UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

ZLONAMERNI PROGRAMI IN ZAŠČITA INFORMACIJSKIH SISTEMOV PODJETJA

Ljubljana, september 2005 GREGOR FRELIH

IZJAVA

Študent Gregor Frelih izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Mojce Indihar Štemberger in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, 9. september 2005 Podpis_____

KAZALO

KAZALO TABEL IN SLIK

Kazalo tabel:

Kazalo slik:

1. Uvod

V današnjem času je računalnik nekaj povsem samoumevnega. Življenja brez njega si ne znamo več predstavljati. Vsi računalniki so med seboj povezani tako ali drugače. Včasih je bilo med seboj povezanih le peščica. In če smo nedolgo tega uporabljali za povezavo v svet modeme, ki so bili povezani le za čas, ko smo povezavo dejansko rabili, je danes širokopasovna povezava že nekaj normalnega. Zadnje velja za gospodinjstva, za podjetja je stalna širokopasovna povezava v svet nujna že nekaj časa.

Neprestana povezanost računalnika na internet povečuje možnost napada nanj. S pametnim ravnanjem so modemski uporabniki lahko »preživeli« tudi brez protivirusne zaščite, na druge oblike pa nihče ni niti pomislil. Takoj, ko računalnik povežemo v svet s stalno povezavo, postane zaščita pred zlonamernimi programi obvezna. Vse to sem občutil tudi na lastni koži. Dokler si nisem omislil ADSL povezave, je bil moj računalnik brez kakršnekoli zaščite. Težav z zlonamernimi programi kljub temu nisem imel. Ob priklopu ADSLja je računalnik ostal neokužen le slab teden. S spremembo načina povezovanja se spremenijo tudi navade uporabnikov. Precej možnosti, ki jih ponuja internet, je bilo prej neizkoriščenih. Hitrosti prenosa so pri modemu tako slabe, da se določenih stvari ne splača uporabljati. Potem se čez noč vse spremeni, izkoristiti želimo vse, kar se nam ponuja. Posledično se poveča tudi ogroženost.

V organizacijah je skrbnikom omrežij že dalj časa jasno, da brez dobre zaščite omrežja in računalniki ne bodo funkcionirali. Domači uporabniki pa to šele ugotavljajo in tako so zelo dobre tarče. Seveda tudi obramba podjetij ni neprebojna, popolne zaščite pa tako ali tako ni, pa naj se še tako trudimo. Neprekinjen pretok informacij je v moderni ekonomiji zelo pomemben. Celi sektorji ekonomije brez računalnikov in računalniških komunikacij ne bi mogli delovati. Zlonamerni programi v takih pogojih lahko povzročijo ogromno škode, zato je preprečevanje takega stanja kritičnega pomena.

V svojem diplomskem delu se bom osredotočil na problem razširitve zlonamernih programov in poskušal prikazati, kako se čim bolje zaščitimo. Oprl se bom na zaščito organizacij. Skrbnikom omrežij je sicer jasno, da je dobra zaščita nujno potrebna. A potrebno je prepričati tudi vodstvo podjetja. Dobra zaščita prinese s seboj stroške, ki jih je potrebno opravičiti. Vendar so učinki nemerljivi. Računalniki ne delajo hitreje, produktivnost ni večja, na prvi pogled po naložbi v zaščito je vse enako kot prej. Veliko lažje je vodstvo v smiselnost naložbe prepričati, ko je že prepozno. Računalniki se okužijo, procesi v organizacije se nekaj dni odvijajo počasneje, nekaj časa morda sploh ne. Ko se to zgodi, vodstvo ni več težko prepričati, denar za nakup je takoj na voljo. Lepo je, če se vodstvo uči na tujih napakah, ne na lastnih.

Na tako dinamičnem področju kot je računalništvo in informatika so spremembe zelo hitre, zato prihaja do zmešnjave in nedorečenosti. V prvem poglavju bom skušal na področje zlonamernih programov vnesti nekaj reda in jih smiselno kategorizirati. Potem bom pogledal, kako je prišlo do takega stanja, kakršnemu smo priča danes. Sledi torej zgodovinski pregled. Na koncu prvega poglavja bom podrobneje predstavil današnje aktualne tegobe in trende.

Drugo poglavje je namenjeno predstavitvi stroškov, ki ji s seboj prinese slaba zaščita. Predstavil bom stroške, ki jih ima podjetje, če je njihova obramba prebita. Prikazane bodo posledice za podjetje, kaj se zgodi v primeru okužbe ali vdora. Konkretne posledice za podjetje bodo predstavljene v neštevni obliki, v števni obliki pa kumulativni podatki za posamezne zlonamerne programe.

V tretjem poglavju bom poskušal pripraviti nabor nasvetov za podjetje, kako se čim učinkoviteje zaščiti. Celovita zaščita je največ, kar lahko sistemski skrbniki v podjetju naredijo za miren spanec, popolna zaščita pa žal niti v teoriji ne obstaja. Predstavil bom rešitve, ki jih lahko uporabijo, na kaj morajo paziti in dodal ceno, kjer se bo dalo.

2. Zlonamerni programi

2.1. Kategorizacija

Operacijski sistemi in aplikacije niso dovzetni za zlonamerne programe, razen če je možno zagnati zunanje programe znotraj tega sistema ali aplikacije. Potencialno ranljivi so (Kaspersky, 2005):

- vsi popularni operacijski sistemi,
- večina pisarniških aplikacij,
- večina grafičnih urejevalcev,
- orodja za management projektov,
- vse aplikacije, ki vsebujejo podporo za izvajanje skript.

Zlonamerni programi se pojavijo, ko so zadoščeni naslednji pogoji (Kaspersky, 2005):

- operacijski sistem je splošno razširjen,
- na voljo je dovolj kvalitetne dokumentacije,
- sistem ni varen ali ima več poznanih ranljivosti.

Tabela 1: Vrste zlonamernih programov

Vrsta zlonamernega programa	Glavne značilnosti	Pomembni predstavniki
Virus	Okuži različne datoteke (izvršne, Wordove, Excelove, itd.). Se sam kopira. Običajno potrebuje človeško interakcijo (odprtje datoteke, branje elektronskih sporočil, zagon sistema ali izvršitev okuženega programa).	Michelangelo, CIH
Črv	Se širi prek omrežja. Se sam kopira. Običajno ne potrebuje človeške interakcije za širjenje.	Morris Worm, Code Red, SQL Slammer
Mobilna zlonamerna koda	Sestavljena iz preprostih programov, ki se jih naloži iz oddaljenega sistema ali izvrši lokalno z minimalno ali brez uporabniške interakcije. Največkrat so napisani v Javaskriptu, VBskriptu, Javi ali ActiveXa.	Cross Site Scripting
Stranska vrata	Obide varnostne protokole z namenom dati napadalcu nadzor nad računalnikom.	Netcat in VNC: oba lahko uporabljamo legalno kot orodje za oddaljeno administracijo ali nelegalno kot orodji za napad.
Trojanski konj, trojanec	Se zamaskira kot uporaben program in s tem zakrije zlonamerno vsebino.	Setiri, Hydan
User-level RootKit	Nadomesti ali spremeni izvršne datoteke, ki jih uporabljajo administratorji in uporabniki.	Linux Rootkit, Universal Rootkit, FakeGINA
Kernel-level Rootkit	Manipulira z jedrom operacijskega sistema z namenom prikrivanja in ustvarjanja zadnjih vrat.	Adore, Kernek Intrusion System
Mešani zlonamerni programi	Združuje različne tehnike že opisane z namenom povečanja učinkovitosti.	Lion, BugBear.b

Vir: Skoudis, 2003, str. 13.

Različni avtorji tudi ponujajo različne kategorizacije. Sam sem se uprl na kategorizacijo avtorjev Skoudisa in Zelsterja. Razvrstitev je zbrana v Tabeli 1 na strani 3, skupaj z osnovnimi značilnostmi. Podroben opis sledi.

Virusi so bili prvi v skupini zlonamernih programov, zato veliko ljudi še danes vse uvršča v to kategorijo. A že dolgo niso več edini in v tem poglavju nameravam jasno razvrstit tipe zlonamernih programov in opisati njihove značilnosti za lažje razumevanje, v katero kategorijo kdo sodi.

2.1.1. Virusi

Virus je program, ki se širi tako, da se pripne na druge programe. Prav tako kot biološki virus potrebuje gostitelja (Hiemstra, 2004). V veliki večini primerov ga mora zagnati človek. Običajno to stori z odprtjem okuženega programa. Ko je enkrat aktiviran, se pripne tudi na druge programe dostopne uporabniku, ki ga je pognal. Z aktivacijo se lahko sproži tudi uničevalni del virusa, kar običajno pomeni brisanje datotek, okvaro datotek ali pa le izpis sporočila na ekranu.

Viruse glede na okolje, v katerem se pojavljajo, razdelimo na (Vuille, 2005):

- datotečne,
- zagonske,
- makro,
- omrežne.

2.1.1.1. Datotečni virusi

Glede na metodo okužbe jih delimo na (Vuille, 2005):

- prepisovalne,
- parazitske,
- spremljajoče,
- povezavne,
- ostale.

Prepisovalni virusi uporabljajo najpreprostejšo metodo okužbe izmed naštetih. Originalni zapis datoteke zamenja s svojim. Odkrijemo jih hitro in lahko, saj operacijski sistem ali okužena aplikacija ne funkcionira več enako kot pred okužbo.

Parazitski virusi spremenijo kodo okužene datoteke, ki zaradi tega ostane delno ali popolnoma delujoča. Svojo kodo lahko zapišejo na različna mesta, na začetku, na koncu ali pa vmes. Vmes se lahko zapišejo tako, da del originalne kode prestavijo na konec.

Spremljajoči virusi ne spreminjajo originalne datoteke, pač pa ustvarijo podvojene datoteko, ki vsebuje virus. Ob zagonu okužene datoteke se najprej izvrši virusov ukaz, nato pa se zažene še originalna datoteka. Običajno preimenujejo končnico prvotne datoteke.

Povezavni virusi prav tako ne spreminjajo vsebine originalne datoteke, pač pa prisilijo operacijski sitem v izvedbo njihove kode. To dosežejo s spremembo polj v datotečnem sistemu.

Ostalih virusov, ki ne spadajo od nobenih zgornjih kategorij, je okoli deset. Nekateri se preprosto zapišejo na disk in upajo, da jih bo uporabnik nekoč zagnal, drugi dodajo vrstico v datoteko, ki se izvrši ob zagonu.

2.1.1.2. Zagonski virusi

Danes poznani zagonski virusi okužijo zagonske sektorje diskete ali trdega diska. Disketo lahko okuži le na en način - tako, da originalni zapis zamenja s svojim. Na trdem disku pa ima več možnosti: lahko zamenja originalni zapis v glavnem zagonskem zapisu, v zagonskem zapisu ali pa spremeni naslove aktivnih zagonskih sektorjev. Največkrat virus prestavi glavni zagonski zapis na drug del diska, sebe pa zapiše na njegovo mesto (Vuille, 2005).

2.1.1.3. Makro virusi

Najbolj so razširjeni makro virusi za Microsoftove pisarniške aplikacije kot so Word, Excel, Power Point itd. Običajno so napisani samo za eno aplikacijo, takšni, ki delujejo v dveh so redki. Makri se izvršijo ob določeni akciji, ki pokliče makro, lahko ob shranjevanju, tiskanju in mnogih drugih situacijah. Avtomatsko se makroji lahko pokličejo ob odprtju ali zaprtju aplikacije.

2.1.1.4. Omrežni virusi

Omrežni virusi uporabljajo omrežna sredstva za svoj obstoj in širjenje. Seveda niso vsi virusi, ki se širijo preko omrežja omrežni virusi. Pravi omrežni virusi so zelo redki. Delujejo le v primeru, da je računalnik povezan v omrežje in se ne zapišejo na disk, pač pa tečejo le v pomnilniku računalnika.

2.1.2. Črvi

Značilna karakteristika črva je, da se širi po omrežju in ne potrebuje gostiteljske datoteke. Se sam replicira in običajno ne potrebuje posredovanja uporabnika računalnika. Posamezni

okuženi računalnik je le en odsek, ki potem skupaj z ostalimi okuženimi tvori močnega črva. Vsi ti računalniki potem delujejo proti istemu cilju.

Glede na metodo okužbe jih delimo na:

- črve elektronske pošte,
- črve takojšnih sporočilnikov,
- internetni črve,
- črve spletnega klepeta,
- črve omrežij za souporabo datotek.

Črvi elektronske pošte se širijo preko okužene elektronske pošte, lahko v obliki priponke, lahko kot povezava do okužene spletne strani. Za širitev lahko uporabi program za elektronsko pošto - Outlook - se direktno poveže z poštnim strežnikom ali pa prek funkcije v Oknih. Naslovnike izbira iz imenikov, ki so na voljo na okuženem računalniku, uporabi naslove iz poštnega nabiralnika ali celo išče po disku možne zapise elektronskih naslovov po značilnih znakih.
Črvi takojšnih sporočilnikov pošiljajo povezave do okuženih spletnih strani vsem lokalnim stikom. S klikom na povezavo se potem uporabnik okuži.
Internetni črvi uporabljajo veliko tehnik za svoje širjenje. Preverjajo oddaljene računalnike, če je kateri od njih ranljiv in se potem skopirajo v mape, ki to omogočajo. Nekateri med njimi se specializirajo na znane pomanjkljivosti v operacijskih sistemih in so bistveno bolj nevarni. Uporabljajo tudi zadnja vrata, ki so jih odprli drugi zlonamerni programi in se prek njih namestijo na računalnik.
Črvi spletnega klepeta se širijo ali prek povezav ali s pošiljanjem datotek. Uporabniki si lahko med seboj poleg sporočil pošiljajo tudi datoteke. Vendar je najprej potrebno potrditi prenos in potem shranjeno datoteko še odpreti. Ciljajo na naivnost uporabnikov.
Črvi omrežij za souporabo datotek se širijo tako kot tudi ostale datoteke v omrežju. Uporabniki ga dajo na voljo drugim in jih premamijo običajno z lažnim imenom, ki nakazuje na to, da gre za datoteko, ki si jo želijo.

2.1.3. Mobilna zlonamerna koda

Mobilna zlonamerna koda je majhen program, ki ga naložimo z oddaljenega sistema. To se zgodi z minimalnim ali celo brez uporabnikovega posredovanja. Večji del jih lahko razvrstimo v tri skupine (Skoudis, 2003, str.13):

- brskalnikove ukazne datoteke,
- kontrolniki activeX,
- programčki v Javi.

Razvijalci spletnih strani v želji po čim lepših in uporabnih spletnih straneh, ki bodo pritegnile obiskovalce k ogledu in vračanju nanje, uporabljajo tudi močnejša programerska orodja od HTMLja. Določenih vsebin se ne da ponuditi brez uporabe Jave ali ActiveXa. V želji po ogledu takih strani, ki so drugače povsem legalne in zelo uporabne, pa se odpre okno tudi za zlorabe.

2.1.4. Trojanci

Trojanci oz. trojanski konji so programi, ki so videti nenevarni, v resnici pa skrivajo zlonamerno naravo. Od tod tudi ime za te programe. Glede na to, kaj storijo na okuženem računalniku, jih delimo na (Viruslist.com, 2005):

- splošne,
- geselne,
- klikajoče,
- vohunske,
- obveščevalne,
- posredovalne,
- snemajoči,
- logične bombe.

