UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

RAČUNALNIŠKI VIRUSI IN NJIHOV VPLIV NA DELOVANJE POSLOVNIH INFORMACIJSKIH SISTEMOV

Ljubljana, april 2004 GREGOR MOZETIČ

IZJAVA

Študent/ka Gregor Mozetič izjavljam, da sem avtor/ica tega diplomskega dela, ki sem ga

napisala pod mentorstvom prof. dr. Borke Jerma Blažič in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne_____ Podpis: _____

KAZALO

UVOD

V današnjih dneh si s težavo predstavljamo, da se je prvi osebni računalnik (PC) pojavil šele avgusta, leta 1981. V samem začetku je računalnike uporabljala le peščica ljudi. Danes pa je postalo življenje brez osebnega računalnika skorajda nemogoče. Nekaterim pomaga pri vodenju podjetja ali obrti, drugim služi za povezavo s svetom, za izobraževanje in nenazadnje so zelo pripravni tudi za igranje računalniških iger. Število najrazličnejših programov nenehno narašča. Poznamo programe za urejanje besedil, risanje, pisanje, projektiranje in načrtovanje, obdelavo slik, preračunavanje podatkov in še marsikaj drugega. Programi so prisotni v malo da ne vseh dejavnostih, s katerimi se srečujemo v vsakodnevnem življenju.

Med koristne programe sem in tja zaidejo tudi nekateri škodljivi programi, ki jim pravimo računalniški virusi. Virusi se nenadzorovano razmnožujejo in uničujejo naše dragocene podatke. O tem, kako delujejo, kako se jih ubranimo, ali kako jih odstranimo, pa večina uporabnikov ne ve skorajda nič. Ustrašimo se, ko zanje slišimo, polni smo napačnih predstav in pogosto se predvsem počutimo prav nemočni.

K hitremu širjenju računalniških virusov je v veliki meri pripomogel nagel razvoj omrežji, ki je dejansko povezal računalnike iz vseh koncev sveta. Surfanje po internetu je danes postal konjiček vseh generacij. Kot pa se rado dogaja, je tudi internet poleg vseh koristi, prinesel s seboj kopico problemov glede varnosti in zaščite naših podatkov (računalnikov). Okužbe datotek, elektronske pošte, napadi na spletne strani in drugo so vse dokaz, da potrebujemo večjo osveščenost in boljšo zaščito naših omrežji.

V diplomski nalogi bom govoril o računalniških virusih, njihovem nastanku in delovanju, kako se pred njimi zaščitimo, in o tem, kako okužene programe zdravimo, in jih s tem ponovno usposobimo za delovanje. Predstavil bom najpogosteje uporabljene programe za odpravo virusov in preventivno zaščito pred njimi, ter navedel njihove prednosti in slabosti.

V prvem poglavju natančneje definiram, kaj je zlonameren program (virus), njegove karakteristike delovanja, in opišem različne vrste zlonamernih programov. Podam klasifikacijo virusov glede na način delovanja in glede na okužen objekt, opišem kaj virusi počnejo, kdo jih piše in kako se razmnožujejo.

Drugo poglavje je namenjeno zgodovini virusov, kjer podam glavne smernice v zgodovini nastajanja zlonamernih programov. Temu sledi pregled situacije danes, ki je podprt s kvantitativno analizo sekundarnih podatkov. Na koncu poglavja natančneje opišem še nekatere najbolj poznane viruse in podam napovedi za prihodnost.

Tretje poglavje razkriva resnost problema virusov v podjetjih in njihovo finančno plat. To pomeni obseg stroškov v primeru okužbe in stroškovno plat preventive pred zlonamernimi programi.

Četrto poglavje opisuje preventivne postopke, ki bodo preprečevali oziroma odpravljali posledice okužb z virusi, načine odkrivanja in nazadnje še postopke odprave virusov.

Zadnje poglavje opisuje protivirusne programe, kako in na kaj morajo podjetja biti pozorna pri nakupu, in na koncu poda še primer analitičnega ocenjevanja aplikacij na trgu, ki lahko služi organizacijam za zgled pri izbiri optimalnega protivirusnega programa.

1. RAČUNLNIŠKI VIRUSI

Računalniški virusi so ena od nevarnosti, ki ogrožajo varnost in integriteto računalniškega sistema. Tako kot ostale grožnje lahko povzročijo izgubo oziroma spremembo podatkov in tako kompromitirajo njihovo celovitost (White et al., 1989, str. 1). Virus bi morda v nekaj preprostih besedah opredelili kot računalniški program, ki ima sposobnost samokopiranja (svojega podvajanja na druge programe) in to brez vednosti (dovoljenja) uporabnika. Virusi se širijo na dva načina: s pomočjo okuženih medijev (diskete, cd, itd.) ali z dostopom do drugih računalnikov, s katerimi smo povezani prek modema ali mrež, v katero je vključenih več računalnikov (Mrhar, 1995, str. 17). Njihovo delovanje, ki je običajno škodljivo, se lahko izraža na različne načine. Lahko nam povzročijo pojavljanje različnih sporočil na ekranu, zbrišejo različne datoteke ali pa celo uničijo strojno opremo. V večini primerov so okužbe z virusi za uporabnika neopazne. Simptomi se pričnejo pojavljati šele čez čas, ko začne računalnik delovati počasneje in programi postajajo vse bolj nestabilni.

Do okužbe z virusom pride v trenutku, ko zaženemo okužen program, ki povzroči nadaljnjo kopiranje virusa na druge datoteke in v končni fazi predhodno omenjene pojave. Da do tega pride, poskrbijo virusi na vrsto načinov – lahko se prilepijo uporabnim programom oziroma se skrijejo v programsko kodo, ki se avtomatično požene ob zagonu različnih vrst datotek.

Splošno označevanje škodljivih programov z imenom virusi je morda nekoliko zavajajoče in v zadnjih časih preveč posplošeno. Razlike med virusi, črvi, trojanskimi konji, logičnimi bombami in potegavščinami (hoax) so postale vse manj opazne. Vsekakor pa je s stališča uporabnika (administratorja), ki želi preprečiti okužbo računalnika s škodljivimi programi, pomembno razlikovanje med različnimi zvrstmi škodljivih programov. Črvi so po delovanju zelo podobni virusom, saj so prav tako sposobni samorazmnoževanja, le da za to ne potrebujejo gostiteljskega programa. Trojanski konji so manjši deli škodljivega programa, vključeni v originalen splošno uporaben program. Logične bombe so kode zlonamernih programerjev vključene v določen program (operacijski sistem) z uničujočim oziroma varnosti škodljivim namenom.

1.1 Kaj je računalniški program

Programe bi lahko posplošeno definirali kot recepte za obnašanje računalnika oziroma kot skupke ukazov in podatkov, ki omogočajo komuniciranje med uporabnikom in računalnikom. Računalnik jih seveda ne prebere, kot to storimo mi, saj ne more razumeti tekstovnih ukazov, pač pa se zanaša na številke. Vzemimo za primer ukaz “ne počni ničesar (do nothing)”, kar je v običajnem Intelovem procesorju število 144. Če to število pretvorimo v binarni sistem, ga lahko zapišemo kot 10010000, kar fizično pomeni navodila za stikala v procesorju – vklopljeno, izklopljeno, izklopljeno, vklopljeno, izklopljeno, izklopljeno, izklopljeno, izklopljeno. Ko poženemo program na našem računalniku, dejansko dajemo napotke

računalniški strojni opremi (hardware), kaj naj z obstoječimi podatki naredi (Norman, 2002, str. 8).

Programi in nekateri podatki se ob zagonu prenesejo v računalnikov notranji spomin (delovni pomnilnik), tako da jih lahko mikroprocesor obdela in nato na izhodnih napravah (zaslon, tiskalnik) prikaže rezultate (Mrhar, 1995, str. 14). Ob tej navedbi definirajmo izraz »rezidenten«. Če je program rezidenten, pomeni da je aktiven v delovnem spominu. Tak program je prisoten v delovnem spominu za daljše časovno obdobje. V času, ko se je še uporabljal operacijski sistem DOS, je bila večina programov nerezidentnih, kar pomeni, da so opravili svojo nalogo in prenehali z delovanjem. V današnjih Windowsih pa je večina programov rezidentnih, dokler jih ne izklopimo.

1.2 Zlonamerni programi

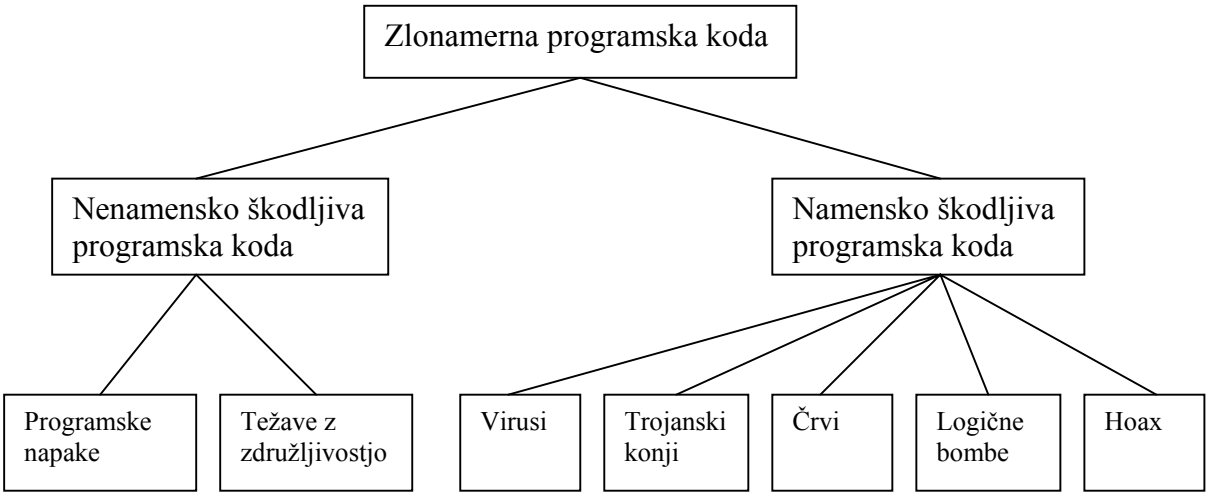
Preden definiramo zlonamerne programe, je pomembno definirati, kdaj lahko program označimo kot zlonameren. Definiranje je oteženo, saj je v veliki meri odvisno od okoliščin, ali je dani program (programska koda) zlonameren ali ne. Vzemimo za primer program za formatiranje trdega diska, ki je lahko označen kot zlonameren ali pa kot koristen. Kako ga bomo označili, je odvisno od namena za katerega je uporabljen.

Zlonamerni program (programska koda) je lahko vsak del programske kode, ki izvede kakršnokoli operacijo proti specifikacijam in namenu sistema samega. Kot sistem imamo v mislih v celoti nameščeno strojno in programsko opremo (Brunstein, 1999, str. 12).

1.2.1 Razvrstitev in definicija zlonamernih programov

Zlonamerno programsko kodo lahko razdelimo na nenamensko škodljivo programsko kodo in na namensko škodljivo programsko kodo. Z izrazom nenamensko škodljiva programska koda označujemo različne programske napake in težave z združljivostjo različnih programov. Z namensko škodljivo programsko kodo (malware) označujemo viruse, trojanske konje, črve, logične bombe in razne potegavščine (Hoax), ki so bili napisani z namenom, da bi škodovali (glej sliko 1).

