com/computer-worm-virus.shtml (10. maj 2006).
154. What is a logic bomb?, http://www.tech-faq.com/logic-bomb.shtml (6. maj 2006).
155. What is ASCII?, Indiana University, Knowledge Base, http://kb.iu.edu/data /afht.html (19. maj 2006).
156. What is freeware and shareware?, https://help.attbusiness.net/index.cfm? fuseActio n=home.viewContent&content_id=7322&category_id=7218 (15. maj 2006).
157. What is shareware?, http://www.pc-shareware.com/whatissh.htm (15. maj 2006).
158. What you can do about spyware and other unwanted software?, http://www. microsoft.com/athome/security/spyware/spywarewhat.mspx (15. maj 2006).
159. World Wide Web, http://www.webopedia.com/TERM/W/World_Wide_Web.html (2. junij 2006).
160. Yahoo.com, http://www.yahoo.com/ (30. maj 2006).