Splošni trojanski konji vključujejo različen nabor programov, ki poškodujejo računalniški sistem, ogrožajo podatkovno integriteto in prizadenejo delovanje računalnika.
Geslni trojanski konji kradejo gesla, običajno gesla, ki omogočajo nadzor nad računalnikom. Poleg tega na računalniku iščejo tudi datoteke, ki bi lahko vsebovala gesla ali druge informacije zaupne narave. Te zbrane podatke potem pošljejo v zakodirani obliki po elektronski pošti do stvaritelja programa.
Klikajoči trojanski konji se uporabljajo za preusmeritev uporabnika na določeno spletno stran. To storijo tako, da ali pošljejo brskalniku ukaz za odprtje določene strani ali pa zamenjajo sistemsko datoteko, kjer so shranjeni naslovi spletnih strani.
Snemajoči trojanski konji s spletnih strani snamejo in naložijo nove zlonamerne programe, ali pa programe, ki potem kažejo oglase na žrtvinemu računalniku. Potem novi program požene, lahko pa ga doda med programe, ki se bodo zagnali ob vklopu računalnika. Vse to brez vedenja uporabnika.
Posredovalni trojanski konji delujejo kot posredovalni strežniki in omogočajo anonimni dostop do interneta preko okuženega računalnika. Zelo priljubljeni so med pošiljatelji neželene elektronske pošte.
Vohunski trojanski konji pod svojim okriljem združujejo nabor različnih vohunskih programov in programov, ki prestrezajo naše vnose preko tipkovnice. Vsi sledijo in beležijo uporabniško aktivnost in te podatke pošiljajo gospodarju. Največkrat se uporabljajo za zbiranje informacij povezanimi z bančnimi računi za omogočanje bančnih prevar.

Obveščevalni trojanski konji posredujejo podatke o okuženem računalniku. Tako potrdijo uspešno okužbo in pošljejo IP naslov, odprte številke vrat (portov), e-poštne naslove itd. Običajno spremljajo druge trojance z namenom obveščanja.
Namen **logičnih bomb** je sabotaža. Ob odprtju okužene stisnjene datoteke se bo njegov računalnik sesul ali zelo upočasnil, disk pa bo zapolnjen z brezpredmetnimi datotekami. Posebej nevarni so za strežnike, ki potem ne morejo več opravljati svoje naloge.

2.1.5. Stranska vrata

Stranska vrata so zaporedje ukazov, ki omogočajo uporabniku, da preskoči standardni varnostni sistem računalnika. Taka stranska vrata si pogosto naredijo sistemski inženirji oziroma zaposleni, ki skrbijo za sistemske programe. Omogoča jim lažji vstop v računalniški sistem. Storilec, ki najde stranska vrata, jih lahko uporabi za kriminalno dejanje (Gradišar, 2003, str. 258-259).

Napadalcu omogočajo nadzor nad sistemom. Nekateri avtorji to kategorijo zlonamernih programov uvrščajo med trojance. Stranska vrata se lahko uporabijo za izvrševanje različnih ukazov in pridobitvijo popolnega nadzora nad okuženim računalnikom. Običajno jih namestijo tako, če niso že nameščena, da izkoristijo ranljivost sistema. Le-ta je lahko posledica napake v samem sistemu ali posledica slabe prilagoditve. Možno je tudi preslepiti uporabnika računalnika, da jih namesti sam.

Programi te skupine delujejo na enak način kot legalni programi za oddaljeno administracijo, ki jih uporabljajo skrbniki računalnikov. To dejstvo otežuje njihovo odkritje. Pravzaprav je edina razlika med legalnimi in nelegalnimi, da so slednji nameščeni brez uporabnikove vednosti. Ko je enkrat nameščen, mnogokrat nadzira lokalni sistem tako, da proces ni viden med aktivnimi programi in procesi.

2.1.6. »User-level RootKit«

So združek stranskih vrat in trojanskega konja. Uporabljajo jih za odprtje in zakritje stranskih vrat. Napadalcu ne omogočajo takojšne pridobitve administratorskih pooblastil, jim pa dopuščajo, da jih pridobijo kasneje. Večina programov tega tipa zamenja več funkcij napadenega operacijskega sistema. Zamenjajo izvršne datoteke in knjižnice.

Ime tega tipa zlonamernih programov izvira iz UNIXove računalniške sfere, iz računa ki ima vsa pooblastila na računalniku. Je tudi najpogostejši za ta tip operacijskega sistema, torej večino Linux distribucij. A ni omejen le na ta operacijski sistem, obstajajo tudi izvedenke za Okna.

2.1.7. »Kernel-level RootKit«

Z manipuliranjem jedra operacijskega sistema lahko omogoči napadalcu, da doseže hitrejšo in popolnejšo kontrolo nad operacijskim sistemom. Z njegovim nadzorom je možno spremeniti obnašanje operacijskega sistema, skriti je možno mape, datoteke, spreminjati vrata in jih odpirati.

2.1.8. Drugi z zlonamernimi programi povezani programi

Sem spadajo programi, ki so sicer legalni, a jih hekerji[1] uporabijo v svojo korist. Vnaprej ni mogoče napovedati, kateri programi bodo padli v to skupino. Če so legalni programi spretno uporabljeni v ilegalne namene, je to zelo težko odkriti. Podkategorije so:

- klicatelji,
- snematelji,
- FTP strežniki,
- posredujoči strežniki,
- telnet strežniki,
- spletni strežniki,
- IRC odjemalci,
- orodja za odkrivanje gesel,
- oddaljena administracija,
- šale in potegavščine.

V tej kategoriji so trenutno najbolj izpostavljeni t. i. klicatelji. Le-ti ne poškodujejo operacijskega sistema ali katere od drugih aplikacij, nameščene na računalnik, lahko pa nas zelo udarijo po žepu. Lastniki določenih spletnih strani uporabljajo ta način za zaračunavanje svojih storitev, ogledov spletnih strani. Največkrat so to spletne strani s pornografsko vsebino. Obstajata dve varianti klicateljev: trojanski klicatelji in zahrbtni klicatelji. Prvi se namestijo brez uporabnikove vednosti in tudi kličejo brez potrditve, drugi pa se prav tako samodejno namestijo, a pred klicem na to opozorijo uporabnika. Ogroženi so le tisti uporabniki, ki imajo na računalnik priklopljen delujoč modem, le-ta pa ima povezavo s telefonsko linijo.

[1] Prevod besede heker (hacker) je zelo zahteven, saj se pod tem pojmom v državah, od koder izvira ta termin, razume v bolj širokem pomenu besede, kot pa razlage, ki krožijo v slovenskem jeziku. Pogosto srečujemo različne prevode, ki pa besedi odvzamejo pravi pomen. Veliki slovar tujk Cankarjeve založbe iz leta 2002 besedo heker prevaja kot tehnično dobro podkovan računalniški navdušenec in kdor vdira v računalniške sisteme.

2.2. Kronološki pregled razvoja zlonamernih programov

Koncept zlonamernih programov se zdi relativno nov. Novice o njihovem obstoju in nevarnosti so prodrle do laične javnosti precej pozno. Razlog se skriva v predhodni manjši razširjenosti osebnih računalnikov in manjšemu številu povezav do interneta. Domači računalniški uporabniki so resnično ogroženi postali šele z razmahom širokopasovnih povezav, pred tem je bila grožnja bistveno manjša.

2.2.1. Prvi pojav virusa v zgodovini

Pojav prvega računalniškega virusa še ni dorečen. Ve se, da so računalniki bili okuženi z virusi že v sedemdesetih letih prejšnjega stoletja. A koncept se je pojavil že prej. Na začetku so od zlonamernih programov obstajali le virusi, kmalu so se pojavili tudi prvi trojanci.

Prvi virus je bil pravzaprav igra, ki jo je ustvarila skupina razvijalcev v ameriškem podjetju Bell (Skoudis, 2003, str. 28). Igra se je imenovala Darwin. Šlo je za boj dveh programov, ki sta jih napisala igralca. Program je lahko sledil in napadal nasprotnikov program ter se razmnoževal. Cilj igre je bil izbris nasprotnikovega programa. Ta koncept se je lahko uporabil tudi v druge namene, ki ob pisanju igre niso bili predvideni.

2.2.2. Zlonamerni programi med letom 1970 in 1980

Omrežje ARPANET, omrežje ameriške vojske in predhodnik interneta, je v začetku sedemdesetih let bilo prvo na udaru. Virus Creeper se je širil preko računalnikov v omrežje priključenih z modemi. Sam je bil sposoben pridobiti nadzor nad računalnikom in se kopirati na druge. Malo kasneje se je kot odgovor pojavil še en virus, ki je imel nalogo izbrisati Creeper-ja z imenom Reaper. Tudi ta se je samodejno širil po omrežju. Bil je napisan anonimno, tako da se ne ve ali je bil to odgovor na prvotni virus ali pa je avtor isti in je le poskušal popraviti svojo napako.

Leto 1974 je bilo v zgodovini virusov leto Rabbit-a. Slovenski prevod virusa je Zajec, razlog za tako ime pa se skriva v dejstvu, da ni počel nič drugega, kot da se je množil. Na okuženem sistemu je delal vedno nove kopije samega sebe in tako prizadel sposobnosti računalnika.

2.2.3. Zlonamerni programi med letom 1980 in 1990

Računalniki so postajali vedno bolj popularni, tako je vedno več ljudi pisalo tudi programe zanje. Napredek v telekomunikacijah je prinesel pripravno podlago za njihovo širjenje – tako

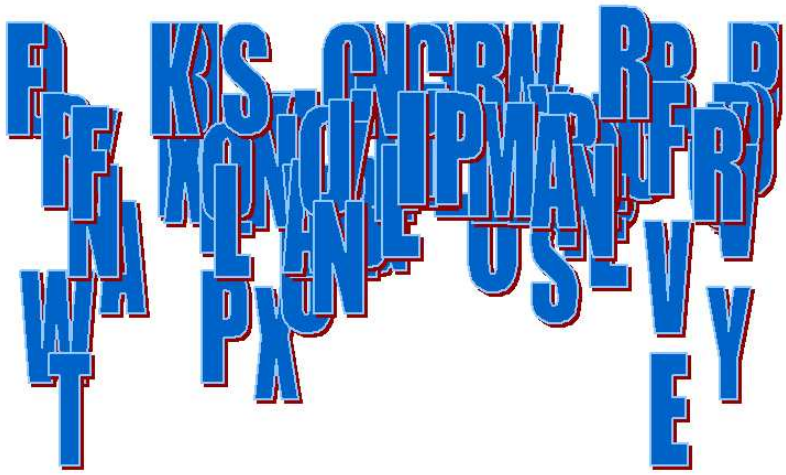
uporabnih kot zlonamernih. Teren je bil tako pripravljen in pojavili so se prvi trojanci. Uporabniki so si program sami naložili na računalnik, medtem ko se sam ni znal širiti.

Elk Cloner se je širil prek okuženih disket na operacijskem sistemu Apple II. Takrat je bil najbolj razširjen in zato najbolj na udaru. Računalniki so se zaganjali z disket in z zagonom sistema je bil zagnan tudi virus. Virus se je potem kopiral na neokužene diskete in se tako širil. Prikazoval je vrteče slike, utripajoča sporočila in šale (Skoudis, 2003, str. 47).

Prvi virus za IBM združljive računalnike se je pojavil v letu 1986. Brian se je zapisal v zagonske sektorje in se bliskovito širil. Glede na to, da je bil pojem virus med takratnimi uporabniki računalnikov popolne neznanka, tudi znanja o zaščiti ni bilo. Informacije o pravilni obrambi je bilo težko dobiti, saj se je pojavljalo mnogo zavajajočih podatkov. Avtor virusa je znan in sicer je šlo za pakistanskega programerja Basita Farooqa Alvija in njegovega brata Amjada. Ni ju bilo težko najti, saj so bili njuni podatki zapisani v kodi virusa. Z virusom sta želela opozoriti na spoštovanje avtorskih pravic. Tako virus, razen da se je zapisal v zagonski sektor in spremenil ime diska v »© Brian«, ni napravil škode.

Leigh je bil prvi, ki je direktno napadal podatke na disku. Na srečo je bilo na univerzi v Leighu dovolj ljudi sposobnih ga ustaviti in tako ni nikoli prišel na računalnike izven univerze. Zanimivo je, da je poleg datotek na disku v končni fazi izbrisal tudi sebe.

Slika 1: Cascade virus



Vir: Virus Screenshots, 2005.

Cascade je bil prvi zakodiran virus in je bil sestavljen iz dveh delov: iz glavnega dela in iz ključa za kodiranje. Tako je virus v vsaki okuženi datoteki deloval na videz drugače. Ob aktiviranju so znaki na zaslonu kaskadno popadali v zadnjo vrstico na zaslonu. Cascade je bil razlog, da je IBM začel razvijati protivirusne programe za splošno uporabo. Pred tem so jih uporabljali le interno.

V letu 1989 se je pojavil do takrat najnevarnejši virus po imenu Datacrime. Na okuženih računalnikih je sprožil nizko nivojsko formatiranje in tako nepovratno uničil podatke na disku. Konec istega leta je bilo po svetu razposlanih 20.000 disket z informacijami o AIDSu. Na disketi se je skrival trojanec, ki se je avtomatično namestil na računalnik in ga tako okužil. Po 90 zagonih računalnika je zakamufliral obstoječe datoteke na disku. Vidna je bila le še ena, v kateri je bil zahtevek po nakazilu denarja na bančni račun. Tako je bilo relativno lahko odkriti avtorja po imenu Joseph Popp, ki pa je bil že pred tem razglašen za duševno bolnega. Kljub temu je bil v Italiji obsojen v odsotnosti.

Epidemija se je razširila v Rusijo, kjer se je pojavilo približno deset virusov, večinoma nekoliko spremenjene verzije že prej omenjenih. Tako se je okužil tudi računalnik Eugena Kasperskyja, ki je kasneje ustanovil Kaspersky Lab in posvetil svoje življenje protivirusnim raziskavam. Istega leta so po svetu ustanovili naslednja podjetja, ki izdelujejo protivirusne programe:

- F-prot,
- ThunderBYTE,
- Norman Virus Control.

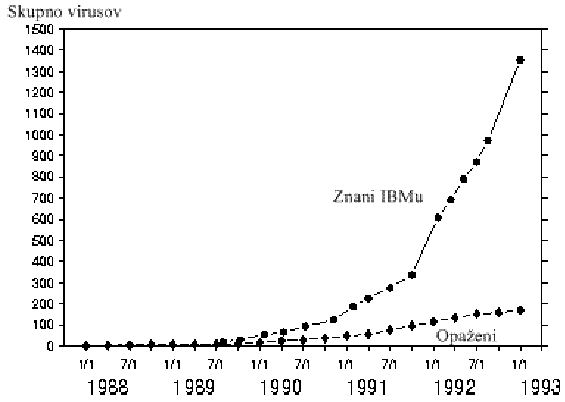
Svoj program za zaščito je zaradi pritiska javnosti izdal tudi IBM, takrat najpomembnejše podjetje na področju informacijske tehnologije. IBM Virscan for MS DOS je bil na voljo za 35 dolarjev.