Slika 1: Škodljiva programska koda



Vir: Helenius, 2002, str. 12.

1.2.1.1 Virus

Računalniški virusi so programi, ki lahko okužijo ostale programe na računalniku, tako da jih spremenijo na način, da vanje vključijo kopijo samega sebe (Cohen, 1986, str. 17). Iz definicije sledi, da program, ki je označen kot virus, nujno ne povzroči škode. Temeljna značilnost virusov, ki jih loči od ostalih zlonamernih programov, je potreba po gostitelju in preverjanje svoje navzočnosti. Zato je cilj vsakega virusa okužba čim večjega števila datotek in posledično daljša časovna eksistenca.

1.2.1.2 Črv

Računalniški črvi so definirani kot neodvisna programska koda, ki se lahko samostojno reproducira. Poudarek je na besedi neodvisna, saj se lahko računalniški črvi, za razliko od navadnih virusov, razmnožujejo, ne da bi potrebovali gostiteljski program. Pomembna razlika med virusi in črvi je tudi ta, da se računalniški črvi množijo prek vseh meja (ne preverjajo svoje navzočnosti), tako da nam sčasoma popolnoma zasedejo celoten prostor na okuženem disku.V nekaterih obravnavah so računalniški črvi definirani kot podskupina virusov, ker naj bi bil računalnik sam dejansko njihov gostitelj.

1.2.1.3 Trojanski konj

Trojanski konji (ime izhaja iz starogrške legende) so manjši deli škodljivega programa, vključeni v originalen, splošno uporaben program (Mrhar, 1995, str. 17). So samostojna programska koda, ki izvrši neko koristno operacijo, istočasno pa namenoma, brez vednosti uporabnika, izvrši še neko destruktivno dejanje (Bontchev, 1998, str. 14). Glavna razlika, ki

ločuje trojanske konje od splošnih virusov in črvov, je nesposobnost samorazmnoževanja. Širijo se lahko le s kopiranjem okuženega programa.Večina trojanskih konjev se aktivira, ko jih požene uporabnik sam (požene program v katerem je skrita škodljiva programska koda) in nam nato najpogosteje uničijo trdi disk. V tem procesu pa se seveda samouničijo.

1.2.1.4 Logična bomba (časovna bomba)

Logična bomba, kakor nam že samo ime pove, je program, ki ob določenem pogoju oziroma logičnem zaključku, »eksplodira«. Tedaj prične s svojim uničujočim delovanjem – brisanjem podatkov, formatiranjem diskov in podobnimi nevšečnostmi. Najpogosteje se sproži ob določenem datumu ali kakšnem drugem izpolnjenem pogoju. Logična bomba deluje samostojno ali je vključena v kakšen drug program. Osnovna značilnost, ki loči logične bombe od virusov, je nesposobnost samorazmnoževanja, saj je njihov namen ostati neviden do pričetka delovanja.

1.2.1.5 Potegavščina (Hoax)

Potegavščine so verižna elektronska pisma, ki vsebujejo lažna svarila pred novimi virusi, trojanskimi konji in raznimi drugimi nevšečnostmi. Ta povzročijo, da jih njihovi prejemniki, razpošljejo vsem svojim znancem, misleč, da jih s tem svarijo pred okužbo. Potegavščine niso pravi virusi, se ne razmnožujejo sami in ne vsebujejo zlonamerne programske kode, ampak imajo lahko zelo podobne učinke kot pravi virusi. Če jim uporabniki nasedejo in jih razpošljejo naprej, lahko to pripelje do preobremenitve poštnih strežnikov in v končni fazi do prenehanja njihovega delovanja. To pa lahko povzroči podjetju velike časovne in finančne izgube. Rezultat je podoben kot pri pravem virusi (npr. Love Bug), le da hoaxerju pri tem ni bilo potrebno napisati niti vrstice programske kode.

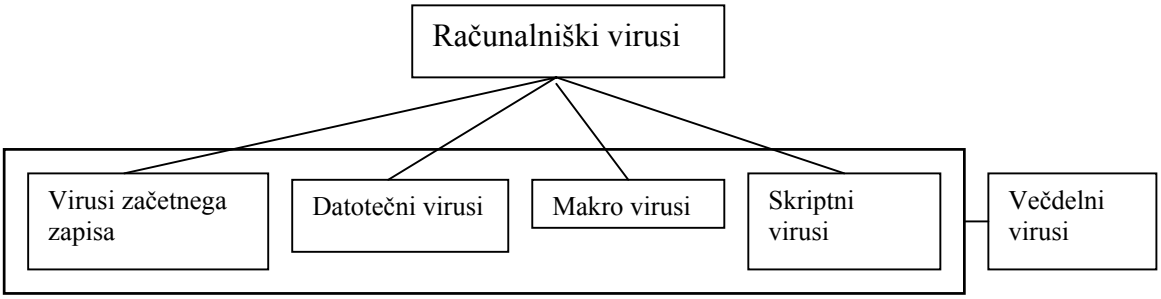
1.3 Klasifikacija računalniških virusov

Računalniške viruse lahko razvrstimo v več razredov. To lahko storimo glede na okužene objekte oziroma glede na značilnosti, ki jih vsebujejo in način delovanja.

1.3.1 Klasifikacija računalniškega virusa glede na okužen objekt

Računalniške viruse lahko glede na okužen objekt razvrstimo na viruse začetnega zapisa, datotečne viruse, makro viruse, skriptne in večdelne viruse. Taka razvrstitev je vidna iz spodnje slike.

Slika 2: Računalniški virusi, razvrščeni glede na okužene objekte



Vir: Helenius, 2002, str. 14.

Virusi začetnega zapisa: So virusi, ki se razmnožujejo z okužbo začetnega zapisa na trdem disku ali disketi. Ker se ta zapis prebere in izvede neposredno ob vklopu računalnika, se virus že v trenutku zagona skrije v sistem, kjer se pritaji, in počaka na primeren trenutek, ko ga uporabnik ali kakšen drugi parameter sproži. Osnovna značilnost virusov začetnega zapisa je iskanje neokuženih začetnih zapisov na disketah in trdih diskih. Prednost tega tipa virusov je ta, da se aktivirajo že pred samim začetkom vzpostavitve sistema in so zato težji zalogaj protivirusnim programom. Ti virusi se ne prenašajo preko mrež, ampak le s prenosnimi mediji.

Datotečni virusi: So virusi, ki se prenašajo (zapišejo) prek izvršilnih datotek (.COM, .EXE) na trdem disku oziroma prek vseh prenosnih medijev (diskete, cd, itd.), ki vsebujejo izvršilne datoteke. Za razliko od skriptnih virusov, so datotečni virusi najpogosteje napisani v strojni kodi in tako s prostim očesom nevidni. Delujejo tako, da se prilepijo na izvršilno datoteko (gostitelja) in z različnimi tehnikami okužijo ostale programe.

Tehnike okužbe datotek:

- prepis (virus se namesti na začetek programa čez originalen program in s tem pokvari originalen program);
- spremljanje (virus ne spremeni programa neposredno, ampak povzroči da operacijski sistem požene virus namesto želenega programa);
- vezava (podobna kot predhodna, le da v tem primeru spremeni začetek gostiteljske datoteke);
- vstavljanje (virus se namesti v neuporabljene praznine gostiteljskega programa in ga pri temu ne okvarijo);
- dodajanje (virus se vstavi na začetek ali konec izvršilne datoteke, ne da bi s tem spremenil programsko skripto – poveča se le velikost datoteke).

Makro virusi: So virusi, ki uporabljajo makro ukaze aplikacij, vstavljene v datoteke za svoje razmnoževanje. Danes večina aplikacij (word, excel itd.) uporablja makro ukaze. Makro virusi so makro programi, ki se lahko kopirajo in širijo iz ene datoteke v drugo (Sophos, 2001, str. 15). Ko odpremo datoteko z makro virusom, se virus preslika v začetni zapis aplikacije in od tega trenutka naprej okuži vse nove datoteke (dokumente), ki jih naredimo (pregledujemo)

s to aplikacijo. Zlonamerni makro virusi lahko spreminjajo tudi samo vsebino dokumenta in so zaradi tega še posebno nevarni.

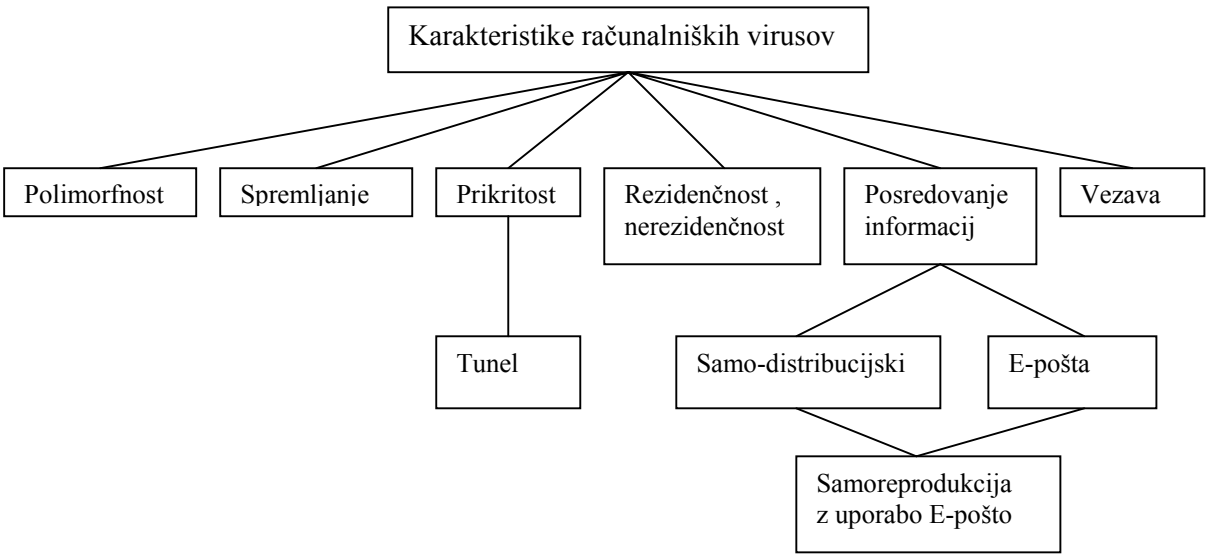
Skriptni virusi: Skriptni virusi so datotečni virusi, ki so za razliko od ostalih virusov napisani v preprosti tekstovni obliki in zaradi tega enostavno berljivi za vsakogar. Ker pa računalniki ne morejo razumeti tekstovnih ukazov direktno, morajo biti ti prvo prevedeni v strojni jezik. Ta postopek se imenuje "prevajanje" in je izveden prek vmesnih programov kot so WSCRIPT.EXE v primeru Visual Basic Script ali COMMAND.COM v primeru DOS skript. Skriptni virusi v večini primerov okužijo prav skriptne datoteke.

Večdelni virusi: Večdelni virusi so virusi, ki uporabljajo vsaj dva od prej navedenih postopkov razmnoževanja. Tako se lahko nekateri virusi razmnožujejo na izvršilnih datotekah in istočasno še z okužbo startnega zapisa, drugi pa lahko okužijo izvršilne in tekstovne datoteke hkrati.

1.3.2 Klasifikacija računalniškega virusa glede na karakteristike (način) delovanja

Vsak virus ima svoje specifične karakteristike delovanja, na podlagi katerih ga lahko razvrstimo po skupinah. Datotečni virus je lahko klasificiran kot rezidenčen virus, prikrit (stealth) virus, samo-distribucijski in mnogoličen (polymorphic) virus. Virus ima lahko več karakteristik, vsak virus pa je bodisi rezidenčen ali nerezidenčen (direct action). Iz naslednje slike je vidna klasifikacija po karakteristikah.

Slika 3: Računalniški virusi razvrščeni glede na značilnosti delovanja



Vir: Helenius, 2002, str. 15.

Rezidenčni virusi: Rezidenčni virusi so v delovnem pomnilniku stalno prisotni in so tehnološko precej dodelani. Ti virusi se namreč v trenutku, ko poženemo okužen program (podobno kot virusi začetnega zapisa), prenesejo v računalnikov delovni pomnilnik. V njem

čakajo, vse dokler ni izpolnjen pogoj za okužbo neokužene datoteke. Datoteke se, denimo, okužijo v trenutku, ko samo pogledamo njihovo vsebino, ali takrat, ko datoteko poženemo ali kopiramo. Skratka, ti programi neprestano opazujejo, kaj počnemo, in šele ob izpolnitvi pogoja (npr. ukaza za kopiranje) se začne njihovo razmnoževanje. Nato počakajo na primeren trenutek za začetek uničevalnega pohoda in škoda je tu. Za delovanje rezidenčnih virusov je dovolj, da le enkrat poženemo okužen program (Mrhar, 1995, str. 27).

Nerezidenčni virusi: So takšni virusi, ki po trenutku, ko so bili zagnani, ne ostanejo aktivni v računalniškem pomnilniku. To pomeni, da se njihovo razmnoževanje izvrši v trenutku, ko je zagnana virusna koda oziroma okužen program. Po prenehanju uporabe okuženega programa virus miruje.

Virus, ki posredujejo informacije: To so virusi, ki imajo namenoma vgrajeno lastnost, ki jim omogoča posredovati določene informacije iz lokalnega računalnika do tujega, oddaljenega računalnika, prek različnih informacijskih poti. Z besedo tuj računalnik je opredeljen računalnik, različen od tistega na katerem je bil virus zagnan. Posredovane informacije so lahko zelo pomembne (osebne).

Samo-distribucijski virusi: So virusi s sposobnostjo samoreprodukcije iz enega sistema v drugega prek različnih informacijskih kanalov.

Virusi E-pošte: Se nanaša na viruse s sposobnostjo pošiljanja elektronske pošte. V tem primeru je lahko v poslanem elektronskem sporočilu virus ali pa tudi ne.

Samoreprodukcija z uporabo e-pošte: To so virusi, ki imajo lastnost, da se sami razpošljejo s pomočjo elektronske pošte in zato spadajo v podskupino samo-distribucijskih in e-poštnih virusov.

Spremljanje: Je značilnost nekaterih virusov, da izkoristijo nekatere specifične značilnosti sistema za svojo reprodukcijo. Kot primer lahko vzamemo MS-DOS-ve izvršilne datoteke COM, ki se zaženejo pred izvršilnimi datotekami s končnico EXE. To pomeni, da v primeru ko imata dve datoteki enako ime, se bo najprej izvršila datoteka s končnico COM. Virus lahko to značilnost sistema izkoristi tako, da se bo v primeru zagona programa najprej zagnala skripta virusa in šele nato želeni program.

Polimorfnost: Je značilnost nekaterih virusov, da lahko z vsako novo kopijo spreminjajo svojo pojavno obliko. To dosežejo tako, da se poslužujejo spremenljivih kodirnih postopkov, spremenljivih zaporedij ukazov, spremenljivih ukazov oziroma kombinacijo vseh teh metod.

Prikritost (stealth): Je značilnost posameznih virusov, da prikrijejo vsaj nekatere spremembe, ki so jih povzročili sistemu. Tako lahko prestrežejo ukaz, s katerim kontroliramo dolžino okužene datoteke, in nam sporočijo originalne podatke o datoteki, s čimer se okužen program na prvi pogled ne spremeni. V primeru, ko jih skušamo odkriti s posebnimi programi, se lahko

celo uničijo. Najpogosteje so ti virusi rezidentni v pomnilniku, da lahko prikrivajo vse spremembe, ki so jih povzročili.

Tunel: Je le lastnost virusov, da prikrijejo spremembe v sistemu. So podskupina prikritih virusov, le da so za razliko od teh vedno rezidentni in pognani pred protivirusnim programom. S tem se izognejo odkritju.

Vezava: Se nanaša na viruse, ki imajo tako programsko kodo, da spremenijo naslove v sistemu, da ti kažejo na njih. V operacijskem sistemu MS-DOS ima vsaka mapa posebne podatke, ki vsebujejo naslove, kje se dejansko nahajajo datoteke, ki se prikažejo v mapi na trdem disku. Prav te naslove pa virusi spremenijo, da kažejo na virus. Šele ko je virusna koda pognana, se požene pravi program.

1.4 Delovanje računalniških virusov

Kot sem že predhodno povedal, so računalniški virusi programi, ki lahko okužijo ostale programe na računalniku, tako da jih spremenijo na način, da vanje vključijo kopijo samega sebe. Računalniški virusi imajo tri temeljne značilnosti delovanja (mehanizme): reprodukcijski mehanizem, aktivacijski mehanizem in nek cilj. *Reprodukcijski* mehanizem izvede naslednje funkcije:

- Preišče računalnik za potencialne programe, ki jih bo virus okužil.
- Ko dobi programe, jih preveri, če so bili že predhodno okuženi.
- Vstavi skrito skripto v program.
- Spremeni zaporedje izvajanja programa, tako da se vsakič, ko je pognan program zažene tudi skripta virusa.
- V večini primerov označi okužen program in s tem prepreči, da bi bil isti program večkrat okužen.

Aktivacijski mehanizem preverja izpolnitev v virusu določenih pogojev. Ko so ti pogoji izpolnjeni virus izvede svoje ciljno dejanje, ki je v večini primerov nekaj škodljivega.

Cilj je običajno neko škodljivo dejanje.

1.4.1 Kaj virusi počnejo?

Med najpogostejše početje virusov spada:

- Virusi - črvi se lahko le razmnožujejo, ne da bi s tem kakorkoli poškodovali podatke. Tako v zelo kratkem času zasedejo celoten prostor na trdem disku ali na omrežju, kar onemogoči vsakršno delo.
- Tudi virusi, ki se le razmnožujejo, lahko uničijo del programa pri tem, ko se lepijo na datoteke.

- Humoristični virusi podatkov običajno ne uničijo, ampak izvedejo nek zabaven dogodek. To je lahko kakšen zabaven napis (WM97/Jerk je izpisal »mislim da je ….. neumen«), animacija, ali celo zaigrana melodija ob določeni uri (Yankee) (Sophos, 2001, str.10).
- Nekateri virusi so namenjeni samo uničevanju in spreminjanju podatkov. Podatke lahko poškodujejo na več načinov: jih zbrišejo (virus Michelangelo zbriše del trdega diska vsakega 6. marca), spremenijo (virus XM/Compatable spreminja podatke v excelovih razpredelnicah) in v najslabšem primeru celo formatirajo trdi disk (Sophos, 2001, str. 10).
- Določeni virusi nam lahko onemogočijo dostop do lastnih dokumentov. Tak je npr. virus WM97/NightShade, ki z geslom zaščiti dokumente in nam tako onemogoči dostop do lastnih dokumentov (Sophos, 2001, str. 10).
- Virusi kraje podatkov po elektronski pošti pošljejo podatke o uporabniku in računalniku na določen naslov (Troj/LoveLet-A) (Sophos, 2001, str. 10).
- Virusi, ki onesposobijo strojno opremo, poskušajo prepisati oziroma zbrisati vgrajen program BIOS in tako onesposobit računalnik. V tem primeru je rešitev le zamenjava BIOS-a (ROM-a). Tak virus je npr. CIH ali Chernobyl (W95/CIH-10xx), ki poskuša zbrisati BIOS 26. aprila (Sophos, 2001, str. 10).

1.4.2 Kdo piše viruse

Nekoč je veljalo, da so viruse pisali le programerji z dobrim znanjem računalniškega programiranja. Danes se je ob pojavu novih pripomočkov (programov) situacija zelo spremenila v prid osebam z manj programerskega znanja. Na prvi pogled je zelo malo razlogov, ki bi lahko spodbujali ljudi k pisanju virusov, saj pisec s tem početjem ne more nič zaslužiti in le redko postane slaven. Pisanje virusov lahko primerjamo z raznimi oblikami vandalizma in grafitov, ki niso usmerjeni k določeni žrtvi. Pisci virusov pripadajo v večini primerov moškemu spolu do 25 let starosti in so v večini primerov samski (Sophos, 2001, str. 21). Najpogosteje pripadajo eni od naslednjih skupin:

- *Programerski eksperimentatorji*: To so programerji na fakultetah ali v laboratorijih, v katerih proučujejo računalniške viruse, hekerji – programerji, ki jim je programiranje v užitek itd. Virusi iz teh izvorov običajno zaidejo v javnost le pomotoma (Mrhar, 1995, str. 35).
- *Šaljivci*: Osebe, ki se s pisanjem virusov predvsem zabavajo. Ti virusi so navadno hudomušni in neškodljivi, čeprav jih, ob odkritju kakšne nove tehnike, škodoželjni programerji hitro prikrojijo v zelo škodljive viruse (Mrhar, 1995, str. 35).
- *Škodoželjni programerji*: Cilj škodoželjnih programerjev je popolno uničevanje podatkov iz različnih vzrokov. Med njimi so najpogosteje odpuščeni programerji in programerji iz vzhodnih držav, ki imajo pogosto izredno dobro znanje programiranja (Mrhar, 1995, str. 35).
- *Mladi programerji*: Ti želijo odkriti tehnologijo virusov in niti ne vedo, v kaj se spuščajo. Mnogi bi se radi s svojim znanjem pokazali pred drugimi (Mrhar, 1995, str. 35).

1.4.3 Razmnoževanje virusov

Razmnoževanje je prvi pogoj za preživetje računalniških virusov. Pametnejši virusi najprej preverijo, če je program že okužen, tako da ga ne okužijo ponovno, čeprav tega ne zmorejo vsi. Virus mora imeti zapisano kodo, ki jo zmore prepoznati, če želi preveriti, ali je nek del diska okužen. Kadar je koda v določenem programu že prisotna, ga virus niti ne bo poskušal okužiti. Ko je nek program okužen, se virus običajno za nekaj časa pritaji in šele kasneje prične z uničujočim delovanjem. Pred tem se mora namreč čim bolj razširiti po preostalih sistemih in programih.