2.2.4. Zlonamerni programi med letom 1990 in 2000

Vsa prej našteta podjetja je zelo zaposlil Mark Washburn, avtor Chameleona. Razvit iz prej omenjenih Vienna in Cascada je nastal virus, ki je bil zakodiran in je spreminjal svojo kodo z vsako novo okužbo. Tako so bili vsi obstoječi programi za zaščito neuporabni, saj so vsi odkrivali okužbe na podlagi prej znane kode. Kmalu so se pojavili algoritmi, ki so bili sposobni odkriti take okužbe in so del protivirusnih programov še danes.

Zaradi širitve IBM kompatibilnih računalnikov in operacijskega sistema MS DOS je bila ta sfera vedno bolj na udaru. Praktično vsak dan so se pojavljale nove grožnje, število virusov je neverjetno naraslo. Na Sliki 2 na strani 13 imamo prikaz naraščanja števila virusov za DOS. Kot vidimo, je število naraščalo zelo hitro, a na srečo jih je bilo veliko razvitih le v laboratorijih in drugih kontroliranih okoljih. Nikoli se niso pričeli nekontrolirano širiti. Pojavil se je celo modul s spremljajočo dokumentacijo, ki je olajšal delo piscem virusov. Zaradi poplave tako napisanih programov ni bilo popolne zaščite, čeprav so na njej delali več mesecev. Poleg tega se je pojavil še Peach, ki je napadal protivirusne programe in onemogočal zaščito sistema ter tako omogočal okužbo sebi in drugim.

Slika 2: Število različnih virusov za DOS



Vir: Kephart, 1993, str. 12.

Marca 1992 je v medijih odjeknila novica o virusu Michelangelo, za katerega so napovedovali, da bo okužil 5 milijonov računalnikov. Čeprav jih je uspel okužiti le nekaj tisoč, se je mnogim vtisnil v spomin zaradi publicitete. Virus je bil odkrit pol leta pred objavo v medijih, ob objavi pa je bil najbolj razširjen. Win.Wir_1_4 je bil prvi pisan za operacijski sitem Okna in ga omenjam le zato, ker je bil prvi, saj je bil slabo napisan in pravzaprav brez okenske funkcionalnosti.

Prvi virus za Okna 95 se je pojavil v začetku leta 1996 z imenom Boza. V istem obdobju se je za predhodno verzijo, Okna 3.x, pojavil Win.Tentacle in okužil bolnišnična omrežja in druge organizacije v Franciji. Bil je prvi, ki se je razširil prosto po omrežju, vsi dosedanji okenski virusi so se nahajali v kontroliranem okolju kot del zbirk piscev virusov ali elektronski revij. IBMov operacijski sitem OS/2 je svojo nadlogo dobil pod imenom OS2.AEP in je napadal datoteke s končnico exe.

Množično okužbo so začeli povzročati makro virusi. Laroux je bil prvi pisan za Microsoft Excel. Njihov obstoj je omogočal Visual Basic, vgrajen v Excel in Word. Pojavila so se celo orodja, ki so omogočala hitro izdelavo makro virusov za prej omenjena Microsoftova pisarniška produkta. Leto 1996 lahko smatramo kot začetno leto napada na Microsoftova operacijska sistema Okna 95 in Okna NT ter pisarniška produkta Excel in Word. V tem letu in enem kasneje je izšlo ducate virusov za oba operacijska sistema in na stotine makro virusov. To so bili torej programi, ki so napadali 32 bitne operacijske sisteme, MS-DOS je namreč 16 bitni operacijski sistem.

V letu 1997 so se virusi premaknili v še eno novo okolje, pojavil se je prvi pisan za Linux operacijski sistem. Imenoval se je Linux Bliss. Homer je bil prvi črv, ki je uporabljal FTP protokol za svoje širjenje, Esperanto pa je bil prvi poskus virusa, ki bi deloval na več platformah. Na srečo neuspešen. Povečanje priljubljenosti spletnih klepetalnic, v okenskem

okolju zlasti programa mIRC, omogoči nov način širjenja zlonamernih programov. Začetna verzija programa je imela varnostno luknjo in je omogočalo izvedbo kode brez posredovanja uporabnika, kar so v kasnejši verziji odpravili. Kasneje so uporabniki okužili svoj računalnik zaradi svoje naivnosti, saj so morali dovoliti prenos in kasneje še program pognati.

Zaradi že nekaj časa vodilne vloge Microsoftovih operacijskih sistemov in pisarniških produktov so se pisci zlonamernih programov osredotočili na to fronto. Širok nabor trojancev je bil narejen za krajo gesel in administracijo na daljavo. Znan je še en primer distribucije okenskega virusa na CDju, ki jo je svoji reviji za področje Anglije, Slovenije, Švice in Italije prilagal PC Gamer. V drugi verziji znani kot Win95.Marburg je bil poleg Win95.HPS prvi nedosovski polimorfni virus.

Prvi virus za Microsoft Access je bil AccesV, odkrit marca 1998. Uporabniki so novico sprejeli mirno, kot kaže so se sprijaznili z dejstvom, da so Microsoftovi produkti ranljivi. Red Team je postavil nov mejnik, saj je okužil exe datoteke v Oknih in se pošiljal po elektronski pošti s pomočjo Eudorinega odjemalca. Win95.CIH z izvorom na Tajskem je povzročal materialno škodo, saj je izbrisal BIOS matične plošče, kar je v najslabšem primeru pomenilo menjavo matične plošče. Java.StrangeBrew je nakazal, da se odpirajo nove možnosti širjenja zlonamerne kode. Čeprav nenevaren, je pokazal, da se bo možno okužiti le z gledanjem spletnih strani.

Širjenje črvov preko elektronske pošte je postalo zelo popularno. Poštna sporočila, na videz poslana od naših znancev, so vsebovala priponke z nevarno vsebino. ZippedFiles je bil na začetku poslan kot datoteka s končnico exe. Ob zagonu je uničil datoteke priljubljenih programov. Ker so ga v taki obliki zelo hitro ustavili, je v naslednji inačici videti kot stisnjena datoteka s končnico zip. Stisnjen z Neolitinim algoritmom je zaradi vrste, ne vsebine, bil neberljiv za protivirusne programe, ki so sposobnost branja takih datotek dobili šele naslednje leto. Danes je praktično nemogoče poslati program preko elektronske pošte s končnico exe, četudi gre za nenevaren program. Vse take datoteke so namreč blokirane na več nivojih in odstranjene.

Črv Babylonia je obrnil nov list v zgodovini zlonamernih programov s svojo sposobnostjo posodabljanja. Vsako minuto se je povezal s strežnikom na Japonskem in preveril, če obstaja novejša verzija. Ob odkritju novejše verzije je le-to naložil na okužen računalnik. Zaradi bližajočega se leta 2000 je bila tudi prisotna propaganda, ki je spodbujala uporabnike k kupovanju zaščite pred virusi. Ob prelomu tisočletja naj bi na plan udarilo mnogo več virusov kot običajno. Kot se je izkazalo kasneje, je šlo za prazne grožnje, za pospeševanje prodaje.

2.2.5. Zlonamerni programi v začetku 21. stoletja

1. maja 2000 se je skriptni virus LoveLetter zapisal v Guinessovo knjigo rekordov kot najbolj razširjen virus na svetu s 3,1 milijoni okuženimi računalniki po vsem svetu (Guinness World Records, 2004). Virus se je skrival v txt in vbs datotekah, ki so do takrat veljale za nenevarne. Pognan je uničeval druge datoteke in se poslal na vse naslove v Outlookovem imeniku. Zaradi preprosto berljive kode je doživel mnogo modifikacij in danes obstaja prek 90 njegovih predelav. Tudi PalmOS, operacijski sistem za dlančnike, je dobil svoj zlonamerni program. Liberty je bil trojanec, ki je zbrisal datoteke na dlančniku, ni pa se znal samodejno širiti.

Leto 2001 je bilo v znamenju izkoriščanja ranljivosti operacijskih sistemov in aplikacij. Najbolj znani so CodeRed, Nimda, Aliz in BadtransII. Za obrambo ni dovolj le posedovanje protivirusnega programa, nujno je sprotno posodabljanje sistema. Nimda je bil sposoben okužiti računalnik, če je uporabnik le pregledoval elektronsko pošto. Če je pogledal sporočilo v okno za predogled, je bilo to dovolj. CodeRed je bil še hujši, pregledoval je računalnike povezane na internet in jih okužil.

Okužbe preko elektronske pošte in interneta so strmo narasle. 90 % okužb se je tako zgodilo preko elektronske pošte. Napadi preko interneta so dosegli novo evolucijsko stopnjo. Nekoč je veljalo, da je moral uporabnik potrditi nalaganje izvršne datoteke preko spleta, v letu 2001 pa je bil dovolj le še obisk okužene spletne strani. Večina napadalcev je uporabljala varnostne luknje v Internet Explorerju.

Programi za takojšno sporočanje kot sta ICQ in Microsoft Messenger so prav tako postali poligon za širjenje novih zlonamernih programov. Programi za neposredno uporabniško povezavo so bili naslednji na vrsti. Mandragore se je širil po Gnutellinem omrežju. To leto je prineslo še eno neprijetno presenečenje: pojavili so črvi, ki se niso zapisovali v datoteke na disku, pač pa so tekli v pomnilniku. To je zahtevalo novo prilagoditev orodij za obrambo in vsi sodobni danes poleg pregleda diska pregledajo tudi pomnilnik.

V letu 2002 nobenemu zlonamernemu programu ni uspelo okužiti ogromno računalnikov. V prejšnjih letih je za večino okužb v letu poskrbelo le nekaj programov (2-3), tokrat pa so bili okužbe v manjšem obsegu. A vseeno se število okužb ni zmanjšalo, kar pomeni da se je povečalo tudi skupno število zlonamernih programov. Da nobenemu od njih ni uspela okužba v večjem obsegu, so zaslužni uporabniki, ki so postali precej bolj ozaveščeni in so zaščitili svoje računalnike bodisi s ustreznimi programi in posodobitvami bodisi z bolj premišljenim vedenjem.

Prvi globalni napad v letu 2003 je 25. januarja izvedel črv Slammer, ki je izkoriščal varnostno luknjo v Microsoftovem SQL strežniku. V samo nekaj minutah je okužil več sto tisoč računalnikov po svetu in zaradi povečanega prometa povzročil sesutje več omrežij ki

tvorijo internet. Črv se je preko porta 1433 ali 1434 zapisal v pomnilnik, njegov izvor umeščajo na daljni vzhod.

Drugi napad je bil usmerjen na osebne računalnike. Črv Lovesan je ciljal na uporabnike Oken 2000 in XP. Širil se je direktno preko interneta, natančneje preko procesa imenovanega RPC DCOM. Uspelo mu je okužiti več milijonov računalnikov po svetu. Tudi v tem primeru gre za »breztelesni« črv in teče direktno v pomnilniku računalnika. Na srečo je napisati tak program izredno težko in od takrat se je pojavil le še eden, a kot vidimo, gre za izredno učinkovit način. Na okuženem računalniku je izpisal sporočilo, da se bo računalnik čez eno minuto znova zagnal. Izvršitev je bilo možno prekinit le z ukazom »shutdown –a«, a večina uporabnikov ga ne pozna. Ob pogosti ponovitvi je vse skupaj resnično preizkušalo živce uporabnikov. Lovesan je začel še en trend, napad na spletne strani. Z okuženih računalnikov je pošiljal zahtevo po ogledu določene spletne strani in glede na to, da je zahteva prišla z mnogo naslovov strežnik, na katerem je stran tekla, ni zmogel obremenitve. Gre za DoS napad, napad zavrnitve storitve. Napadel je Microsoftov strežnik in tako želel onemogočiti posodobitev ogroženih računalnikov, a na srečo napad ni uspel.

Sobig.f je črv, ki za svojo širitev uporablja elektronsko pošto. Prva verzija se je pojavila januarja z imenom Sobig.a, z verzijo f pa je bilo 8 mesecev kasneje okuženo vsako deseto sporočilo. Črv je pripravljal teren za izvršitev ukaza, ki bi ga moral dobiti 22. avgusta, a so strežnik pravočasno ugasnili.

Slammer in Lovesan sta utrla pot črvu Swenu, ki se je širil preko elektronske pošte, IRCa in P2P omrežij. V svojem sporočilu se je predstavljal kot varnostni popravek za Microsoftova Okna, v sporočilu je bil njihov logo, povezava do popravka in zelo prepričljiv tekst. Uporabniki so se v tem času že naučili, da so posodobitve pomembne, zato so kliknili na povezavo. Kljub temu, da je bila povezava na videz do Microsoftove strani, je bila v resnici do okuženih strežnikov in posledično do črva.

Najresnejšo do sedaj znano epidemijo je povzročil črv Mydoom.a. Širil se je po vnaprej okuženih računalnikih podobno kot Sobig, s sporočilom podobnim Swenu in odprl stranska vrata, da je lahko izvedel DoS napad, podobno kot Lovesan, na domačo stran podjetja SCO. Napad je bil uspešen, stran je bila kar nekaj časa nedosegljiva. Mydoom.a je okužil več milijonov računalnikov in ustvaril več elektronskih sporočil kot Sobig.f. Skozi zadnja vrata, ki jih je na računalniku odprl Mydoom, so kasneje nameščali svoje programe tudi drugi avtorji. Izbrisali so prvotni program in namestili svojega.

Pravkar omenjeno tehniko je uporabil tudi Netsky.b, poleg Mydooma je brisal tudi Bagla. V svoji kodi je imel zakodirano sporočilo, ki je pozivalo avtorje rivalskih virusov na obračun, ki so ga avtorji Bagla tudi sprejeli.

Sasser je v Evropi povzročil resen izbruh. Izkoriščal je ranljivost oken in se širil podobno kot Lovesan, z direktnim priklopom na računalnik preko interneta. Avtor je najstnik Sven Jaschan in so ga aretirali. Obsojen je bil na leto in devet mesecev pogojne kazni (Pogojna kazen za izumitelja uničujočega virusa, 2005). Tako mila kazen zaradi dejstva, da so ga obravnavali kot mladoletnika, saj v času prestopka še ni dopolnil 18 let. S svojim delom je pokazal, da za uspešen napad ni potrebna originalnost, uspešne so tudi predelave in kopije že uporabljenih programov.

2.3. Zlonamerni programi danes

Tabela 2: 20 najpogostejših zlonamernih programov junija 2005

Mesto	Sprememba v mestu	Ime	Odstotek
1.	+1	črv elektronske pošte Netsky.q	14,67
2.	-1	internetni črv Mytob.c	13,58
3.	+5	črv elektronske pošte Zafi.b	8,01
4.	-1	črv elektronske pošte Zafi.d	6,54
5.	-1	internetni črv Mytob.be	6,12
6.	=0	internetni črv Mytob.bk	6,07
7.	-2	črv elektronske pošte NetSky.aa	4,41
8.	nov	internetni črv Mytob.bt	2,65
9.	-1	črv elektronske pošte Netsky.b	2,52
10.	+8	internetni črv Mytob.bi	2,11
11.	+3	internetni črv Mytob.au	1,85
12.	povratnik	črv elektronske pošte Netsky.d	1,73
13.	-1	internetni črv Mytob.u	1,62
14.	-4	internetni črv Mytob.ar	1,59
15.	-8	črv elektronske pošte LovGate.w	1,59
16.	-5	internetni črv Mytob.q	1,37
17.	-1	internetni črv Mytob.t	1,30
18.	-1	črv elektronske pošte Mydoom.l	1,20
19.	povratnik	črv elektronske pošte Mydoom.m	1,17
20.	povratnik	črv elektronske pošte Bagle.ah	1,04
Ostali zlonamerni programi			18,86

Vir: Gostev, 2005.