2. EVOLUCIJA PROBLEMATIKE RAČUNALNIŠKIH VIRUSOV

V samem začetku računalništva računalniki med seboj niso bili povezani oziroma so bili slabo povezani. Prav to je bil eden od poglavitnih razlogov za zelo počasno širjenje virusov. Datoteke so se prenašale preko BBS-ja (bulletin board system) in na disketah. Te značilnosti prenosa podatkov so onemogočale neomejeno širjenje virusov. Širjenje virusov je bilo geografsko omejeno.

Kmalu zatem se je kot posledica tehnološkega razvoja začela povečevati povezanost računalniških sistemov. Sprva se je to najbolj opazilo v podjetjih, ki so imela največ kapitala za tehnološko posodabljanje, takoj zatem pa še v privatnem sektorju. Najprej so se pojavila lokalna omrežja (LAN – Local Area Network), nato so se ta začela širiti v regionalna omrežja (WAN – Wide Area Network) in v končni fazi je nastal Internet. Vsa ta povezanost predstavlja idealno okolje za širjenje virusov, ki niso več geografsko omejeni.

Danes živimo v družbi, v kateri je v ospredju globalna tehnologija in globalno poslovanje, vodeno prek sodobnih komunikacijskih kanalov. Računalniki so poglavitni del te tehnologije in zato postanejo vse informacije, ki jih vsebujejo, globalne. Vse to žal velja tudi za viruse, ki se v današnjih dneh veliko lažje širijo, kot so se v preteklosti.

2.1 Zgodovina virusov

Teorije o programih, ki so se sposobni razmnoževati sami, zasledimo že leta 1949 – pri madžarskem znanstveniku Johnu von Neumannu. Prvi računalniški virus je bil narejen na računalniku Apple IIe okoli leta 1981 in se je imenoval ″Elk Cloner″. Ta virus ni brisal ali spreminjal podatkov, temveč je le izpisal poezijo ob petdesetem zagonu diska. Na osebnih računalnikih (PC) so se virusi pojavili leta 1986 - ″Brain″ ali ″Pakistan″, ravno tako neškodljivi, saj so imeli le publicistične namene. Zamisel o uničujočih programih se je porodila v ameriškem vojaško-znanstvenem okolju. Leta 1987 so se pojavili trije novi koncepti virusa. Prvi je bil virus ″Lehigh″, ki je kot prvi okužil datoteko ″command.com″, ki je ključna pri delovanju operacijskega sistema. Drugi je bil ″Jerusalem″, ki je bil prvi rezidenčen

virus v delovnem spominu. Tretji pa je bil virus ″Stoned″, ki je bil prvi virus začetnega zapisa. Leta 1989 se je pojavil prvi polimorfen virus, imenovan ″Washburn″, ki neprestano spreminja svojo pojavno obliko, in tako otežuje delo protivirusnim programom. V istem letu se je pojavil še ″Frodo″, ki je bil prvi prikriti (stealth) virus, in ″AIDS″ - prvi trojanski konj. Leta 1991 se je pojavil prvi večdelni (multipartite) virus z imenom ″Tequila″. Leta 1994 se je pojavil prvi hoax (potegavščina) z naslovom ″Good Times″, ki je svaril pred neobstoječimi virusi in nas naprošal, naj o tem obvestimo tudi svoje znance. Leta 1995 se je pojavil prvi makro virus (Concept), ki okuži Wordove dokumente. Leta 1998 se pojavi prvi virus s sposobnostjo onesposobitve BIOS-a - ″CIH″. Razvoj virusov kaže na to,da imajo avtorji virusov vedno več orodji, s katerimi si lahko pomagajo pri pisanju, in hkrati postajajo vedno bolj domiselni.

2.2 Kvantitativna analiza pojavljanja virusov

Če govorimo o problematiki virusov, je prav, da si podrobneje ogledamo, kako se je kvantitativno spreminjal ta problem skozi leta. V vsakoletni kontinuirani (od leta 1996 naprej) raziskavi laboratorija ICSA, ki predstavlja del organizacije TruSecure, je nazorno prikazana tendenca razvoja problema virusov skozi leta. Za razlago bom uporabljal še ugotovitve A. Coultharda in T. A. Vuorija v delu »Computer viruses: a quantitative analysis«.

2.2.1 Osnovne značilnosti raziskave

Raziskava podjetja ICSA leta 2001 je zavzemala vzorec 933.918 računalnikov in strežnikov. Vsi ti računalniki so bili kompatibilni z Intelovo tehnologijo. Raziskava je vključevala večja podjetja s po 500 ali več osebnimi računalniki, z dvema ali več lokalnimi omrežji in z dvema ali več dostopi na daljavo. Raziskava A. Coultharda in T. A. Vuorija pa je zavzemala manjši vzorec, ki je obsegal le 16 večjih podjetij z vsaj 10.000 osebnimi računalniki.

2.2.2 Ugotovitve raziskave

Od vseh organizacij, ki so sodelovale pri raziskavi, so se v obravnavanem obdobju vse vsaj enkrat srečale z virusom. Sodelujoče organizacije so v obravnavanem obdobju zabeležile 1.2 milijona okužb z virusi, kar prevedeno pomeni 113 okužb na 1000 računalnikov na mesec. Iz spodnje tabele je razvidno, kako se povečuje število okužb iz meseca v mesec čez opazovano obdobje.

Tabela 1: Mesečna stopnja okužbe na 1000 računalnikov

Leto	**Nov. – Dec.**
1996	10
1997	21
1998	32
1999	80
2000	91
2001	103
2002	105

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 9.

Zanimiv je tudi porast okužb iz leta 1998 na 1999, kar je v glavni meri posledica makro virusa imenovanega Melissa in izbruhu podobnih virusov in črvov, ki so se sami širili preko elektronske pošte.

V raziskavi so se tudi osredotočili na najpogostejše viruse, s katerimi se srečujejo podjetja. V tabeli 2 je vidno, s katerimi virusi so se najpogosteje srečevale organizacije v obdobju od januarja do decembra 2002.

Tabela 2: Najpogostejši virusi v letu 2002

	Ime Virusa	**Pogostost okužbe/1000 PCjev na mesec**
1	Klez	32
2	BugBear	29
3	BadTrans	22
4	Yaha	18
5	Sircam	12
6	Funlove	7
7	LoveLetter	6
8	Elkern	5
9	Magistr	4
10	Nimda	2

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 12.

Poudariti velja dejstvo, da je med desetimi najpogostejšimi virusi kar osem črvov, eden je makro virus (Elkern) in eden je datotečni virus.

Anketirance so vprašali tudi po zadnji hudi nesreči z virusi. Hudo nesrečo so definirali z vsako nesrečo, v kateri je bilo okuženih vsaj 25 računalnikov z istim virusom, in v približno istem časovnem obdobju, oziroma kot vsako nesrečo, ki je imela za posledico veliko denarno ali drugo škodo. Rezultati ankete so pokazali, da je od januarja 2001 skoraj tretjina (28%) anketirancev doživela hudo nesrečo, katere vzrok so bili virusi. Časovno so potekale nesreče tako, kot je prikazano v tabeli 3.

Tabela 3: Mesec zadnje hude nesreče

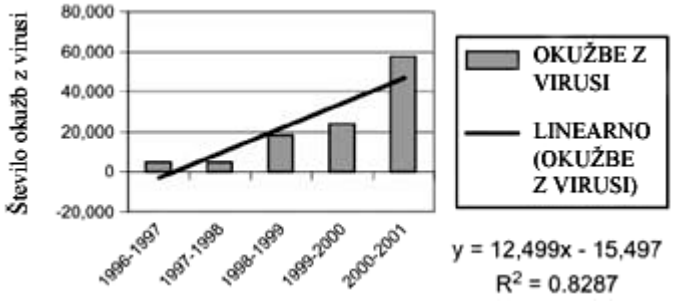
Mesec zadnje hude nesreče	%	n
December 2002	10	8
November 2002	9	7
Oktober 2002	25	20
September 2002	4	3
Avgust 2002	5	4
Julij 2002	5	4
April 2002	3	2
Marec 2002	5	4
Oktober 2001	14	11
September 2001	21	17

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 13.

Že ob prvem pogledu izstopata podatka za oktober 2002 in september 2001. Septembrske nesreče so bile v glavnem posledica pojave črva z imenom Nimda, oktobrske pa so bile posledica pet različnih virusov. V preteklosti ni bilo veliko hudih nesreč, povezanih z virusi, in sicer vse do marca 1999, ko se je pojavil makro virus Melissa. Od tega leta naprej se je pojavil vsako leto vsaj en resen virus, ki je povzročal hude nevšečnosti. Tako je Melissi sledil virus Loveletter leta 2000 in Nimda leta 2001.

Iz zgornjih podatkov in iz spodnje slike je razvidna velika stopnja povezanosti med okužbami z virusi in časom (koeficient korelacije R=0.91).

Slika 4: Število okužb z virusi (od maja 1996 do maja 2001)

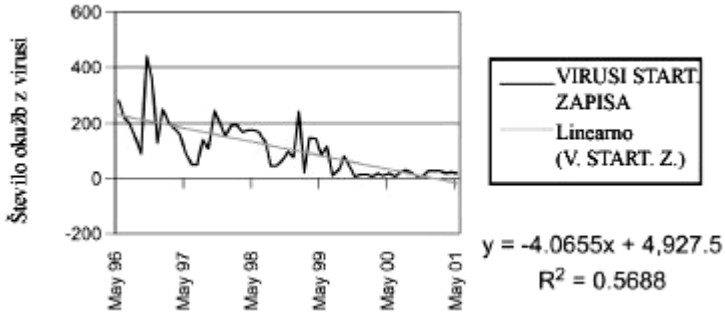


Vir: Coulthard, 2002, str. 402.

2.2.3 Virusi začetnega zapisa (boot sector virus)

Virusi začetnega zapisa so bili aktualni za čase DOS-a, ko se je v veliki meri še uporabljalo diskete za prenašanje podatkov, tako da je bilo v zadnjih petih letih opaziti znaten padec te vrste virusov. To je dobro razvidno tudi iz slike 5, ki kaže močen trend padanja števila virusov startnega zapisa z leti. To potrjuje tudi korelacijski koeficient (R= - 0,75).

Slika 5: Virusi startnega zapisa (od maja 1996 do maja 2001)



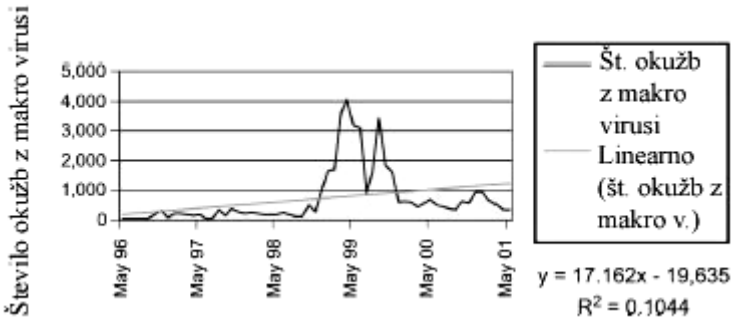
Vir: Coulthard, 2002, str. 403.

Kljub negativnemu trendu virusov startnega zapisa, so ti še vedno prisotni tudi v današnjih dneh. To pomeni, da bi bilo prenagljeno odpisati nevarnost, ki jo predstavljajo.

2.2.4 Makro virusi

Čeprav se veliko govori, da število okužb z makro virusi hitro narašča, statistične raziskave kažejo prej trend upadanja oziroma zelo slabe rasti. Iz slike 6 je razvidna šibka linearna povezanost naraščanja makro virusov z leti. Korelacijski koeficient je R=0,32, kar pomeni da gre za zanemarljivo pozitivno korelacijo med spremenljivkama. Na to oceno ima v veliki meri vpliv porast makro virusov leta 1999, sicer bi lahko govorili o trendu upadanja nesreč z makro virusi. Največje število okužb je bilo septembra leta 1999, ko so okužbe z makro virusi predstavljale veliko večino (90%) vseh okužb. To se je drastično spremenilo leta 2000 in 2001, ko so okužbe z makro virusi predstavljale le še slabo desetino (9%) vseh okužb.

Slika 6: Okužbe z makro virusi (od maja 1996 do maja 2001)



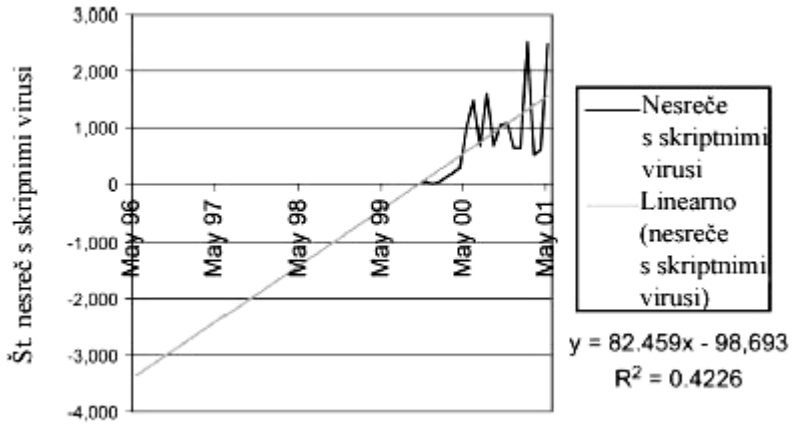
Vir: Coulthard, 2002, str. 403.

2.2.5 Skriptni virusi

Po podatkih protivirusnega proizvajalca Sophos (2000) je le 6% obstoječih virusov skriptnih virusov. Zanimivo je tudi, da teh 6% skriptnih virusov povzroča več kot tretjino vseh okužb z virusi. Vse te ugotovitve se kažejo tudi v stopnji, s katero naraščajo nesreče zaradi skriptnih virusov. Prvo poročilo o nesreči zaradi skriptnega virusa sega v oktober leta 1999 (Wildlist International, 2001) in od tedaj naprej se je število takšnih nesreč hitro povečevalo (glej sliko

4). V obdobju od maja 1999 do maja 2000 so skriptni virusi povzročili 3% nesreč, kar se je zelo spremenilo v obdobju od maja 2000 do maja 2001, ko so skriptni virusi povzročili več kot 21% vseh nesreč. Hitra stopnja rasti v številu nesreč, ki so jih povzročili skriptni virusi v zelo kratkem času, kaže na srednje do močno linearno povezanost rasti števila skriptnih virusov v času. To je vidno iz premice trenda in korelacijskega koeficienta (R= 0,65) s slike 7.

Slika 7: Nesreče s skriptnimi virusi (od maja 1996 do maja 2001)

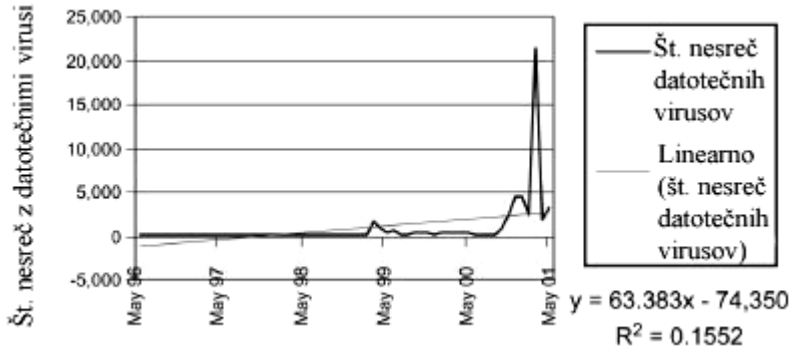


Vir: Coulthard, 2002, str. 404.

2.2.6 Datotečni virusi (file virus)

Datotečni virusi so edina zvrst virusov, ki je čez petletno opazovano obdobje številčno neprestano rasla. Kljub stalni rasti nesreč zaradi datotečnih virusov analiza trenda pokaže le zmerno linearno odvisnost naraščanja nesreč zaradi datotečnih virusov z leti. V tem primeru je korelacijski koeficient R= 0,39, kar je razvidno iz slike 8.

Slika 8: Št. Nesreč z datotečnimi virusi (od maja 1996 do maja 2001)



Vir: Coulthard, 2002, str. 405.

2.3 Opis nekaterih najbolj poznanih virusov

Število virusov narašča iz dneva v dan, kar pa pomeni, da so vsi enako nevarni in obstojni. Sledi opis nekaj najbolj znanih virusov, ki so se zapisali v zgodovino, bodisi zaradi okužbe zelo velikega števila računalnikov bodisi zaradi njihove časovne obstojnosti ali načina delovanja.

- *Cih (W95/cih.1003.A/Chernobyl)* se je pojavil 26. aprila 1998 in je bil prvi virus, ki je resno poškodoval strojno opremo računalnika. Napisal ga je taivanski programer Chen Ing-Hau za operacijski sistem Windows 95. To je datotečni virus, ki se sproži vsakega 26. aprila (kasneje vsakega 26. v mesecu – izpeljanke) v mesecu in uniči računalniški BIOS, tako da je računalnik neuporaben do njegove zamenjave. Virus okuži izvršilne datoteke, a pri tem ne spremeni njihove velikosti.
- *Melissa (W97M/Melissa.A@mm)* virus se je prvič pojavil marca 1999 kot delo 31 let starega ameriškega programerja Davida I. Smitha, ki ga je pustil v okuženem dokumentu (password.doc) na novičarski skupini »alt.sex.usenet«. To je bil eden od prvih virusov elektronske pošte, ki se je sam množično razpošiljal na prvih petdeset naslov v osebnem imeniku okuženega računalnika. Melissa je makro virus (Word 97 in Word 2000), ki se je zelo hitro širil, saj je prejemnik okuženega dokumenta mislil, da mu ga pošilja znanec in tako ni nič posumil.
- *CodeRed (NT/CodeRed.A) črv* se je pojavil avgusta 2001. Za razliko od ostalih črvov, je bil ta prisoten le v delovnem spominu (RAM-u) računalnika. Tako ni okužil nobene datoteke oziroma se ni nahajal na trdem disku računalnika. Večina programov danes deluje tako, da se ob zagonu naložijo v delovni spomin (memory resident) in so tam aktivni do prekinitve programa. Prav v tem je ključna razlika CodeRed virusa, ki je s tem v začetku povzročal velike težave protivirusnim programom. Črv se je zelo hitro širil po računalniških mrežah in izkoriščal pomanjkljivosti Windowsov 2000 oziroma internetnih strežnikov (IIS).
- *LoveLetter (VBS/LoveLetter.A@mm)* virus se je pojavil maja 2000 in se pot pretvezo ljubezenskega pisma zelo hitro razširil po celem svetu. To je skriptni črv napisan v Visual Basicu, ki se na okuženem računalniku, ki ima naložen Microsoftov Outlook, sam razpošlje naprej. Virus izvira iz Filipinov in se poslužuje radovednosti uporabnikov za svoje razširjanje, saj pošta, v kateri se skriva, nosi naslov »Love Letter« in s tem zlahka zavede naivnega uporabnika, da pogleda priponko.
- *Nimda (W32/Nimda.A@mm)* virus se je pojavil 18. septembra 2001. Zaradi svoje kompleksnosti, med drugim se tudi sam razpošilja preko elektronske pošte (priponka »readme.doc«), se je zelo hitro razširil po celem svetu. Nimda je prvi črv, ki je spremenil obstoječe spletne strani tako, da so začele ponujati okužene datoteke za prenos na osebni računalnik. Bil je tudi prvi, ki je uporabil navadne osebne računalnike za iskanje nezaščitenih internetnih strani, ki jih je nato okuži. Kompleksnost Nimdi omogoča, da okuži datoteke, se razpošilja prek elektronske pošte, okuži internetne strani in se širi tudi prek lokalnih mrež.

- *Sircam (W32/Sircam.A@mm)* črv sprva ni izgledal nevaren, saj je tipičen črv, ki se sam razpošilja prek elektronske pošte in ima fiksen del sporočila v pošti. Zaradi te lastnosti naj bi se ga hitro odkrilo in nevtraliziralo, a pokazalo se je, da je to eden od najbolj uspešnih črvov (najbolj razširjenih) doslej. To je vsekakor posledica lastnosti črva, da iz okuženega računalnika naključno izbere en dokument, ki ga pošlje kot priponko v elektronski pošti. Stranski učinek črva je seveda tudi velika možnost, da izbere kakšen zaupen dokument in ga nato pošlje naprej.
- *SoBig (W32.SoBig.F@mm)* črv se je pojavil 18. avgusta 2003 in je povzročil kar precej razburjenja tudi v Sloveniji, saj je to sodoben virus, ki pobrska po imeniku okuženega računalnika, nabere naslove in se začne razpošiljati nanje. Razburjenje pa je povzročila specifičnost tega virusa, ki podpisuje naslovnike med sabo in nikoli ne podpiše dejansko okuženega računalnika (lastnika). Vse to je v kar nekaj primerih pripeljalo do navzkrižnega obtoževanja resnično nedolžnih. Med drugim lahko ta virus tudi ukrade nekatere sistemske informacije in gesla.

2.4 Napovedi za prihodnost

Večina podjetij, ki izdelujejo protivirusne programe in strokovnjakov meni, da bodo virusi tudi v prihodnje povzročali veliko težav. Spremembe so in bodo zagotovo opazne tudi v prihodnje v prevladovanju nesreč zaradi določene podskupine virusov. Kot kažejo raziskave, bo število virusov startnega zapisa vedno manjše, kar je predvsem posledica sprememb v operacijskih sistemih. Število makro virusov bo še vedno naraščalo, le da se je ta rast glede na pretekla leta zelo upočasnila. Nekateri skriptni jeziki so jasno pokazali, da imajo vse potenciale, da lahko tudi v prihodnje povzročajo veliko varnostnih težav. To pomeni, da bodo skriptni virusi povzročali veliko problemov tudi v prihodnje. Zadnja leta kažejo ponovno rast datotečnih virusov in črvov, ki so bili v preteklosti že v zatonu. K temu so v glavnem pripomogle nove tehnologije prenosa podatkov in novi, naprednejši programi.

Večina informacijskega okolja se zelo hitro spreminja. Pojavljajo se novi standardi, rešitve, programska in strojna oprema, kar pa v sebi prinaša tudi nove možnosti za zlorabo. Tudi internet kot okolje postaja vedno bolj kompleksen in povezan, kar nedvomno odpira vrata zlonamernim programerjem. Kako bodo spletni teroristi zlorabili vse pomanjkljivosti, je skoraj nemogoče predvideti. Velika verjetnost je, da bo naslednja velika virusna epidemija posledica neke nove tehnologije ali programske opreme, ki so zadnje čase vedno slabše preizkušene (npr. Windowsi XP ob izidu).