V Tabeli 2 imamo lestvico dvajsetih najpogostejših zlonamernih programov v juniju 2005. Takoj opazimo da gre pravzaprav le za dva tipa črvov, za črve elektronske pošte in internetne črve. Vodilni na prvem mestu je zopet Netsky.q, ki je po treh mesecih na prvem mestu zamenjal internetni črv Mytob.c. V drugem stolpcu vidimo tudi spremembe mest za ostale zlonamerne programe, v zadnjem pa njihov delež med vsemi.

2.3.1. Črvi neposrednega sporočanja

Širjenje črvov preko programov za neposredno sporočanje je bilo, relativno gledano, največje v letu 2005. Absolutno gledano predstavljajo majhen delež med vsemi programi. Kaže, da so v začetni fazi razvoja. Napisani so večinoma v Visual Basicu zato lahko sklepamo, da so njihovi avtorji novi na prizorišču. Ta programski jezik se je lahko naučiti, a je preokoren za resne projekte na tem področju. Večinoma so kopije že objavljenih kod zlonamernih programov, samo preneseni v novo okolje.

Najbolj zanimiv je način, kako ti črvi pridejo do svojih žrtev. Čeprav programi za neposredno sporočanje omogočajo izmenjavo datotek večinoma ne uporabljajo te metode za svoje širjenje. Namesto tega pošiljajo povezavo do okužene strani. To metodo so včasih uporabljali črvi elektronske pošte. Uporabniki omrežja mislijo, da gre za zanesljiv vir in kliknejo na povezavo. Tako se tudi sami okužijo. Naslednji na vrsti so vsi, ki jih imajo na svojem seznamu, se pravi ljudje, s katerimi pogosto komunicirajo. Tudi ti bodo kmalu dobili sporočilo s povezavo do okužene spletne strani. Črvi potem izkoristijo funkcijo brskalnika, ki samodejno namesti kodo, dobljeno na spletni strani.

Število črvov neposrednega sporočanja narašča stalno, protivirusni programi pa še ne znajo direktno nadzirati prometa teh programov na strežniku. Težava je v stalnih spremembah aplikacij in v protokolu, ki ga uporabljajo. Prestreže ga šele program, ki teče na računalniku (Hindocha, 2003, str.13).

2.3.2. Omrežja botov

Izraz omrežja botov se nanaša na omrežje okuženih računalnikov, ki so oddaljeno nadzorovani in opravljani s strani zlonamernega uporabnika. Ne gre za nov koncept. Prva taka omrežja so se na črnem trgu pojavila že leta 2002. Število takih omrežij se veča proporcionalno s številom uporabnikov interneta, kot tudi s številom pomanjkljivosti, odkritih v Oknih.

Širitvi teh omrežij so botrovali trije dejavniki v lanskem letu:

1. Odkritje RPC DCOM pomanjkljivosti v Oknih 2000 in XP.
2. Črv elektronske pošte MyDoom je na okuženih računalnikih odpiral vrata v območju med 3127 in 3198, kar je omogočilo vsem dostop do računalnika. Posebna petbajtna kombinacija je omogočila dostop in mnogi so začeli uporabljati ta stranska vrata.
3. Kritična pomanjkljivost LSASS, katero je izkoriščal Sasser, je bil zadnji dejavnik, ki je pripomogel k razmahu omrežij botov.

Ocenjeno je, da se število računalnikov v teh omrežjih poveča vsak mesec za 300.000 do 350.000, skupno število pa je več milijonov. Vsi ti računalniki se uporabljajo za pošiljanje nezaželene elektronske pošte, napade zavrnitve storitve na spletne strani in pošiljanje novih trojanskih konjev.

2.3.3. Zlonamerni programi za mobilne telefone

Novo poglavje v zgodovini informacijske varnosti se je odprlo leta 2004. Pojavil se je prvi črv Cabir, katerega cilj so bili mobilni telefoni. Glede na razvoj telefonov, ki postajajo že kar mali prenosni računalniki, je bilo to mogoče pričakovati.

Koda Cabirja se je kmalu pojavila prosto dostopna na internetu. Posledica tega je bila, da se je pojavilo več programov, ki so imeli praktično enako kodo na različnih delih sveta. Originalnosti med pisci zlonamernih programov za mobilne telefone ni. Aktualni so novi tipi trojancev in križancev med virusi in črvi. Preneseni so iz računalniškega okolja na mobilne telefone.

Trenutno je bilo odkritih 5 zlonamernih programov, ki jih uvrščamo med trojance, dva črva in en hibrid med črvom in virusom. Vsi imajo v sebi del kode Cabirja, ki jim omogoča širjenje. Črv Comwar je bil napisan za širjenje preko MMSov. Na srečo je bil slabo napisan, drugače bi se lahko zelo hitro širil in prizadel tako telefone kot tudi stabilnost omrežja. Ti programi že povzročajo sive lase varnostnim strokovnjakom in upravljavcem mobilnih omrežij po celem svetu.

2.3.4. Novo obnašanje trojanskih konjev

Trojanski konji so začeli uporabljati virusni način okužbe, okužili so datoteke s svojo kodo v samem operacijskem sistemu. Med viruse jih ne moremo uvrstiti, saj se sami ne replicirajo.

Snemajoči trojanski konj Win32.agent.ns je primer takega ravnanja. Ko se je enkrat znašel na računalniku, je poleg snemanja drugih trojancev s spleta okužil tudi sistemsko datoteko wininet.dll. Vanjo je dodal svojo kodo. To datoteko nato kliče Internet Explorer vedno, ko deskamo po spletu.

Pojav opozarja na to, da je pomembno ne le pregledovanje novih datotek na disku, pač pa tudi starih. Zaradi prihranka na času se dostikrat pregleduje le nove datoteke, a kot vidimo, to ni dovolj. Poleg pregleda velikosti je pomembna tudi vsebina. To je naloga protivirusnih programov, nastavitev le-teh pa uporabnikova.

2.3.5. Politika in zlonamerni programi

Zlonamerni programi s politično noto niso novost, a so bili v letu 2005 posebej aktivni. V Evropi so se tega leta pojavili prvič. Najaktivnejša je bila družina črvov elektronske pošte Win32.Sober. Črvi te družine so bili znani že leto in pol poprej in več njihovih variant ima v sebi politično sporočilo. Tako je maja 2005 več milijonov uporabnikov elektronske pošte prejelo sporočilo s skrajno desničarsko propagando. Za pošiljanje sporočil so služili računalniki, okuženi z eno od variant črva Sober. Bilo je očitno, da je avtor to načrtoval. Kaže sicer, da je deloval na lastno pobudo, a podobne metode bi lahko v prihodnosti uporabljale tudi razne politične skupine.

V Aziji je prišlo že do pravih spletnih vojn. Spor med pakistanskimi in indijskimi hekerji je znan že dalj časa. Naslednji na tem področju so Kitajci, ki so svoje hekerje zaposlili v boju z Japonci. Kitajska vlada je ustanovila celo posebne šole, kjer se mladina kali za udiranje v računalniške sisteme in podobno. Tako so Kitajci napadli Japonske vladne strežnike. Na nekatere so vdrli, nekatere so sesuli. Kitajci pa se niso spravili le na Japonce, pred tem so se lotili tudi že Tajvana in Južne Koreje.

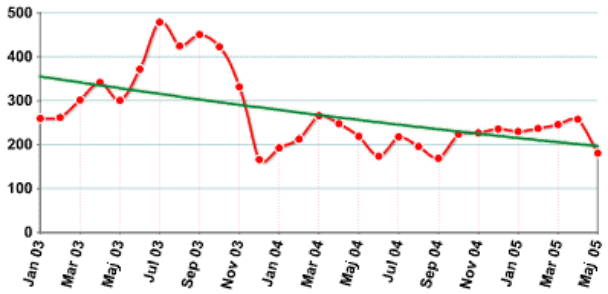
2.4. Današnji trendi

2.4.1. Virusi in črvi

Virusi in črvi so skupina zlonamernih programov, ki se sama replicira in jih zato na tem mestu obravnavam ločeno. Slika 3 na strani 21 prikazuje število novih primerkov, ki jih uvrščamo v to skupino. Kot lahko vidimo, se njihova skupna popularnost zmanjšuje, če gledamo celotno obdobje. Če se osredotočimo le na zadnje leto, pa vidimo, da je trend stabilen, okoli 200 novih se pojavi vsak mesec.

V Tabeli 3 na strani 21 je prikazana še podrobnejša razčlenitev, ki omogoča lažjo analizo. Če pogledamo številke, vidimo, da so beležile upad vse vrste v letu 2004 z izjemo internetnih črvov. Zadnji so pridobili tudi v letu 2005 glede na 2004. Skupaj s črvi elektronske pošte so v letu 2005 glede na 2004 prispevali k skupnem porastu črvov. Kategorija virusov pa vseskozi upada. Klasični virusi, prvotni zlonamerni programi, so že skoraj izginili. V primerjavi z drugimi vrstami zahtevajo več dela, njihova učinkovitost pa je manjša. Zato je upad popolnoma razumljiv.

Slika 3: Število na novo odkritih virusov in črvov od januarja 2003 do maja 2005



Vir: Mashevsky, 2005.

Glavna razloga za skupni upad črvov elektronske pošte gre iskati v prizadevanju proizvajalcev protivirusnih programov po hitri zaščiti in splošni osveščenosti uporabnikov. Prav tako so v podzemlju vedno bolj priljubljeni trojanci, ki se jih v nasprotju s črvi elektronske pošte lažje in hitreje razvije, poleg tega pa zasedejo manj prostora, kar omogoča hitrejši prenos.

Tabela 3: Stopnje rasti virusov in črvov v letu 2004 in 2005

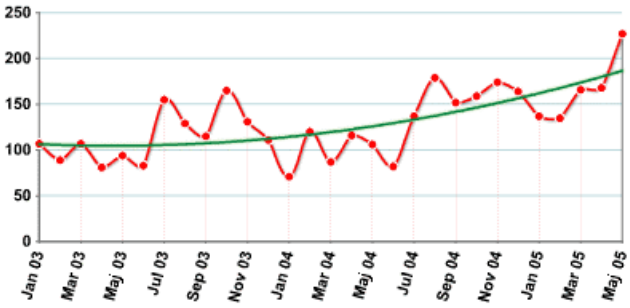
Vrsta	Rast v 2004 glede na 2003	Rast v 2005 glede na 2004
Črvi elektronske pošte	-20%	8%
Črvi takojšnih sporočilnikov	(v povprečju 1 na mesec)	(v povprečju 28 na mesec)
Črvi spletnega klepeta	-28%	-1%
Internetni črvi	21%	29%
Črvi omrežij za souporabo datotek	-50%	-36%
Črvi	-1%	24%
Virusi	-54%	-28%
Virusi in črvi skupaj	-37%	7%

Vir: Mashevsky, 2005.

2.4.2. Trojanski konji

Trojanski konji ali krajše trojanci vseskozi pridobivajo na popularnosti. Njihova rast se po mlačnem začetku v letu 2003 vseskozi stopnjuje in prekaša vse druge. V zadnjem letu so postali najbolj priljubljeno orožje napadalcev.

Slika 4: Število na novo odkritih trojanskih konjev od januarja 2003 do maja 2005



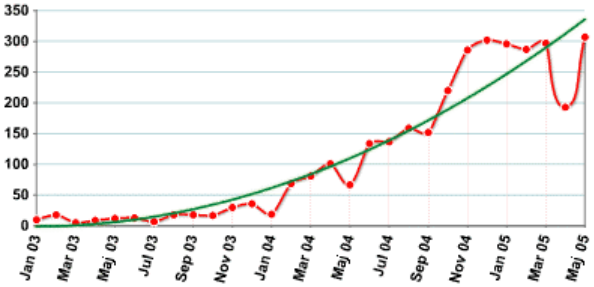
Vir: Mashevsky, 2005.

Priljubljenost trojanskih konjev se skriva tudi v finančnih motivih napadalcev. Včasih avtorji virusov niso imeli finančnih koristi od svojega dela, gnali so jih drugi cilji. Avtorji trojancev želijo biti plačani in tako je lahko razložiti, zakaj taka rast. Če pogledamo podrobneje, ugotovimo, da k rasti zelo prispevajo geselni, vohunski in snemajoči trojanski konji. Prvi dve skupini zbirata podatke, ki se jih da prodati. Tudi tretja omogoča finančne koristi, saj se z njihovo pomočjo na okuženem računalniku po lastni želji obnavljajo in nalagajo drugi zlonamerni programi. Širijo se večinoma preko elektronske pošte in spodrivajo črve elektronske pošte. So tudi razlog za upad slednjih.

2.4.3. Oglaševalni programi

Oglaševalni programi so nameščeni na računalnik z namenom oglaševanja izdelkov in storitev. Število teh programov je, glede na leto poprej, neverjetno naraslo v letu 2004, in sicer kar za 789 %. To kaže, kakšno zanimanje obstaja za navedene programe.

Slika 5: Število novih programov za oglaševanje od januarja 2003 do maja 2005



Vir: Mashevsky, 2005.

Potrebno je omeniti, da so oglaševalni programi legalni, zato jih ne moremo uvrstiti med zlonamerne programe. Mirno pa lahko rečemo, da hodijo po črti med legalnim in nelegalnim početjem in najbrž je le vprašanje časa, kdaj bodo postali nelegalni. V njih so že odkrili nekaj nelegalnih vsebin in početij. Na sodišču je več primerov, v katerih so proizvajalci oglaševalnih programov na zatožni klopi, zato jih tudi omenjam na tem mestu. Dan, ko bomo dodali novo kategorijo med zlonamerne programe, najbrž ni prav daleč.

3. Ocene škod

Že v prejšnjih poglavjih sem omenjal, da je pisanje zlonamernih programov vedno bolj povezano z denarjem. Avtorji želijo nekaj zaslužiti. Seveda gre za nelegalno pridobljeno premoženje, vendar se za svojim računalnikom doma počutijo varne pred policijo, kar jim daje pogum za vdore v računalnike. Seveda pa niso samo take vrste zlonamernih programov nevarne. Škodo v podjetju povzročijo tudi ostale oblike.

Škodo, povezano z zlonamernimi programi, je izredno težko oceniti. Še posebej s številkami. Nekaj podjetij se s tem vseeno ukvarja in njihov izsledke bom tudi predstavil. A na račun vseh objavljenih številk je moč slišati ogromno kritik. Primarni razlog za to je, da gre za ocene škod. Pri tem pa lahko vsak poda svojo oceno in jo zagovarja z argumenti. Analize podjetja Mi2g so citirane v mnogih časopisih, objavljene pa so bile tudi v ameriškem poročilu za kongres in v poročilu združenih narodov. V tabeli 4 na strani 25 vidimo, do kakšnih razlik prihaja pri ocenah dveh vodilnih podjetij na tem področju.