3. VIRUSI IN OCENA VPLIVA NA POSLOVANJE PODJETJA (ORGANIZACIJE)

S hitrim razvojem novih tehnologij in z njihovim naraščajočim uporabljanjem v vsakdanjem poslovanju organizacij, se je vsekakor povečala njihova učinkovitost. To potrjuje tudi trud in velike finančne investicije podjetij v tehnološki razvoj, saj le tako lahko ostanejo konkurenčna na trgu. Vzporedno s tehnološkim razvojem in razvojem programske opreme je potekal tudi razvoj škodljive programske kode – virusov. Prav ta je drastično spremenil poslovanje podjetij v zadnjih letih in pokazal tudi na slabe plati tehnološkega razvoja, ki je sprva obljubljal le koristi. Podjetja so tako dolžna poskrbeti za varnost svojih računalniških sistemov in za zaupnost podatkov, kar nedvomno zahteva dodatne finančne vložke v usposabljanje zaposlenih in nabavo ustrezne protivirusne programske in strojne opreme.

3.1 Resnost problema

Skoraj ni več dne, da ne naletimo v medijih na kakšno novico o nesrečah v organizacijah, katere vzrok so bili virusi. Problem virusov pa ne zadeva zgolj velikih organizacij, temveč prav vsa podjetja, od najmanjših do največjih in tudi osebnih uporabnikov. Seveda je škoda, ki jo utrpijo velika podjetja, veliko večja od škode v malih podjetjih in zaradi tega deležna večje medijske pozornosti. Pomembno je dejstvo, da skorajda ni več podjetja, katerega poslovanje ne bi bilo odvisno od računalnika in elektronskega omrežja (ne glede na tip). Ta univerzalna odvisnost podjetij od računalnikov obenem pomeni, da je domala vsako podjetje v nevarnosti pred okužbo, ki lahko pripelje do velikih nevšečnosti. Podjetje lahko zaradi okužbe z virusi bodisi začasno preneha s poslovanjem, bodisi utrpi na ugledu v javnosti, izgubi pomembne podatke itd.. To so le nekateri od mnogih problemov, s katerimi se srečujejo podjetja, ki privedejo do odziva podjetij na krizno situacijo. Odzivna strategija je zagotovo zelo draga za podjetje in le redkokdaj celovito uspešna. Boljša je preventivna strategija, saj je v večini primerov uspešnejša in veliko cenejša.

Iz spodnje tabele so vidni učinki virusov na organizacijo in zaposlene. Anketirana podjetja so bili vprašana po najpogostejših posledicah okužbe z virusi. Na razpolago so imeli več odgovorov, zato vsota odstotkov ni 100.

Tabela 4: Učinek virusov

Odgovori	%	n
Izguba produktivnosti	75	230
Računalnik je bil neuporaben	69	212
Pokvarjene datoteke	62	190
Nedostopnost podatkov	49	150
Izgubljeni podatki	47	143
Izguba uporabnikovega zaupanja	33	102
Motnje, zaklepanje	18	54
Nezanesljive aplikacije	13	40
Težave s prebiranjem datotek	12	37
Težave s shranjevanjem datotek	9	29
Zamrznitev sistema	9	28
Težave s tiskanjem	7	21
Grožnja izgube službe	2	6

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 23.

Iz ankete je razvidno, da posledice okužbe z virusi ne zadevajo le izgub denarja, resursov in časa, potrebnega za obnovitev predhodnega stanja, ampak so posledice veliko širše in včasih nenapovedljive.

Problem virusov in varnosti podatkov je zelo resen in to dokazuje tudi dejstvo, da je vsaj protivirusni program postal del osnovne opreme skoraj vsakega računalnika, ki služi za poslovne namene. To pa še zdaleč ni dovolj za celovito preprečitev okužb, vendar je le začetek preventive in boja proti virusom. Zavedanje resnosti problema je vsekakor primarnega pomena za uspešno preventivo.

3.2 Finančna plat virusov v podjetju

Kljub temu, da se je zavedanje problema virusov v zadnjih leti zelo povečalo, je škoda, ki jo povzročijo virusi, vsako leto še vedno zelo velika. Temu pripomore v veliki meri iznajdljivost programerjev, ki odkrivajo nove metode delovanja virusov, podcenjevanje nevarnosti in v veliki meri tudi naivnost (neizobraženost) uporabnikov. Na to kaže tudi nedavna raziskava (10.9.2003) podjetja Panda Software, ki je pokazala, da 38 odstotkov sodelujočih v anketi verjame, da ne potrebujejo zaščite, saj ne uporabljajo veliko interneta, obiskujejo samo zaupanja vredne strani in izmenjujejo elektronsko pošto samo s sorodniki ali prijatelji. Podobne trende je odkrila tudi raziskava ponudnika internetnih storitev BT Openworld, ki je pokazala, da skoraj tretjina (28%) britanskih malih podjetij meni, da protivirusni programi in požarni zidovi niso pomembni.

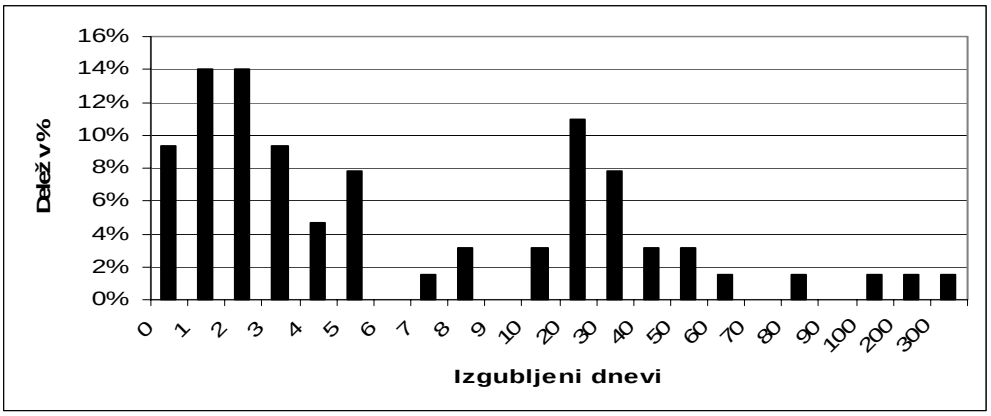
Pomanjkljiva osveščenost je eden primarnih vzrokov nezadostne IT (informacijsko tehnološke) varnosti. Stanje po različnih državah Evrope je, kot je pokazala mednarodna raziskava, ki jo je izvedla Panda Software, različno. Medtem ko ima v Španiji komaj nekaj

več kot tretjina podjetij pravilno nameščen in posodobljen protivirusni program, so rezultati za Italijo in Francijo še veliko slabši – manj kot četrtina oziroma petina podjetij. Posledice dejstva, da je v današnjem nevarnem okolju, ki ga predstavljajo računalniški virusi, toliko računalnikov brez zaščite, lahko boleče občuti veliko malih in srednjih podjetij. Obširna epidemija uničevalnih zlonamernih kod lahko uniči podatke, prizadene produktivnost in povzroči škodo ugledu podjetja v primeru, da podjetja nehote širijo viruse svojim strankam in drugim. Stroškovni vidik virusov pa predstavlja bodisi odpravo posledic okužbe v organizaciji, bodisi nabavo ustreznega zaščitnega sistema. Izkušnje organizacij kažejo, da je vsekakor ceneje vzpostaviti ustrezne zaščitne mehanizme, kot pa odprava posledic okužbe z virusi.

3.2.1 Izguba kot posledica okužbe z virusi

Čeprav se je osveščenost glede problematike virusov v zadnjih letih zelo povečala, ostajajo izgube še vedno na zelo visoki ravni. Na to opozarja tudi podatek, da so virusi globalni ekonomiji povzročili za okoli 12 milijard škode v prvih šestih mesecih leta 2000 (Norman, 2002: 38). Ta podatek nam jasno kaže, da je treba še veliko postoriti glede zaščite pred virusi. Iz ankete skupine ICSA Labs (slika 9) je razvidna kumulativa izgubljenih dni po osebi zaradi okužbe z virusi.

Slika 9: Vsota izgubljenih dni po osebi na podjetje izražena v odstotkih



Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 21.

Iz slike je jasno razvidno, da je večina podjetij izgubila tja do pet delovnih dni, oziroma da je 62 odstotkov anketirancev zaradi okužbe z virusi izgubilo manj kot deset dni. Seveda je bilo tudi nekaj večjih podjetij, ki so v kumulativi izgubila tja do tristo delovnih dni, tako da se je povprečni čas za ponovno vzpostavitev normalnega delovanja podjetij premaknil na triindvajset (delovnih dni) dni po osebi.

Slika 10: Stroški na podjetje v dolarjih

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 22.

Anketirance so vprašali tudi o oceni škode, izražene v dolarjih. V oceno, so jih zaprosili, naj vključijo tudi stroške izgubljenega delovnega časa, nadur, potrebnih za ponovno vzpostavitev normalnega delovanja sistemov, izgubljenih priložnosti itd. Rezultati ankete (slika 10) so pokazali, da je v povprečju strošek odprave posledic okužbe z virusi znašal nekaj več kot 81.000,00 dolarjev, medtem ko je mediana stroškov znašala 9.500,00 dolarjev in najpogostejši odgovor je bil 10.000,00 dolarjev. Opazne so velike razlike med povprečnimi stroški, mediano in najpogostejšim odgovorom, kar pa je v glavnem posledica nekaj velikih podjetij, ki so zabeležila stroške, ki so presegali 1.000.000,00 dolarjev. Ne glede na to, da so povprečni stroški okužbe in odprave posledic virusov rahlo pretirani zaradi vpliva velikih podjetij, vseeno ugotavljam, da ostajajo stroški okužbe za podjetje zelo visoki.

3.2.2 Stroškovna plat preprečevanja

Kot smo videli, so lahko stroški okužbe z virusi zelo visoki in vredno je razmisliti o ustrezni zaščiti ter seveda o njeni stroškovni upravičenosti. V zdajšnjih časih, ko se nevarnost in škoda, ki ju povzročajo virusi, povečujeta iz leta v leto, je zaščita nujnost vsakega resnega podjetja. Poudariti velja, da je kljub še tako dobri zaščiti podatkov, grožnja okužbe z virusi vedno prisotna, saj nobena zaščita sistema ni popolna, še manj pa znanje uporabnikov, ki ga uporabljajo. Zaradi nepopolnosti varnostnih mehanizmov si velja v organizaciji najprej zamisliti sistem varnostnega arhiviranja pomembnih podatkov. Varnostne kopije pomembnih podatkov so najboljša zaščita pred virusi, okvarami strojne opreme, programskimi hrošči in pred naravnimi katastrofami. Na trgu obstaja kopica rešitev za varnostno arhiviranje podatkov, tako da se lahko podjetje odloči za ZIP enote, ki stanejo okoli 20.000 SIT, prenosne trde diske, katerih cena se giblje od 30.000 SIT navzgor, posebne magnetne kasete ali pa za snemalnike CD-ROM, ki imajo ceno od 10.000 SIT navzgor in katerih mediji so zelo poceni. Zelo hitro se uveljavljajo tudi zapisovalniki DVD-ROM, na katere lahko zapišemo še večjo

količino podatkov kot na navadne CD-je. Cena DVD-R enot je v zadnjem letu zelo padla, tako da lahko dobimo snemalnik že za 40.000 SIT.