Razloga za pomanjkanje empiričnih podatkov sta predvsem dva:

1. podjetja nočejo razkriti vdora v svoj sistem,
2. podjetja sama ne morejo oceniti, koliko so dejansko bila oškodovana.

Dejavniki, zaradi katerih podjetja pogosto nočejo razkriti informacij o napadu, so posledica strahu pred različnimi posledicami takega razkritja (Cashell, 2004, str. 13):

- *Vpliv finančnih trgov*
  Javna oznanitev bi lahko pripeljala do padca cen delnic na borzi, lahko se spremeni njena tveganost, banke bi povišale premije za najemanje kreditov.

- *Ugled in zaupanje*
  Negativna publiciteta škoduje ugledu podjetja ali znamke in vodi v izgubo potrošnikovega zaupanja. Nedosegljivost spletne strani prek katere podjetje posluje

(npr. prodaja svoje izdelke), lahko vodi v izgubo nekaj že pridobljenih strank kot tudi nekaj potencialno novih.

- *Strah pred tožbo*
  Deležniki lahko zahtevajo povrnitev škode. Če vdor ni prvi, jih lahko obtožijo malomarnosti.
- *Strah pred odgovornostjo*
  Varovanje podatkov v podjetjih je zahtevano tudi v zakonu. Zlasti so občutljiva podjetja in organizacije, ki hranijo velike količine osebnih podatkov (ZZZS, ZPIZ, banke, zavarovalnice…)
- *Signal napadalcem*
  Javno priznanje opozori tudi ostale potencialne napadalce na ranljivost sistema. Hitro se lahko zgodi nov napada, še predenj podjetje vzpostavi boljšo zaščito.
- *Strah pred izgubo službe*
  Zaposleni v informatiki se bojijo za svojo službo in poskušajo prikriti napad pred svojimi nadrejenimi.

Nekaj od naštetih stroškov bi trpeli posamezniki, nekaj organizacija kot celota. Nastopili bi praktično takoj po razkritju informacij. Na drugi strani bi bili pozitivni učinki vidni, če bi nastali, šele po določenem obdobju. Koristi bi imela tudi konkurenca, tako da bi bili pozitivni učinki porazdeljeni med mnoge. Njihovo zadržanost torej lahko razumemo.

Čeprav so podjetja zadržana do razkrivanja takega tipa informacij, bi pričakovali, da jih merijo vsaj za interno uporabo. Take meritve bi jim pomagale opravičiti stroške za zaščito, vedeli bi, koliko je smiselno zapraviti. Vendar pa za tako meritev ni izdelanih modelov. Napadi lahko pripeljejo do več vrst stroškov in določene med njimi je zelo težko meriti, morda celo nemogoče.

Stroške napadov lahko razdelimo v dve kategoriji (Cashell, 2004, str. 15):

1. neposredne,
2. posredne.

Med neposredne stroške prištevamo:

- povrnitev sistema v prvotno stanje,
- izpad prihodka,
- manjšo produktivnost,
- zmanjšanje vrednosti ukradenih ali ogroženih informacij.

Čeprav gre za neposredne stroške, jih je težko meriti. Napad lahko pospeši že predvidene nadgradnje sistem in že smo v dilemi, kam to pripisati. Izpad prihodka lahko merimo na podlagi predhodnega obdobja, a lahko gre za enkraten efekt, če izgubimo stranko za vedno pa za dolgotrajen.

Med posredne stroške prištevamo:

- izgube ugleda podjetja,
- izgube ugleda znamke,
- stroške tožb,
- stroške zavarovanja,
- stroške financiranja.

Posredne stroške je izredno težko meriti. Seveda se v ekonomski teoriji že pojavljajo načini merjenja praktično vsega premoženja, tako številnega kot neštevnega. Podjetja potrebujejo informacije, na podlagi katerih lahko sprejemajo odločitve o poslovanju. Zato tudi poskušajo meriti bolj zapletene stroške in premoženje. Točnost dobljenih ugotovitev pa je stvar razprave.

Ocena škode, ki so jo v prejšnjem letu povzročili zlonamerni programi v svetovnem merilu, je med 169 in 204 milijardami dolarjev, kar je največ do sedaj. Po svetu je okoli 600 milijonov računalnikov z nameščenimi Okni, tako je povzročena škoda na računalnik med 281 in 340 dolarji (Jaques, 2005).

Tabela 4: Ocenjeni stroški napadov izbranih virusov in črvov med leti 1999 in 2003 v milijardah dolarjev

Napad	**Leto**	**Mi2g**	**CEI**
SoBig	2003	30,91	1,10
Slammer	2003	1,05	1,25
Klez	2002	14,89	0,75
BadTrans	2002	0,68	0,40
Bugbear	2002	2,70	0,50
Nimda	2001	0,68	1,50
Code Red	2001	2,62	2,75
Sir Cam	2001	2,27	1,25
Love Bug	2000	8,75	8,75
Melissa	1999	1,11	1,10

Vir: Cashell, 2004, str. 12.

Kako sta podjetji ocenili te številke? Mi2g kot vire navaja osebne stike z bankami, zavarovalnicami in pozavarovalnicami, spremljanje hekerskih elektronskih oglasnih desk in anonimne obveščevalce, člane hekerskih združb (SiPS, 2004, str. 1). Ekonomske informacije so zbrane iz različnih virov in ekstrapolirane na globalno raven z uporabo primernih algoritmov. Le-ti so ključ za številčne ocene. CEI (Computer Economics Inc.) zbira podatke s pomočjo svojih strank in drugih organizacij po svetu, anket o varnostnih praksah in stroških,

pregleduje statistična poročila in raziskave ter poročila o aktivnostih zlonamernih programov. Izdelali so metodo, s katero merijo stroške ponovne vzpostavitve prvotnega stanja, izgube produktivnosti in prihodka. Na podlagi tega potem ocenijo škodo za celotni svet (Cisco, 2002, str. 16).

V Tabeli 4 ni omenjen črv MyDoom, ki je povzročila za približno 38,5 milijard dolarjev škode do februarja 2004 (Mi2g, 2004). Prizadetih je bilo več kot 215 držav, med njimi najbolj (Sherriff, 2004):

1. ZDA med 12,2 in 15 milijardami dolarjev,
2. Velika Britanija med 10,3 in 12,7 milijardami dolarjev,
3. Francija med 1,5 in 1,9 milijardami dolarjev,
4. Kitajska med 1,4 in 1,7 milijardami dolarjev,
5. Avstralija med 1,2 in 1,5 milijardami dolarjev,
6. Kanada med 1,1 in 1,3 milijardami dolarjev,
7. Južna Koreja med 0,9 in 1,2 milijardami dolarjev,
8. Nemčija med 0,8 in 0,9 milijardami dolarjev,
9. Italija med 0,7 in 0,9 milijardami dolarjev,
10. Španija med 0,6 in 0,8 milijardami dolarjev.

V Sloveniji je nevarnost usmerjenih napadov nižja zaradi jezikovne prepreke. Vendar nam to ne sme dati lažnega občutka varnosti. Generalna policijska postaja je bila od začetka leta 1999 do konca leta 2003 obveščena o 92 vdorih. Škoda je s strani policije ocenjena na 46.385.000 tolarjev (Goljevšček, 2004, str. 44).

4. Celovita obramba pred zlonamernimi programi

Obramba mora biti sestavljena iz več komponent. Zlasti je pomembna zaščita v organizacijah. Organizacije so namreč tiste, ki najbolj občutijo posledice pomanjkljive zaščite. Skrbniki omrežja v organizaciji so v zelo zoprnem položaju. V primeru, ko dobro opravijo svoje delo, rezultati niso vidni. V nasprotnem primeru, ko je delo v organizaciji zaradi pomanjkljive varnosti oteženo, se to takoj opazi. Poleg tega ni nujno, da so samo oni odgovorni. Lahko je krivo vodstvo, ki ni dodelilo dovolj finančnih sredstev, lahko so krivi uporabniki.

Za učinkovito celovito zaščito v organizacijah je pomembno (Šuster, 2005):

- za vsakodnevno delo z računalnikom se ne sme uporabljati administratorskih privilegijev,
- stalno posodabljanje operacijskih sistemov in drugih programskih rešitev (popravki),

- nastavitve brskalnika,
- požarni zid,
- protivirusna zaščita,
- zaščita pred vohunskimi programi,
- izobraževanje uporabnikov.

Na kratko si poglejmo vsako izmed naštetih točk. Administratorski privilegiji omogočajo programom, ki so zagnani v tem profilu, da imajo dostop do prav vseh datotek na disku, tudi ključnih datotek operacijskega sistema. Zlonamerni program je v tem profilu bistveno bolj učinkovit, česar mi nočemo. Nujna je skrb za stalno posodabljanje operacijskega sistema in ostalih programskih rešitev, nameščenih na računalnik. Pisci zlonamernih programov zelo radi izkoriščajo znane ranljivosti. Pravilne nastavitve brskalnika onemogočajo samodejno izvajanje mobilne zlonamerne kode ali celo onemogočajo njeno izvajanje kljub privolitvi uporabnika. Tako zaščitimo uporabnike pred samim seboj. Požarni zid ločuje zunanje in notranje omrežje organizacije. Računalnike znotraj organizacije zaščiti pred napadi od zunaj. Protivirusna zaščita je najpomembnejša kategorija od vseh naštetih. Vedno zmogljivejši protivirusni programi neprestano bedijo nad početjem uporabnika za računalnikom. Tudi v primeru zagona zlonamernega programa dober protivirusni program prepreči okužbo in širitev. Zaščita pred vohunskimi programi je šele v povojih, a vedno bolj pridobiva na pomembnosti. Zasebnost je pomembna, še pomembnejše je varovanje podatkov v organizaciji. Z vidika stroškov in prijaznosti uporabe bi bilo najbolje, če bi bila protivirusna zaščita in zaščita pred vohunskimi programi združeni. A na žalost gre trenutno za dve ločeni področji. Zadnja točka je izobraževanje uporabnikov, saj previdni in skrbni uporabniki lahko preprečijo marsikatero okužbo. Osnova za previdnost in skrbnost je znanje o škodljivosti, nevarnosti in posledicah okužbe z zlonamernimi programi.

4.1. Protivirusna zaščita

Protivirusna zaščita pravzaprav pomeni zaščito pred vsemi zlonamernimi programi. Vedeti moramo, da je virus in protivirusni program generično ime, ker je bil virus in obramba pred njim prva. Podobno kot je generično ime za mobilni telefon mobitel. Do sedaj sem se v svoji diplomski nalogi izogibal generični uporabi imena virus, v tem poglavju pa se ne morem, ker bi nastala zmešnjava. Vsi proizvajalci namreč navajajo, da ponujajo protivirusno zaščito.

Od vseh naštetih kategorij za celovito zaščito je protivirusna zaščita daleč najpomembnejša. V današnjem času je postala že pravzaprav samoumevna, kar za ostale kategorije ne morem reči. Zato ji bom v nadaljevanju posvetil največ pozornosti.

Ustrezno zaščito potrebujejo tako podjetja z dvoslojno kot z troslojno (večslojno) zasnovo informacijske arhitekture. Troslojna arhitektura temelji na osrednjih strežnikih in skupinah

strokovnjakov, ki zagotavljajo njihovo razpoložljivost. Skrbništvo in vzdrževanje programov se izvaja na enem mestu (Kovačič, 2004, str. 37). Zaščita pred zlonamernimi programi je v tem primeru še pomembnejša.

4.1.1. Izbira programa

Ponudba na področju protivirusnih programov je vedno bogatejša. Izbira ustreznega programa za podjetje ali organizacijo je tako vedno zahtevnejša. V nadaljevanju bom predstavil kriterije, ki olajšajo izbiro.

V tabeli 5 sem povzel prednosti in slabosti najbolj znanih protivirusnih programov in njihove cene. Zaradi različnih strategij prodaje sem lahko primerjavo naredil le tako, da sem si izbral skupno časovno enoto in število licenc. Tako je časovno obdobje veljavnosti licence eno leto in je upoštevan prvi nakup. Večina podjetij ponuja popust na količino nakupljenih licenc in na zakup za daljše časovno obdobje. Pri nekaterih podatkov ni bilo možno dobiti, saj cen ne objavljajo, pogajajo se z vsakim kupcem posebej. V Prilogi 1 so nazorno prikazani tudi rezultati testa na protivirusnih programih. Kaj testirajo bom opisal v nadaljevanju.

4.1.1.1. Odkrivanje

Najpomembnejša funkcija protivirusnega programa je seveda odkrivanje virusov. Toda kako ugotoviti ali program dejansko deluje tako, kot se je oglaševalo? To odpre dve podvprašanji (Castelli, 2002, str. 4):

1. Koliko virusov program dejansko prepozna?
2. Pod kakšnimi pogoji program opazi virus? Jih prepozna če pridejo preko omrežja, elektronske pošte ali če so že v spominu računalnika?

Lahko bi se lotili testiranja programov sami, vendar je število programov že zelo veliko, poleg tega gre za tvegano početje. Ugotovitev, da je program neučinkovit, bi nas lahko drago stala – imeli bi okužen računalnik. Razen če bi ustvarili pogoje za varno testiranje – drago in zamudno. Na srečo obstajajo organizacije, ki se ukvarjajo s testiranjem protivirusnih programov in svoje rezultate objavljajo na spletu. Dostop do njih je brezplačen.

- Virus Bulletin podeljuje logo 100 % izdelkom, ki prestanejo njihov test. Sestavljen je iz testa na zahtevo in v realnem času. Za pridobitev loga mora odkriti vse viruse, ki se trenutno pojavljajo in okužujejo računalnike po svetu (Virus Bulletin, 2005). Rezultate testa si lahko ogledate prilogi 1.

- Laboratorij West Coast ponuja dva nivoja kontrolnih potrditev za protivirusne programe. Proizvajalci morajo za teste svojih izdelkov plačati. Prvi nivo uspešno prestanejo vsi tisti programi, ki odkrijejo vse viruse, ki se pojavljajo. Za drugi novi pa poleg uspešno opravljenega prvega nivoja zahtevajo tudi, da je sposoben popraviti spremembe na sistemu, ki so posledica okužbe. To mora storiti brez vpliva na stabilnost računalnika. V test so vključeni le tisti virusi, ki jih je teoretično mogoče tako odstraniti (West Coast Labs, 2005).

- ICSA (mednarodno računalniško varnostno združenje) prav tako testira izdelke proti plačilu izdelovalca. Za pridobitev njihovega certifikata mora protivirusni program prav tako odkriti vse viruse, ki se pojavljajo po svetu, poleg tega pa še vse, ki so zajeti v kolekciji združenja (Cybertrust, 2005).

4.1.1.2. Tehnologija

Pomembno je vedeti, kakšna tehnologija je vključena v proizvod. Tehnološko dovršen program bo omogočal dobro zaščito. Protivirusni program zazna večino potencialnih groženj na podlagi baze virusnih definicij. A ne vse, odkrivati jih poskušajo tudi na podlagi algoritmov za pregledovanje kode v datotekah. Protivirusni programi vseskozi preverjajo datoteke v uporabi, na začetku, ko do njih dostopamo. Želja po čim manjši obremenitvi računalnika izključuje možnost stalnega preverjanja vseh datotek. Poglejmo si podrobno, kaj vse mora imeti dober protivirusni program (Castelli, 2002, str. 5-6):

- *Protivirusni program mora biti združljiv z operacijskim sistemom*
  Paziti moramo kateri verziji operacijskega sistema je protivirusni program namenjen. Lahko se nam zgodi, da ne bo delal na starih verzijah, prav tako so pogosto ločene verzije za strežnike in delovne postaje.

- *Odkrivanje v realnem času in na dostop*
  Nujna sestavina sodobnega protivirusnega programa je sposobnost pregledovanja v realnem času in na dostop. To omogoča prestrezanje virusov takoj ob poskusu okužbe. Pregledovati mora vse možne tarče okužbe.

- *Odkrivanje na zahtevo*
  Zagotavlja neokuženost vseh datotek na disku. Vedno ga je pametno pognati po posodobitvi protivirusnega programa. Tako najdemo tudi najnovejše grožnje.

- *Hevrističnost*
  Hevristična tehnologija omogoča zaščito pred osnovnimi neznanimi virusi. Tako lahko prestreže nekatere viruse, ki so se ravnokar pojavili, čeprav jih nima v svoji bazi virusnih definicij.

- *Sposobnost pregledovanja vseh datotek*
  Včasih so virusi pregledovali le specifične vrste datotek, saj drugih virusi niso okuževali. Za tako zastarelo tehnologijo danes ni več prostora. Pomembno je pregledovanje prav vseh možnih datotek.

- *Blokiranje ukaznih datotek*
  Sposobnost blokiranja virusov, ki temeljijo na ukaznih datotekah.

- *Sposobnost pregledovanja priponk elektronske pošte*
  Nekateri virusi so se sposobni širiti preko priponk elektronske pošte ne da bi kdo odprl priponko.

- *Sposobnost pregledovanja stisnjenih datotek*
  Virus se ne more pognati v stisnjenem stanju, a vseeno je ta funkcija pomembna. Virusi so tako prestreženi preden se jim je ponudila možnost delovanja.

4.1.1.3. Vzdrževanje

Vse protivirusne programe je potrebno vzdrževati. Pomembno je, da je to čim bolj enostavno, tako da ne vzame veliko časa skrbnikom omrežja in uporabnikom za računalniki. To je kategorija, ki lahko doprinese k večji učinkovitosti v organizaciji, če ne ovira vsakodnevnega dela. Avtomatizirano posodabljanje definicij in protivirusnega programa v ozadju, brez kakršnihkoli obvestil uporabniku je najboljša rešitev.

- *Posodabljanje virusnih označb*
  Posodabljanje mora biti čim bolj pogosto, standard danes je enkrat na teden, nekateri pa izdajajo označbe celo dnevno. Posodabljanje mora biti samodejno, ročno posodabljanje je stvar preteklosti. Posodobitve morajo biti v majhnih datotekah. Uporabna je tudi funkcija posodabljanja delovnih postaj preko strežnika lociranega v podjetju, le-ta pa dobi posodobitve na strežniku proizvajalca.

- *Posodabljanje protivirusnega programa*
  Posodobitev samega protivirusnega programa mora biti čim lažja. Zahteva po odstranitvi stare verzije, preden se namesti novo, ne bi smela biti prisotna. Zahteva po ponovnem zagonu računalnika tudi ni zaželena, še posebno, če gre za strežnik.

4.1.1.4. Zmogljivost

Protivirusni program bo imel vedno vpliv na hitrost delovanja računalnika. Računalnik se počasneje zažene, zaseda pomnilnik in obremenjuje procesor. Mislim da ni potrebno posebej poudarjati, da je naša želja izbrati program, ki ima dobro optimizirano kodo in zahteva malo

sistemskih sredstev. Testiranja se lahko lotimo sami, vendar podobno kot pri prvi točki zahteva to veliko časa in posledično denarja. Žal ne obstaja neodvisna organizacija, ki bi preverjala to lastnost protivirusnih programov, a vedno se najdejo testi v računalniških revijah in spletnih straneh z ustrezno vsebino. Ni tako pregledno in reprezentativno, vseeno pa bomo dobili nekaj informacij za lažjo odločitev.

4.1.1.5. Prilagodljivost

Pomembna lastnost protivirusnega programa za podjetja je njegova prilagodljivost. Centralna prilagodljivost je zelo zaželena, saj omogoča hitro posodabljanje. Olajšano je uveljavljanje novih pravil in pregledovanje obvestil.

- *Večnivojska podpora*
  Podpora proizvajalca je pomembna in zaželena. Usklajena mora biti z potrebami podjetja. V kritičnih situacijah je pomembno hitro in pravilno ukrepanje in v takih primerih je podpora strokovnjakov bistvena.

- *Spletna podpora*
  Spletna podpora v obliki spletnih strani, kjer so zbrane informacije in kjer se lahko posreduje vprašanja je že standardna. Razlika je v njihovi preglednosti in ažurnosti. Vam bo proizvajalec odgovoril, če mu pošljete primer sumljive datoteke?

- *Opozorila*
  Opozorila proizvajalca, ob pojavu novo odkritega virusa in navodili za zaščito, lahko pomenijo razliko med preprečevanjem in zdravljenjem. Obvestilo, preden so na voljo nove virusne označbe, pomaga pri preventivnih ukrepih.

4.1.1.6. Ranljivost proizvoda

Implementacija novega programa v korporativno okolje ne sme odpreti novih varnostnih lukenj. Spisek najdenih pomanjkljivosti objavlja Security Focus. Tako lahko izberemo najpopolnejši program, sprotno spremljanje pa nam omogoča miren spanec.

4.1.1.7. Zanesljivost proizvajalca

Izbira novega poslovnega partnerja mora biti vedno preudarna. V večjih organizacijah in sodelovanju skozi daljše časovno obdobje je izbira zanesljivega ponudnika proizvoda in storitev bistvenega pomena. Kako dolgo je proizvajalec na trgu, njegov tržni delež in velikost podjetja. Tako bomo izbrali nekoga, katerega produkt bomo uporabljali več kot eno leto, za kolikor dolgo veljajo licence.

Tabela 5: Pregled prednosti, slabosti in cen protivirusnih programov po proizvajalcih

IME PROIZVAJALCA (PROIZVODA)	PREDNOSTI	SLABOSTI	CENA	
			WIN XP	WIN 2003
Alwil (Avast!)	• zelo majhne posodobitve • posodobitve na pobudo Alwilovega strežnika, ne po intervalih (bolj ažurno) • majhna poraba pomnilnika • zelo visoka stopnja nastavljivosti / prilagodljivosti • zadovoljiva splošna detekcija z močno detekcijo trojancev (generično zaznavanje) • odlična brezplačna tehnična podpora • zvočna opozorila	• vsi ne marajo preoblek • nekaterim se zdi grafični vmesnik neurejen • začetniki se znajo zgubiti v nastavitvah	47,54$	399$
Computer Associates (InoculateIT/eTrust)	• majhne posodobitve • dva pregledovalna motorja • nizka poraba sredstev • zelo dobro odkrivanje	• na trenutke zmeden in grd uporabniški vmesnik	38$	865$
Doctor Web (DialogueScience)	• močna detekcija in hevristika • zelo lahek za sistem in hiter • preprost in učinkovit uporabniški vmesnik	• tehnična podpora ne odgovarja vedno	33,84$	33,84$
Eset (NOD32)	• preprost in učinkovit uporabniški vmesnik • dokaj visoka stopnja nastavljivosti • zelo visoka hitrost pregledovanja • zelo močna hevristika • majhne posodobitve	• detekcija trojancev je precej slaba • IMON HTTP pregledovalni modul povzroča precej težav pri brskanju po spletu • precej lažnih alarmov na račun močne hevristike	50,82$	64,31$
F-Secure	• zelo enostaven, pregleden in učinkovit uporabniški vmesnik • zelo visoka stopnja odkrivanja (ena najboljših) • hitre in majhne posodobitve • trije simultani pregledovalni motorji	• dokaj visoka poraba sredstev • hitrost • najdražji protivirusni program na trgu	88,55$	NP

Nadaljevanje Tabele 5: Pregled prednosti, slabosti in cen protivirusnih programov po proizvajalcih

IME PROIZVAJALCA (PROIZVODA)	PREDNOSTI	SLABOSTI	CENA	
			WIN XP	WIN 2003
Frisk (F-Prot)	• zelo lahek za sistem (porabi najmanj sredstev od vseh) • hitrost • majhne posodobitve • dobro odkrivanje	• nima pregledovalnika elektronske pošte (ne pregleduje dospele pošte dokler je ne odpremo)	50$	50$
Grisoft (AVG)	• nizka poraba sredstev • enostaven in učinkovit vmesnik • zelo dobro odkrivanje klicateljev	• ne najboljše splošno prepoznavanje	20,48$	NP
H+BEDV (AntiVir)	• dokaj nepotraten za sistem • zadovoljiva hevristika • visoka nastavljivost • dobro splošno odkrivanje	• nekaterim ne bo všeč grd vmesnik • velike posodobitve definicij (običajno okoli 1,5 MB) • velike posodobitve jedra • nerodno posodabljanje definicij in jedra • zelo počasni strežniki za posodobitve	72,56$	57,06$ (najmanj 10 licenc)
Kaspersky	• zelo visoka stopnja odkrivanja (ena najboljših) • majhne posodobitve • redne (hitre) posodobitve (na vsake 3 ure) • visoko odkrivanje trojancev • dobra Win32 in makro hevristika	• zmeden uporabniški vmesnik • srednja do visoka poraba sredstev • uporablja NTFS ADS označevanje datotek (lahko povzroča spore z drugimi programi)	36,33$	NP
McAfee Inc. (prej Network Associates)	• zelo visoka stopnja odkrivanja (ena najboljših) • zelo močna hevristika na vseh področjih • lep in enostaven vmesnik • preprost in učinkovit za začetnike • dobro odkrivanje trojancev	• resna omejenost nadzora / nastavitev • odzivnost opozorilnega okna • obupno ročno posodabljanje • dokaj visoka poraba sredstev • definicije izdajajo tedensko • za delovanje vmesnika zahteva omogočene kontrolnike ActiveX • McAfee Security Center pokvari splošni vtis (je neuporaben in nadležen dodatek)	59,99$	NP

Nadaljevanje Tabele 5: Pregled prednosti, slabosti in cen protivirusnih programov po proizvajalcih

IME PROIZVAJALCA (PROIZVODA)	PREDNOSTI	SLABOSTI	CENA	
			WIN XP	WIN 2003
Norman	• nizka poraba sredstev • odkrivanje • SandBox hevristika • majhne posodobitve	• rahlo zmeden in včasih grd vmesnik • občasno počasno pregledovanje Win32 datotek zaradi SandBox-a	39,35$	66,41$
Panda Software	• dobro odkrivanje • lep in pregleden uporabniški vmesnik • zvočna opozorila • nova TruPrevent hevristika	• precej hroščev • visoka poraba sredstev • za delovanje porabi veliko procesorske moči	55,28$	162,21$
Softwin (BitDefender)	• zelo dobro odkrivanje (eno boljših) • odzivnost protivirusne ekipe • zelo pregleden in enostaven vmesnik • ščiti lastne in sistemske registrske vnose (zagon) • dobra tehnična podpora • majhne in redne posodobitve (večkrat dnevno)	• dokaj visoka poraba sredstev • včasih zelo počasen • združljivostne težave	36,65$	NP
Symantec (Norton)	• lep in pregleden vmesnik • enostavnost • dokaj nizka poraba sredstev • blokiranje črvov (mini požarni zid)	• redke posodobitve virusnih definicij (podobno kot pri McAfee) • za delovanje vmesnika zahteva omogočene kontrolnike ActiveX • ni tehnične podpore • za delovanje uporablja veliko procesov	NP	NP
Trend Micro (PC-cillin)	• lep in pregleden vmesnik • dobro odkrivanje • dobro generično odkrivanje trojancev • redne posodobitve • blokiranje omrežja (preprečuje širjenje okužb po lokalnem omrežju) • osnovni požarni zid	• slaba odzivnost pregledovanja v realnem času • ne najnižja poraba sredstev • za delovanje porabi veliko procesorske moči	72,56$	NP

Vir: Računalniške novice, spletne strani izdelovalcev protivirusnih programov, lastna izdelava, 2005.

4.1.1.8. Pregled prednosti in slabosti protivirusnih programov

V tabeli 5 na strani 32 so nazorno prikazane glavne prednosti in slabosti posameznih protivirusnih programov. Glede na predstavljene kriterije za izbor najbolj primernega programa za posamezno organizacijo sem poudaril glavne karakteristike posameznega programa, zaradi katere izstopa iz množice. Seveda so posamezne zaščite dražje od drugih in je dobro, da lahko prednosti tehtamo tudi relativno na ceno. Tako sem navedel tudi cene, ki jih podajajo proizvajalci na svojih spletnih straneh.

Vsi navedeni protivirusni programi so, kot se vidi tudi v prilogi 1, prestali test s strani Virus Bulletina. To je zagotovilo, da gre za zelo dobre programe. Vseeno velja, da so nekateri še malo boljši pri odkrivanju kot ostali (Kaspersky, McAfee, F-Secure). Kar nekaj se jih lahko pohvali z majhno porabo sredstev (Avast!, F-Prot, AVG, Norman, Norton). Pri hitrosti pregledovanja je najurnejši NOD32.

Na podlagi slabosti se lahko nekatere programe zelo hitro izloči, če nas navedene pomanjkljivosti motijo. Uporabniški vmesniki so v okenskem okolju pomembni, zato je zaželeno, da je le-ta čim lepši in preglednejši. V primeru, ko navadni uporabniki nimajo stika z njim, se da to pomanjkljivost zanemariti. Zelo velika zamera gre produktu Norton proizvajalca Symantec, saj za svoje delovanje potrebuje vključene kontrolnike ActiveX. Le-te se pogosto izključujejo za povečanje varnosti. Hroščatega programa prav tako nihče noče in Panda mora najprej izboljšati to področje. Nekatere programe se lahko izloči zaradi porabe sistemskih sredstev. V primeru, ko je v organizaciji veliko starih računalnikov, jih ne sme dodatno obremenjevati še protivirusni program.

4.2. Zaščita pred vohunskimi programi

Vohunski programi so tehnika prikritega zbiranja informacij na računalnika. Ti podatki so nato prodani zainteresiranim strankam. Zbrane informacije so različne. Nekateri zbirajo samo podatke o vrsti operacijskega sistema, ki je nameščen, ali kakšna je zmogljivost internetne povezave. Drugi zbirajo osebne podatke – beležijo obnašanje uporabnika na spletnih straneh (katere obiskuje, kako pogosto), lahko celo pregledujejo datoteke s informacijami osebnega značaja (Ropelato, 2005).

Omenil sem že, da protivirusna zaščita pravzaprav pomeni zaščito pred zlonamernimi programi. Pravzaprav gre za pravni vidik, saj protivirusni programi nudijo zaščito pred nelegalnimi programi, medtem ko imamo v tej skupini programe, ki so največkrat legalni. Seveda ne vsi in področja delovanja protivirusnega in protivohunskega programa se dostikrat pokrivajo. Vsekakor pa eden drugega ne nadomeščata.