Ob rednem arhiviranju podatkov je zelo pomembna tudi namestitev protivirusnega programa, ki preprečuje, da bi do okvar v sistemu sploh prišlo. Na trgu se je uveljavilo kar nekaj protivirusne programov. Med najbolj znanimi so Norton Antivirus (www.norton.com), McAfee Virus Scan (www.mcafee.com), Trend Micro PC-cillin (www.trendmicro.com), F-Secure (www.fsecure.com) in Sophos Anti-Virus (www.sophos.com). Cene protivirusnih programov se gibljejo od 16.000 do 25.000 SIT, oziroma od 6.000 do 10.000 za OEM različice. Vsi ti programi omogočajo tudi redno brezplačno nameščanje popravkov z interneta za zaščito pred novimi virusi, kar pa v večini primerov traja le eno leto. Po poteku tega obdobja je treba kupiti novo različico protivirusnega programa, oziroma nadgradnjo, ki predstavlja ponoven strošek za podjetje.

K stroškovni plati preprečevanja okužb z virusi sodi tudi izobraževanje kadrov, ki mora potekati kontinuirano. V tem primeru so stroški od podjetja do podjetja zelo variabilni in prepuščeni presoji vodilnih v podjetju. Velja pa si zapomniti, da je velikemu deležu okužb v podjetjih botrovalo prav neznanje zaposlenih in ne neprimerna programska zaščita. Oglejmo si malo banalen primer, ki se je zgodil tudi v Sloveniji: Po elektronski pošti je krožila potegavščina (hoax), ki je uporabnike svarila naj pregledajo mapo C:\Windows\ in naj v primeru, če najdejo datoteko XY v njej, to nemudoma zbrišejo, ker imajo virus. Kljub temu, da se veliki večini uporabnikov zdi to zelo smešno, se je dejansko zgodilo, da so nekateri uporabniki zbrisali sistemsko datoteko in si tako sami onesposobili sistem. Zato velja, da je investicija v izobraževanje zaposlenih vedno ekonomsko upravičena, čeprav se zdi velikokrat odvečna.

4. PREPREČEVANJE, ODKRIVANJE IN ODPRAVA VIRUSOV

Že od nekdaj velja, da se najbolje zaščitimo pred virusi, če računalnika ne povezujemo z drugimi računalniki, niti prek modema niti v mrežo, in nanj ne nameščamo nobenih novih programov. Vendar je to v današnjih časih skoraj nemogoče, zato je bolje, da vzpostavimo dobre zaščitne postopke, ki bodo preprečevali oziroma odpravljali posledice okužb z virusi. Če organizacija nima rutiniranih postopkov upravljanja s podatki in nevarnostmi, ki jim pretijo, je verjetnost, da bo okužba z virusi povzročila škodo velikih razsežnosti, zelo visoka. V nasprotnem primeru, ko ima organizacija postopke in strategije jasno izdelane, se verjetnost okužbe zelo zmanjša oziroma je odprava posledic učinkovitejša. Zavedati se je treba, da je tudi ob uporabi najboljših protivirusnih programov možnost okužbe še vedno prisotna, saj predstavlja programska oprema le del zaščitne politike podjetja. Prav jasno definirani postopki ukrepanja oziroma politika organizacije so primarnega pomena za učinkovit boj proti virusom. Veliko vlogo pri preventivi predstavlja tudi sprotno izobraževanje zaposlenih o nevarnostih, ki pretijo organizaciji.

4.1 Kje najpogosteje naletimo na viruse?

Poti, po katerih lahko virusi okužijo računalnik, je pri sedanji tehnologiji ogromno oziroma vedno več. Tako lahko dobimo virus, ko brskamo po internetu, ko pregledujemo elektronsko pošto, ko prenašamo programe s spleta, ko nameščamo novo – okuženo programsko opremo, ko vstavimo v računalnik okužen medij itd. Če je v preteklosti veljalo, da so največji vzrok okužbe računalnikov v domačem okolju, mnogokrat pa tudi v podjetjih, otroci, ki so nameščali okužene računalniške igrice, se je trend vira okužbe v zadnjih letih temeljito spremenil. To je jasno pokazala tudi raziskava podjetja ICSA Labs, pri kateri so preverjali vire okužbe sistemov v zadnjih letih (tabela 5).

Tabela 5: Viri okužbe z virusi v odstotki, 1996-2002

Vir okužbe	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**
Priponke v e-pošti	9	26	32	56	87	83	86
Prenašanje prog. s spleta	10	16	9	11	1	13	11
Brskanje po spletu	0	5	2	3	0	7	4
Neznan izvor	15	7	5	9	2	1	1
Distribucija prog.	0	3	3	0	1	2	0
Diskete: drugi mediji	71	84	64	27	7	1	0

Vir: ICSA Labs Virus Prevalence Survey 2002, 2003, str. 24.

Anketirance so vprašali po izvoru njihove zadnje okužbe z virusi. Tudi v tem primeru je vsota po posameznih letih večja od sto odstotkov, saj so lahko anketiranci navedli več izvorov okužbe. Iz ankete je razvidno, da je število okužb prek priponk v elektronski pošti naraščalo iz leta v leto, z izjemo leta 2001, ko je zaznati zanemarljiv padec. Očiten je tudi znaten padec okužb z virusi začetnega zapisa, ki so se prenašali v veliki meri preko disket, in se leta 2002 niso več pojavili v anketi. Okužbe, katerih izvor je bilo brskanje po spletu in prenašanje raznih datotek iz spleta, so se gibale v konstantnih mejah tja do 7% pri brskanju po spletu, oziroma do 16% pri prenašanju datotek. Upal pa bi si trditi, da bodo podatki za leto 2003 pokazali velik porast okužb, katerega izvor je brskanje po spletu, saj se je že v prvi polovici leta 2003 pojavilo kar nekaj takih virusov, ki so izkoriščali varnostne luknje programske opreme (npr. črv SoBig).

Zgornje ugotovitve morajo služiti organizacijam kot svarilo, kam vlagati vire za preventivo in na kaj je treba še posebej opozoriti uslužbence za uspešen boj proti virusom. To pomeni, da je opravilom z elektronsko pošto treba določiti jasne smernice uporabe, oziroma kaj lahko in česa ne smejo, kadri početi pri uporabi elektronske pošte.

4.2 Protivirusni postopki

Od prvega virusa v osemdesetih letih pa vse do danes je število virusov naraščalo z eksponentno funkcijo. Na srečo je vzporedno z nastajanjem virusov potekal tudi razvoj podjetij, ki so se ukvarjala s to problematiko. Veliko jih je v dolgotrajnem, stroškovno dragem in tehnično zahtevnem boju z virusi propadlo, nekatera pa so le uspevala in so tako prisotna na trgu še danes ter njihove rešitve uporablja veliko število uporabnikov. Za vsa ta podjetja so značilni nekateri skupni postopki ukrepanja pri problemih, povezanih z zaščito pred računalniškimi virusi. Med te postopke sodijo:

- *Pregledovalniki (ang. scan)*, ki so najbolj razširjena vrsta protivirusnih programov. Njihov princip delovanja je zelo preprost in temelji na primerjavi seznama virusnih kod, ki jih primerja s kodami virusov, prisotnimi v delovnem pomnilniku, na disku v računalniku ali na katerem drugem mediju (disketa, CD itd.). Vsak virus ima namreč v sebi zapisanih nekaj ukazov in podatkov, ki so značilni samo zanj ali za njegove izpeljanke. Ko pregledovalnik naleti na kodo virusa, ki ustreza eni od kod, shranjenih v seznamu protivirusnega programa, za trenutek zaustavi delovanje računalnika, uporabniku pa sporoči svoje odkritje. Ti programi delujejo tako, da najprej pregledajo računalnikov delovni pomnilnik (virus se tu najprej pojavi), nato preverijo začetni zapis, kasneje pa še sistemske in izvršilne datoteke. Pred leti je bila slabost teh programov ta, da so morali imeti vsakokrat na voljo najnovejše verzije pregledovalnikov, ki imajo v svojih seznamih zapisane tudi kode najnovejših virusov. V nasprotnem primeru niso služili odkrivanju novih virusov (Mrhar, 1995, str. 42). Danes, ko je navadna internetna povezava v domeni vsakogar za majhne stroške, pa se pregledovalniki v večini primerov posodabljajo sami, vsakič, ko se povežemo na internet, in imajo tako vedno na razpolago kode najnovejših virusov, ki jih je protivirusno podjetje (programska hiša) odkrilo.
- *Stalno prisotni detektorji,* za katere je značilen nenehen nadzor nad delovanjem računalnika. Programi so namreč vedno prisotni (rezidenčni) v računalnikovem delovnem pomnilniku, kjer se stalno izvajajo. Detektor pregleda vsako datoteko, s katero delamo. Običajno lahko preprečimo še zapisovanje podatkov v začetni zapis na trdem disku ali disketi, onemogočimo pisanje v izvršilne ali sistemske datoteke, prepovemo formatiranje diska in podobno. Kadar pride do kršenja zgoraj naštetih prepovedi, nas program na to opozori in vpraša, ali želimo določen ukaz vseeno izvesti ali ne. Najpogosteje velja, da v primeru, ko uporabnik ni programer, naj ne bi pisal po izvršilnih in sistemskih datotekah ali po startnem zapisu diska. Slaba lastnost rezidenčnih detektorjev je, da precej upočasnijo delovanje sistema (saj istočasno deluje več programov), včasih pa tudi v prestrogem nadzoru računalnika. Če namreč prepovemo kakršnokoli pisanje v računalniški spomin, nas bo program ob zapisovanju poljubnih (npr. poslovnih) podatkov opozoril na delovanje detektorja. Te prekinitve so za uporabnika marsikdaj moteče, tako da izklopi sistem nadzora. V tem primeru imajo virusi prosto pot za širjenje in razmnoževanje po računalniku (Mrhar, 1995, str. 43).
- *Detektor sprememb* je program, ki si zapiše kontrolne podatke o datotekah v isti imenik na disku, kjer so te datoteke shranjene. Kontrolni podatek o datoteki je pogosto sestavljen iz

matematične kombinacije, ki upošteva uro in datum nastanka datoteke, njeno dolžino in podobno, te vrednosti pa se ob okužbi spremenijo. Ko detektor sprememb naslednjič preveri datoteke in ugotovi spremenjeno vrednost kontrolnega podatka, nam to sporoči in nas opozori, naj preverimo, ali je morda prišlo do okužbe z virusom. Med glavne slabosti teh programov sodi obremenitev računalnika z novimi datotekami, v katerih so zapisane vrednosti nadzorovanih podatkov. Ti programi tudi ne ločijo med virusi in običajnimi ukazi, zato velikokrat prekinejo naše delo. Prednosti teh so v sprotnem obveščanju o vsaki spremembi v datotekah, kar pomeni, da nam nudijo zaščito tudi pred novimi virusi, ki jih programske hiše še niso odkrile. Težave nastopijo le pri skrivnih virusih (ang. stealth viruses), ki prestrežejo ukaze o kontroli datotek (Mrhar, 1995, str. 44).