Tabela 6: Primerjava programov za zaščito pred vohunskimi programi

Mesto	1	2	3	4	5	6	7	8	9	10
Cena *(cena za eno leto)	$29.99*	$19.95*	$29.95*	$29.95	$29.99	$29.95	$29.95	$41.91	$39.95	$39.99
Skupna ocena										
Ocene										
Nabor funkcij										
Učinkovitost										
Preprostost uporabe										
Prilagodljivost										
Preprostost uporabe										
Podpora										
Funkcije										
Število iskanih elementov	36,000	NP	*53,248	37,691	22,984	23,675	NP	36,254	NP	NP
Sposobnost restavriranja	✓	✓	✓	✓				✓	✓	✓
Označi resnost grožnje	✓	✓	✓	✓	✓	✓		✓		
Opisi najdenih vohunskih programov	✓	✓	✓	✓	✓	✓	✓	✓		
Planiranje preverjanja	✓	✓	✓	✓	✓	✓	✓			✓
Avtomatsko posodabljanje	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Blokiranje seldilnih piškotov	✓	✓	✓		✓	✓	✓		✓	
Blokiranje in zaščita v realnem času	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Preverja izmenljive enote	✓	✓	✓	✓	✓			✓		
Sposobnost odkrivanja in izbrisa										
Oglaševalni programi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vohunski programi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sledilci pritiskov tipk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Trojanski konji	✓	✓	✓	✓	✓	✓	✓	✓		
ActiveX kontrole	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Klicatelji	✓	✓	✓	✓	✓	✓	✓	✓		
Izkopavanje podatkov	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Paraziti	✓	✓	✓	✓	✓	✓		✓		
Orodne vrstice	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Snemanje mimogrede	✓	✓	✓	✓	✓	✓	✓	✓		
Sledilni piškoti	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Vhose vohunskih programov v registru	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ugrabitve brskalnikov	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tehnična pomoč, ki je na voljo										
Brezplačen telefon	✓	✓	✓							✓
Vgrajena pomoč	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Baza znanja	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Forum / Elektronska pošta	✓	✓	✓	✓		✓	✓	✓	✓	✓
Nalinijski klepet					✓					✓
Podprti operacijski sistemi										
XP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2000	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
98	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
95				✓		✓		✓	✓	
NT	✓		✓	✓	✓		✓		✓	
ME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Vir: Anti-Spyware software review, 2005.

Izbor programa za zaščito pred vohunskimi programi je podvržen istim kriterijem, kot izbor protivirusnega programa. Problem nastane, ker so praktični vsi produkti na trgu malo časa. Izbor je tako zelo zahteven, a na srečo ne tako kritičen. Prisotnost vohunskega programa je sicer moteča, a na srečo dela ne onemogoča, poleg tega ne ogroža drugih. Tudi ponudniki programov za zaščito so usmerjeni bolj na zaščito delovnih postaj kot strežnikov. Uvedba takih programov v korporativno okolje je bistveno zahtevnejša od uvedbe protivirusne zaščite.

Med vohunske programe uvrščamo tudi tiste trojanske konje, ki v svoji funkciji zbirajo podatke. Ti so nelegalni, protivirusni programi jih prestrezajo. To je že eno od področij, kjer se bosta izbrana programa pokrivala.

Svoj program za zaščito pred vohunskimi programi je izdal tudi Microsoft. Trenutno je še v testni fazi, a odločitev giganta nakazuje na to, da postaja to pomembno področje, tudi s finančnega vidika. Trenutno je še zastonj, a ko bo izdana končna verzija in bo na voljo tudi poslovnim sistemom, bo skoraj zagotovo plačljiv.

V tabeli 6 na strani 36 so zbrani podatki o trenutno najboljših protivohunskih programih, skupaj s funkcijami in ceno. Za najboljši program na testu se je izkazal Spyware Eliminator. Pri Spy Sweeperju je potrebno upoštevati, da v številu iskanih elementov zajema tudi piškotke, ki jih ostali programi ne upoštevajo pri skupni številki iskanih elementov.

4.3. Izobraževanje uporabnikov

Izobraževanje uporabnikov je pomembno, saj veliko zlonamernih programov cilja na naivnost le-teh. Oboroženi z znanjem lahko med elektronskimi sporočili ločijo resnična in zlonamerna. Zavedati se morajo tudi tveganosti prinašanja različnih podatkovnih nosilcev med računalniki. Doma imajo običajno slabše zaščitene računalnike. Lahko so okuženi in tega niti ne vedo, potem to prenesejo še na delovno mesto. Kot smo videli v zgodovinskem pregledu, je bilo kar nekaj izbruhov posledica neznanja.

Težko je opredeliti nek nivo, ki bi ga moral vsak dosegati. Računalnik je za večino pripomoček za učinkovitejše delo in podrobno znanje o njegovem delovanju ni potrebno. Prepoznavanje zlonamernih programov že sodi v deteljno znanje. Vseeno je z vidika učinkovitosti organizacije potrebno, drugače lahko zastane celotni poslovni sistem. Odkriti je potrebno pravo mero, da ne zbudimo nasprotovanja in dosežemo cilj - to je povečanje varnosti.

4.4. Požarni zid

Požarni zid je sestavni del vsakega malo večjega omrežja v podjetju. Ločuje notranje in zunanje omrežje. Bistvo požarnega zidu je v zagotavljanju varnosti med dvema omrežjema. Požarni zid glede na določena pravila dovoli ali zavrne tok podatkov preko njega. Do odprtega dela lahko dostopa vsak. Za zavarovane dele je potrebno geslo (Swire, 2001, str. 9).

Med naprednejše funkcije požarnega zidu spadajo (Wikipedija, 2005):

- Preslikava (zasebnih) omrežnih naslovov (angl. oznaka NAT), ki omogoča skupno rabo internetne povezave.
- Demilitarizirana cona (angl. oznaka DMZ), ki omogoča ločen priklop bolj izpostavljenih naprav.
- Kontekstno odvisni nadzor dostopa, ki na podlagi protokolov dinamično dovoli dostop do storitev.
- Nudijo kodirane tunelske povezave in tako omogočajo navidezna privatna omrežja (angl. oznaka VPN).

Poznamo dve vrsti požarnih zidov:

- strojne,
- programske.

Strojni požarni zid ima veliko večjo zmogljivost in visoko ceno. Primeren je za večje poslovne organizacije. Prednost strojnega je pogosto v hitrosti, saj so normalno strojne rešitve precej hitrejše in tako omogočajo večjo prepustnost. Seveda imamo tudi tu visok razpon v ceni. Obstajajo ceneni požarni zidovi, ki pa so primerni samo za domačo rabo. Pogosto povzročajo težave, še posebej če imamo vzpostavljenih veliko povezav. Prednost programskih požarnih zidov je običajno v enostavnejši uporabi, predvsem pa je razlika v ceni. Za domačo uporabo obstajajo tudi brezplačni požarni zidovi.

4.5. Popravki

Brez nameščenih najnovejših popravkov je računalnik še posebej ranljiv. Že večkrat v tekstu sem omenil, da pisci zlonamernih programov zelo radi izkoriščajo pomanjkljivosti programov. Zadnji Microsoftov operacijski sistem Windows XP so z zadnjimi popravki zelo pridobila na varnosti. Preden se program prenese s spleta, dobimo opozorilo. Prav tako dobimo opozorilo pred odprtjem. Privzeti nivo varnosti je povečan.

4.6. Nastavitev brskalnika

Ameriška nacionalna varnostna agencija je objavila zelo obsežen članek o nastavitvah Internet Explorerja. Ta brskalnik je vključen v Microsoftova Okna, zato ga uporablja večina uporabnikov za svoje delo. Povzetek bistvenih ugotovitev bi bil, da je potrebno izklopiti večino funkcij, ki omogočajo zaganjanje in nameščanje mobilne zlonamerne kode (Doernberg, 2002).

4.7. Neuporaba administratorskih privilegijev

Novejši operacijski sistemi poznajo več načinov dela na sistemu. Vsak je namenjen določenemu profilu uporabnika glede na naravo njegovega dela. Pomembna sta dva:

- administrator (skrbnik),
- uporabnik.

Administrator ima popoln nadzor nad sistemom in dostop do vseh datotek, ne glede na to, kako pomembne so. Lahko jih namešča, briše, spreminja. V tem profilu zagnani programi imajo prav tako neomejen dostop. Iz tega sledi, da lahko zlonamerni programi posežejo kamorkoli v sistem. To jim močno olajša delo. Uporabniški profil ima le toliko pravic, kolikor jih uporabnik potrebuje za vsakdanje delo.

4.8. Stroški zaščite

Navodila za celovito zaščito organizacije sem že podal. Večkrat sem omenil, da je težko prepričati vodstvo v smiselnost nakupa. Podjetja običajno delimo na mala in velika glede na število zaposlenih ali po kakšnem od numeričnih kazalcev, sam pa jih bom razdelil glede na to, ali imajo zaposlene skrbnike omrežij ali ne. Ali imajo svojo službo za informatiko? V malih podjetjih jih običajno nimajo, saj nimajo dovolj računalnikov, da bi lahko opravičili stroške. Najete imajo zunanje sodelavce ali podjetja, ki skrbijo za omrežno opremo in računalnike. Predstavil bom, kako v malem podjetju sledijo 7 točkam za celovito zaščito in kako v velikem. Poleg tega bom ocenil še stroške.

4.8.1. Malo podjetje

Za primer malega podjetja bom vzel podjetje, ki ima 20 računalnikov in se ukvarja s storitveno dejavnostjo. Imajo predstavitveno spletno stran, ki je naložena na strežniku enega

od ponudnikov interneta v Sloveniji. Za dostop do interneta uporabljajo ADSL povezavo. Kako sledijo nasvetom za celovito zaščito.

Prvi točki, to je neuporaba administratorskih privilegijev, ne sledijo. V primeru, ko imajo boljše računalnike z nameščenimi Windowsi XP ali 2000, so uporabniki hkrati tudi administratorji na svojem računalniku. Klicati zunanjega vzdrževalca bi bilo precej zamudno in drago. Podjetje nima pavšalnega vzdrževanja opreme, izvajalca plačuje po opravljenih urah. En obisk tako stane približno 10.000 SIT (Računovodja.com, 2005), če gre za lažje opravilo, ki vzame približno 1 uro. Vseeno bi bilo priporočljivo, da uporabljajo za vsakdanje delo uporabniški profil. V primeru, ko je potrebno na računalnik kaj namestiti, pa se prijavijo v administratorski profil.

Stalno posodabljanje operacijskih sistemov je bolj izjema kot pravilo. Nameščanje posodobitev je enostavno, saj so tako ali tako prijavljeni kot administratorji. Tudi če ne bi bili, nameščanje popravkov ne vzame veliko časa, če to počnemo redno. Poleg tega lahko sprožimo posodobitev ob odhodu z dela in zjutraj, ko se vrnemo, je vse končano.

Nastavitve brskalnika so ostale privzete, take kot so bile ob namestitvi. Namestitev operacijskega sistema na delovno postajo nas bo stala 9.400 SIT (Računovodja.com, 2005). Toliko stane gola namestitev, nastavitve bodo ostale privzete. Izvajalec ne more vedeti, kakšen nivo varnosti je najbolje nastaviti z vidika podjetja, saj ne ve, kaj vse bodo uporabljali. Da bi to ugotovil, bi porabil več časa, kar bi računal podjetju. Tako vsaj ena stran običajno ni pripravljena sprejeti dodatnih stroškov.

V požarni zid kot samostojno komponento omrežja mala podjetja niso pripravljena vlagati. Običajno je preprost požarni zid vgrajen v usmernik. Če je pravilno nastavljen, tudi zadostuje potrebam podjetja. Sprejemljive rešitve za podjetja se začnejo pri ceni 30.000 SIT.

Protivirusna zaščita je edina, ki je praviloma vedno prisotna tudi na računalnikih v malih podjetjih. Glede na to, da so grožnjah veliko govori po sredstvih javnega obveščanja, vsi poznajo pomembnost protivirusne zaščite. Problem je le, da to ni dovolj, česar se ne zavedajo. Najcenejša zaščita bo podjetje stala od 350 USD naprej v enem letu.

Na drugi strani je zaščita pred vohunskimi programi popolnoma zapostavljena. Glede na to, da povprečnemu uporabniku razlika ni jasna, je to razumljivo. Kot sem že omenil, ta kategorija programov ni tako nevarna za delovanje podjetja, a zna vseeno povzročiti nekaj sivih las. Malim podjetjem bi priporočil, da si kupijo eno verzijo programa, kar jih bo stalo približno 30 USD. To verzijo potem namestijo na računalnik vsake toliko časa, ga pregledajo in potem zbrišejo. To ponovijo na vseh računalnikih.

Osnovni nivo poznavanja zlonamernih programov je v malih podjetjih zelo priporočljiv. Glede na to, da bodo za zaščito večinoma skrbeli sami, je to praktično nujno, ali pa bodo prej

ali slej naleteli na težave z zlonamernimi programi. Priporočljivo bi bilo, da se eden v podjetju izobrazi v tej smeri in potem pomaga in svetuje tudi ostalim.

4.8.2. Veliko podjetje

Zaščita v velikem podjetju je bistveno večjega pomena kot v manjšem podjetju. Zadnje se lahko še znajde tudi brez računalnikov, le bolj zamudno bo vse skupaj, večja podjetja pa imajo svoje poslovanje popolnoma odvisno od računalnikov. Zaposlene imajo svoje informatike, ki skrbijo za brezhibno delovanje omrežja in računalnikov. Ti se zavedajo pomembnosti zaščite, prepričati morajo še vodstvo. Recimo da ima podjetje 500 računalnikov.

Neuporaba administratorskih privilegijev za vsakodnevno delo je postala stalnica in je samoumevna v vseh bolje ozaveščenih podjetjih. Ponekod so šli celo tako daleč, da ni skrbniki omrežja niso administratorji pod svojim imenom. Njihov profil je tak kot profil ostalih uporabnikov. Zaradi narave dela seveda poznajo tudi administratorska gesla, a morajo zamenjati profil. To je seveda pohvalno, saj pripomore k celotni varnosti omrežja.

Stalno posodabljanje operacijskih sistemov je zelo pomembno v velikih podjetjih. Še posebej strežnikov. Vestni upravitelji omrežja bodo pazili na to. Tudi posodabljanje vseh ostalih računalnikov je pomembno. Najboljša strategija je, da se popravki nameščajo takoj po izidu. Še bolje je, če ima podjetje temu namenjen strežnik v notranjem omrežju, preko katerega se nameščajo popravki, kar pohitri in poenostavi ves postopek.

Nastavitve brskalnika morajo biti čim bolj restriktivne, potem pa jih malo sprostimo, če se izkaže, da je potrebno. Glede na to, da uporabniki nimajo administratorskih privilegijev, si sami ne morejo spreminjati nastavitev. Najboljše je centralno nastavljanje, ki se potem odraža na vseh računalnikih v isti skupini. Spremembe so tako hitre in poceni, saj ni potrebno nikomur obiskati vseh računalnikov v organizaciji in ročno spreminjati nastavitev.

Veliko podjetje brez požarnega zidu ne more normalno funkcionirati. Komunikacij v notranjem omrežju je preveč in so preveč dragocene, da bi bile nezavarovane. Požarni zidovi, namenjeni tako velikim organizacijam, so zelo zmogljivi. Ne samo, da ne spuščajo določenih komunikacij zunanjega omrežja z notranjim, preprečujejo tudi obratno pot. Cena za požarni zid ni nizka, odvisna je od potreb organizacije. Ciscov požarni zid, ki zmore milijon povezav, stane 22.900 USD (Miracle, 2005). Ni samostojna komponenta, vgradi se v usmerjevalnik (serijo 6500). Poleg tega je razširljiv, če zmogljivosti niso zadostne se doda nov modul.

Protivirusna zaščita je v tako velikem podjetju samoumevna. Vprašanje je le, za kateri izdelek so se odločili. Vse skupaj je lahko centralno upravljano (priporočljivo). Skrbniki omrežja tako dobijo poročilo o grožnjah takoj, ko jih program zazna, lahko na svoj

računalnik, lahko celo v obliki SMS sporočila. Za tako velika podjetja proizvajalci protivirusnih programov ponujajo popuste. Ob nakupu 20 licenc namesto ene npr. NOD32 po licenci stane pol manj (NOD32, 2005). Koliko bo popusta za 500 licenc ni navedeno, a lahko ocenim, da bo zaščita računalnikov in strežnikov stala vsaj 2 mio SIT.

Zaščita pred vohunskimi programi je od vseh kategorij najbolj prezrta. Je nova kategorija, aktualna vedno bolj v zadnjem času. Obstaja nekaj dobrih brezplačnih rešitev, ki so sicer še v testnih verzijah, a zadostijo potrebam. Seveda niso popolne, a so brezplačne. Proizvajalci teh produktov tudi ne ciljajo še na podjetja, marveč na posameznike. Podjetje bi nakup zaščite stal 15.000 USD, kar je absolutno preveč.

5. Sklep

V svojem diplomskem delu sem predstavil koncept zlonamernih programov in jih razvrstil v kategorije. Zelo hitro sem ugotovil, da je razvrstitev ni lahka. Srž problema tiči v samem poimenovanju, ki je posledica zgodovinskega razvoja. Marsikateri avtor postane nedosleden in viruse, ki so le ena kategorija zlonamernih programov, povzdigne na prvo mesto. Virus postane skupen izraz za vse tipe zlonamernih programov. Poleg tega vedno več zlonamernih programov vsebuje več značilnosti, zaradi katerih jih lahko uvrščamo v različne kategorije. Raba izraza virus postaja vse bolj neustrezna tudi zato, ker vse bolj izgubljajo na pomenu. Njihova aktualnost se vsako leto zmanjšuje, pridobivajo pa ostali. Vseeno so bili, kot smo videli v zgodovinskem pregledu, virusi prvi,. Od tod izvira uporaba tega izraza v generičnem smislu in kot tako jo lahko do neke mere razumemo.

V veliki meri sem se posvetil celoviti zaščiti pred zlonamernimi programi. Sledenje navodilom omogoča visoko stopnjo zaščito. A sledi razočaranje. Popolne zaščite ni in jo je tudi teoretično nemogoče vzpostaviti. Vedno se tudi v najpopolnejši obrambi skrivajo pomanjkljivosti, ki so lahko posledica premnogih dejavnikov. Ena od njih so lahko uporabniki, ki v svoji naivnosti ali namerno povzročijo ranljivost sistema, za druge pa morda niti ne vemo, dokler se ne pokažejo skozi neljubi dogodek.

Stroški okužbe so lahko ogromni. Naj gre za premišljen nameren napad ali pa le za smolo. V zadnjem poglavju sem prikazal probleme z merjenjem. Podal sem ocene najvidnejših ocenjevalcev. Čeprav kritike niso skope, pa se tudi kritiki strinjajo, da stroški obstajajo. Tega nihče ne more zanikati. Gre la za razpravo o tem ali so astronomski ali le veliki.

Opozoril bi še na en vidik zlonamernih programov. Samo varovanje in zaposleni v podjetju, zadolženi za varnost informacijskih sistemov, bi se morali šteti med stroške povzročenih s

strani zlonamernih programov. Določena tehnologija, programi in zaposleni so v podjetju izključno kot posledica tega. Brez obstoja zlonamernih programov bi bili brez pomena.

Protiargument bi bil, da v makroekonomskem smislu to niso stroški. Zaposleni imajo plače, kupuje se nova oprema. Od tega živijo proizvajalci opreme in programov za varovanje, ki imajo svoje zaposlene. Pravzaprav zlonamerni programi povečujejo blaginjo.

Litertatura

1. Cashell Brian et al.: The Economic Impact of Cyber-Attacks. Congressional Research Service. 45 str.
   [URL: http://www.cisco.com/warp/public/779/govtaffairs/CRS_Cyber_Attacks.pdf], 1.4.2004.
2. Castelli Jacqueline: Choosing your anti-virus software. SANS Institute. [URL: http://www.sans.org/rr/papers/download.php?id=784&c=b26c7842fa6125908a216de88f8b6651], 2.4.2002.
3. Doernberg Curt: Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy. 49 str. [URL: http://www.nsa.gov/snac/webs/ie_5_5.pdf], 7.2002.
4. Goljevšček Katja, Dernovšek Igor: Virusi, črvi in druge pošasti. Gospodarski vestnik, Ljubljana, 53(2004), 52, str. 43-44.
5. Gostev Alexander: Virus Top Twenty for July 2005. Kaspersky Lab.
   [URL: http://www.viruslist.com/en/analysis?pubid=167966751], 1.8.2005.
6. Gradišar Miro: Uvod v informatiko. Ljubljana : Ekonomska fakulteta, 2003. 516 str.
7. Hiemstra Johan: Malicious Code. TechExams.net.
   [URL: http://www.techexams.net/technotes/securityplus/malicious_code_sd.php], 6.9.2004.
8. Hindocha Neal: Threats to Instant Messaging. Symantec Security Response. 24 str. [URL:
   http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf] 3.1.2003.
9. Jaques Robert: Cost of malware soars to $166bn in 2004. Vnunet.com.
   [URL: http://www.vnunet.com/2126635], 1.2.2005.
10. Kaspersky Lab: Three Criteria for Malware Existence.
    [URL: http://www.viruslist.com/en/viruses/encyclopedia?chapter=153279591], 15.4.2005.
11. Kephart Jeffrey O., White Steve R.: Measuring and Modeling Computer Virus Prevalence. Oakland (CA), Institute of Electrical and Electronic Engineers, 1993. 13 str.
12. Kovačič Andrej et al.: Prenova in informatizacija poslovanja. Ljubljana : Ekonomska fakulteta, 2004. 345 str.
13. Mashevsky Yury: Watershed in malicious code evolution. Kaspersky Lab. [URL: http://www.viruslist.com/en/analysis?pubid=167798878], 29.7.2005.
14. Ropelato Jeff: What is Spyware?.
    [URL: http://anti-spyware-review.toptenreviews.com/what-is-spyware.html], 20.6.2005.
15. Sherriff Lucy: Counting the cost of cybergeddon. The Register.
    [URL: http://www.theregister.co.uk/2004/02/27/counting_the_cost_of_cybergeddon/], 27.2.2004.

16. Skoudis Ed, Zeltser Lenny: Malware: Fighting Malicious Code. Upper Saddle River (N.J.) : Prentice Hall PTR, 2003. 672 str.
17. Swire Peter P.: What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory. Arxiv. 54 str. [URL: http://arxiv.org/ftp/cs/papers/0109/0109089.pdf], 24.9.2001.
18. Šuster Gregor: Boj z vohunsko programsko opremo. KOMPAS Xnet. [URL: https://www.ntk2005.microsoft.si/slovenija/ntk2005/udelezenci/predavatelj/material/1129_2.PPT], 19.5.2005.
19. Vuille Gérard: Computer Virus Classification. Metropolitan Network BBS. [URL: http://www.avp.ch/avpve/classes/classes.stm], 3.5.2005.

Viri

1. Alwil Software. [URL: http://www.avast.com/], 2.7.2005.
2. Anti-Spyware software review. TopTenREVIEWS, Inc [URL: http://anti-spyware-review.toptenreviews.com/], 2.8.2005.
3. Cisco Systems: Economic Impact of Network Security Threats. 17 str. [URL: http:// www.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.pdf], 2002.
4. Computer Associates. [URL: http://home.ca.com/dr/sat4/ec_MAIN.Entry17c?CID=182708&PN=5&SP=10007&SID=35715&PID=666151&DSP=&CUR=840&PGRP=0&CACHE_ID=182708], 2.7.2005.
5. Cybertrust: Anti-Virus Certification Criteria. [URL: https://www.icsalabs.com/icsa/topic.php?tid=4a9d$80389867-30af3d4c$5524-512093a1], 15.6.2005.
6. Doctor Web. [URL: http://www.drweb.com/], 2.7.2005.
7. Eset. [URL: http://www.nod32.com/home/home.htm], 2.7.2005.
8. Frisk. [URL: http://www.f-prot.com/], 2.7.2005.
9. F-Secure. [URL: http://www.f-secure.com/], 2.7.2005.
10. Grisoft. [http://www.grisoft.com/doc/1], 2.7.2005.
11. Guinness World Records: Guinness World Records 2005. Enfield (UK) : Guinness, 2004. 288 str.
12. H+BEDV. [URL: http://www.antivir.de/en/index.html], 2.7.2005.
13. McAfee Inc.. [URL: http://www.mcafeesecurity.com/us/audience/enterprise_home.asp?wt.mc.n=us_us_learnmore_ent&wt.mc_t=int_pro_hom&cid=10350], 2.7.2005.
14. Mi2g: MyDoom becomes most damaging malware as SCO is paralysed. [URL: http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/010204.php]. 1.2.2004.
15. Miracle: Cisco Firewall Services Module.

[URL: http://store.yahoo.com/shopmiracle/ws-svc-fwm-1-k9.html], 1.9.2005.
16. NOD32: Cenik verzij. [URL: http://www.nod.si/], 1.9.2005.
17. Norman. [http://www.norman.com/], 2.7.2005.
18. Panda Software. [URL: http://www.pandasoftware.com/], 2.7.2005.
19. Pogojna kazen za izumitelja uničujočega virusa. Sta. Dnevnik, Ljubljana, 9.7.2005.
20. Računalniške novice. [URL: http://www.racunalniske-novice.com/main/], 2.7.2005.
21. Računovodja.com: Referenčni cenik storitev združenja za računalništvo in informatiko za storitve s področja IT.
[URL: http://racunovodja.com/mdokumenti/cenzdruz.asp], 1.9.2005.
22. Seven Firewalls Fit for Your Enterprise. Networkcomputing. [URL: http://www.networkcomputing.com/shared/printArticle.jhtml?article=/921/921f2report.html&pub=nwc], 10.8.2005.
23. SiPS, mi2g: Frequently Asked Questions – SIPS & EVEDA – v1.00. 5 str.
[URL: http://www.mi2g.com/cgi/mi2g/press/faq.pdf], 17.3.2004.
24. Softwin. [URL: http://www.bitdefender.com/], 2.7.2005.
25. Symantec. [URL: http://www.symantec.com/index.htm], 2.7.2005.
26. Trend Micro. [URL: http://www.trendmicro.com/en/home/us/enterprise.htm], 2.7.2005.
27. Virus Bulletin: VB 100% test procedures.
[URL: http://www.virusbtn.com/vb100/about/100procedure.xml], 15.6.2005.
28. Virus Screenshots.
[URL: http://www.kaspersky.com/press?chapter=146158526], 24.7.2005.
29. Viruslist.com: Trojan Programs.
[URL: http://www.viruslist.com/en/virusesdescribed?chapter=152540521], 15.4.2005.
30. West Coast Labs: West Coast Labs Technology Reports.
[URL: http://www.westcoastlabs.org/checkmarkcertification.asp], 15.6.2005.
31. Wikipedija: Požarni zid.
[URL: http://sl.wikipedia.org/wiki/Po%C5%BEarni_zid], 30.6.2005.

Priloge

Priloga 1: Rezultati testa protivirusnih programov

ggifggifusershttp://www.virusbtn.com/print/vb100/archives/products.xml?table
Introduction

This summary table displays the results of the most recent comparative reviews for each platform tested. For more information on how each product has performed in all previous *VB* comparative reviews (back to 1998), click on the product name. To see the full results for each of the comparatives listed, click on the date of the test.

Results table

Key: Pass Fail No entry

	NetWare Aug *04*	Windows Server 2003 Nov *04*	Windows NT Feb *05*	Red Hat Linux 9 Apr *05*	Windows XP Jun *05*
AhnLab			VB100%		VB100%
Aladdin Knowledge Systems (eSafe)					
Alwil (Avast!)		VB100%	VB100%	VB100%	VB100%
ArcaVir (ArcaBit)			X		X
Authentium (formerly Command Software Systems)		VB100%	VB100%		VB100%
Avira			VB100%	VB100%	VB100%
BLC Win Cleaner		VB100%	VB100%		X
CAT QuickHeal	X	VB100%	VB100%	VB100%	X
Computer Associates (InoculateIT/eTrust)	VB100%	X	VB100%		VB100%
Computer Associates (Vet)		X	VB100%		VB100%
Doctor Web (formerly DialogueScience)	VB100%	X	VB100%	VB100%	VB100%
Eset (NOD32)	VB100%	VB100%	VB100%	VB100%	VB100%
F-Secure		VB100%	VB100%	VB100%	VB100%
Fortinet			VB100%		X
Frisk (F-Prot)		VB100%	X	VB100%	VB100%
GDATA		VB100%	VB100%		VB100%

GeCAD (RAV)	▭	▭	▭	▭	▭
Ggreat	▭	▭	▭	▭	▭
Grisoft (AVG)	▭	100%	100%	100%	100%
H+BEDV (AntiVir)	▭	100%	100%	100%	100%
Hauri (ViRobot)	▭	✗	▭	▭	✗
Ikarus	▭	▭	▭	▭	▭
Kaspersky	100%	100%	100%	100%	100%
Leprechaun VirusBuster II	▭	▭	▭	▭	▭
McAfee Inc. (formerly Network Associates)	100%	100%	✗	100%	100%
MicroWorld (eScan)	▭	100%	✗	✗	100%
NWI Virus Chaser	▭	▭	100%	▭	100%
Norman	100%	100%	100%	100%	100%
Panda Software	▭	▭	▭	▭	▭
Proland Software	▭	▭	▭	▭	▭
Secure Resolutions	▭	▭	✗	▭	▭
Softwin (BitDefender)	▭	100%	100%	100%	100%
Sophos	100%	100%	100%	✗	100%
Symantec (Norton)	100%	100%	100%	▭	100%
Trend Micro (PC-cillin)	▭	100%	▭	100%	▭
Unasoft	▭	✗	✗	▭	✗
VirusBuster	100%	100%	100%	✗	100%

Vir: Virus Bulletin, 2005

Slovar tujih izrazov

TUJI IZRAZ	SLOVENSKA RAZLAGA
backdoor	stranska vrata
BBS	elektronske oglasne deske
CD	zgoščenka
denial of service, krat. DoS	zavrnitev storitve
file-sharing network	omrežja za souporabo datotek
hoax	potegavščina
instant messaging	takojšnje sporočanje
internet relay chat	spletni klepet
master boot record	glavni zagonski zapis
peer to peer programs, krat. P2P	programi za neposredno uporabniško povezavo
port	vrata
proxy srver	posredovalni strežnik
router	usmerjevalnik
server	strežnik
Trojan	trojanski konj, trojanec
Windows	Okna
workstation	delovna postaja
worm	črv