4.3 Zaščita pred virusi

Za zagotovitev splošne zaščite pred napadi računalniških virusov in ostalimi varnostnimi grožnjami, ki pretijo sistemu, morajo poslovodje skupaj z zaposlenimi odstraniti oziroma kar se da zmanjšati ranljivost sistema. Glavne točke ranljivosti sistemov so v večini primerov naslednje:

- *Pomanjkljivo zavedanje problema s strani uporabnikov* – uporabniki kopirajo in delijo okuženo programsko opremo, ne zaznajo simptomov okužbe računalnika in ne razumejo dobro varnostnih prioritet. To izhaja predvsem iz dejstva, da večina uporabnikov ni strokovno dovolj podkovana o varnosti in zaščiti računalniških sistemov. V praksi tudi ni potrebe po temu. Minimalna pozornost za osnove varnosti je vseeno zaželena tudi iz strani navadnih uporabnikov, če je naš cilj preprečiti okužbe z virusi. Ta minimalna pozornost zahteva, da uporabniki poznajo dejavnike, ki lahko spravijo sistem v nevarnost. Seznanjeni morajo biti s tem, kaj lahko in česa ne smejo na računalniku početi. Tak primer predstavlja elektronska pošta, ko uporabniki odpirajo vse priponke, ki pa so eden glavnih virov okužb (Jackson, 2001, str. 2).
- *Neažurirana baza poznanih virusov* – glede na karakteristiko pojavljanja novih virusov je pogost pojav, da zaščitne (prepoznavne) kode virusov protivirusna podjetja objavijo z rahlim zamikom. Po drugi strani je tudi pogost pojav, da sami uporabniki ne nameščajo popravkov za protivirusni program s spleta dovolj pogosto. To pa omogoča novim virusom prosto pot do naših računalnikov.
- *Izklopljen protivirusni program* – vsak uporabnik ima možnost izklopiti protivirusni program, kot tudi sposobnost, da na svoj računalnik namesti nove necertificirane aplikacije, kar lahko pripelje do okužbe. Tudi ta primer potrjuje potrebo po jasno definiranih pravilih ustrezne uporabe računalnika v podjetju.
- *Pomanjkljiva varnostna politika podjetij in odsotnost kriznega načrta* – vsako resno podjetje bi moralo imeti izdelan krizni načrt, ki določa odgovornosti zaposlenih v primeru okužbe z virusi in postopke ukrepanja. Krizni načrt mora biti nujni sestavni del varnostne politike vsakega podjetja.

- *Pomanjkanje, oziroma neustrezna varnostna kontrola* – Še vedno je veliko podjetij, ki se ne zaveda resnosti problema varnosti podatkov. To se kaže v tem, da ne uporabljajo nobene programske in strojne zaščite, ki bi preprečevala okužbe računalniških sistemov.
- *Varnostne luknje in hrošči programske opreme* – v zadnjih časih je pogost pojav, okužba računalniških sistemov kljub nameščeni protivirusni programski opremi. V tem primeru so avtorji virusov izkoristili varnostne pomanjkljivosti programske opreme (npr. virus Blaster – win Xp in win 2000). Zato je primarnega pomena nameščanje popravkov programske opreme, ki jih programske hiše redno izdajajo.

4.4 Neznani virusi

Marsikdaj se računalnik okuži z virusom novejše izdelave, tako da ga program za iskanje virusov ne more odkriti. Če ne uporabljamo detektorja sprememb, je zelo koristno prepoznati vsaj nekaj znakov, ki kažejo na to, da je v našem računalniku prišlo do okužbe z virusom. Znaki okužbe so lahko:

- Upočasnjeno delovanje računalnika oziroma izvajanje programov, ki se v najslabšem primeru lahko celo zaustavi.
- Velikost datotek (predvsem izvršilnih s podaljškom .COM in .EXE) se nenadoma podaljša. Datoteke imajo spremenjen datum in uro svojega nastanka.
- Trdi disk ali disketna enota delujeta (prižiga se lučka), čeprav jih ne uporabljamo. Včasih se lahko pojavi sporočilo, da nekega programa ni mogoče kopirati, čeprav ničesar ne kopiramo. Tako sporočilo nastane zaradi prikritega ukaza virusa, ki se želi reproducirati.
- Na zaslonu se dogajajo nenavadne stvari, kot je izpisovanje sporočil, izginjanje črk, glasba itd.
- Računalnik se samodejno izklaplja (resetira) ali pa se njegovo delovanje brez vzroka zaustavi.

4.5 Ukrepanje ob pojavi virusa

Ob spoznanju, da se je v računalniku naselil virus, je bistvenega pomena hitro ukrepanje, saj virus zlahka izkoristi vsak zamujeni trenutek za svoje razmnoževanje, če ne celo za uničevanje podatkov. V takem primeru se izkaže koristnost kriznega načrta, ki mora določati naslednje:

- Odgovorno osebo ali skupino ljudi (formalno ali neformalno določeno), ki so pooblaščeni za ukrepanje ob pojavu okužbe.
- Postopke za odkrivanje okuženih računalnikov in načina okužbe.
- Navodila, kako izolirati okužene računalnike od ostalih računalnikov, dokler se s teh ne odstrani vseh virusov.
- Poti obveščanja uporabnikov, katerih računalniki so morda tudi okuženi z virusom, in postopke, kako naj ti preprečijo nadaljnjo širjenje virusa.
- Postopke za odstranitev virusov iz okuženih računalnikov.

- Navodila za prepoznavanje virusa odgovornega za okužbe in njegovih specifičnih lastnostih. Tu mislim predvsem na pomanjkljivosti v sistemu, ki jih je virus izkoristil, da je lahko prišlo do okužbe.

Za osebnega uporabnika, ki se sreča z virusom, je najpomembnejše, da hitro sledi naslednjim navodilom:

- Zaključi naj delo z aplikacijami, v katerih se nahaja, in če je povezan v mrežo, naj to povezavo čim prej izklopi (najhitreje se to lahko stori s fizičnim izklopom omrežnega priklopa).
- Vključi naj program za iskanje in odpravo virusov. V veliki večini primerov ostalo opravi protivirusni program sam. Lahko pa se zgodi, da protivirusni program kakšne okužene datoteke oziroma virusa ni sposoben popraviti (odpraviti) in nam tako ponudi, da okuženo datoteko izbrišemo ali damo v karanteno. V karanteno je smiselno dati okuženo datoteko le, če nam je ta nujnega pomena, saj v tem primeru upamo, da bo v bližnji prihodnosti programska hiša (protivirusno podjetje) razvila popravek, ki bo omogočal odstranitev virusa z okužene datoteke (datoteke v karanteni). Pogost je tudi pojav, ko virus okuži tudi protivirusni program in sistemske datoteke, kar pa nam onemogoča odstranitev virusa z računalnika oziroma zagon računalnika. Za take primere nam protivirusni programi ob namestitvi ponujajo možnost izdelave varnostnih disket, ki vsebujejo sistemske datoteke, podatke o disku in particijah, protivirusni program in definicije virusov. S temi disketami lahko zaženemo računalnik in odstranimo viruse, ki jih sicer ne bi bili sposobni.
- Ko s postopkom čiščenja virusov zaključi, je priporočljivo, da uporabnik računalnik izklopi in znova zažene program za iskanje virusov. Če je virus še vedno prisoten, je treba ponoviti zgornje postopke oziroma uporabiti varnostne diskete.
- Če se virus ponovno pojavi, je priporočljivo poiskati informacije o pravilnem odstranjevanju in zaščiti na spletni strani proizvajalca protivirusne programske opreme. Tak primer je bil z virusom Blaster, ki ga je protivirusni program zaznal, a ga nikakor ni mogel odstraniti. V tem primeru je bilo treba obiskati spletno stran proizvajalca protivirusne programske opreme, s katere smo lahko prenesli poseben program, ki je virus odstranil. Dobili smo tudi informacije o varnostni luknji operacijskega sistema, ki je omogočala vdor virusa in o spletni strani, s katere smo lahko pobrali popravek za operacijski sistem.
- Po odstranitvi virusa z računalnika je pomembno, da uporabnik pregleda tudi vse medije(diskete, cd-je itd.), ki jih uporablja in se tako prepriča, da niso ti vir okužbe.

4.6 Protivirusna politika podjetja

Že večkrat sem omenil, da je za zaščito pred virusu zelo pomembno, da imamo izoblikovana protivirusna pravila, ki sicer samostojno ne morejo sama preprečiti možnosti okužbe računalnika, temveč ob doslednem upoštevanju vseh pravil hkrati, lahko njihov sinergičen

učinek zelo pripomore pri preprečevanju okužbe računalnika. Podjetje TruSecure svetuje uporabo naslednjih pravil, ki so primarnega pomena za varno delo:

1) Namestitev priznane in certificirane protivirusne programske opreme na vse računalnike v podjetju.
2) Prijavo v novičarsko skupino kot je npr. TruSecure Monitor(Virus Bulletin itd.), ki nas obvešča o novih virusih in zaščito pred temi.
3) Če nam programska oprema omogoča sprotno posodabljanje baze poznanih virusov s spleta, moramo to storiti vsaj enkrat mesečno, oziroma v najmanj dveh dneh po prejetem svarilu novičarske skupine (Posodabljanje baze poznanih virusov ni dovolj, če uporabljamo staro verzijo protivirusnega programa.)
4) Če sprotno posodabljanje prek spleta ni omogočeno, moramo to storiti vsakič, ko nam proizvajalec pošlje popravke.
5) Usposabljanje zaposlenih za pravilno posodabljanje baze poznanih virusov.
6) Priporočene nastavitve protivirusnega programa:
    a) Neprekinjeno delovanje protivirusnega programa v ozadju (real time) mora biti VKLJUČENO;
    b) Pregledovanje delovnega spomina, zagonskih in sistemskih datotek – VKLJUČENO;
    c) Nastavitev programa, da pregleduje VSE datoteke – VKLJUČENA;
    d) Vklopljen mora biti tudi dnevnik, ki beleži vse okužbe oziroma poskuse okužb z virusi.
7) Priporočljive varnostne nastavitve operacijskega sistema, ki so povezane z virusi:
    a) Zagotovitev namestitve vseh varnostnih popravkov operacijskega sistema.
    b) Namestitev le nujnih (osnovnih) komponent operacijskega sistema, saj virusi velikokrat izkoriščajo pomanjkljivosti dodatnih komponent.

Podjetje TruSecure priporoča tudi naslednje nastavitve programske opreme (zaželena je uporaba čim večjega števila teh nastavitev za učinkovito sinergijo) :

1. Nastavitev MS Worda, da shranjuje vse tekste v obliki *.RTF (rich text format), saj se lahko na tak način enostavno izognemo makro virusom.
    - Dokumente moramo shraniti v obliki RTF in ne samo spremeniti oznake iz DOC v RTF – učinek ni enak.
    - Uporabnikom je lahko izjemoma dovoljeno, da dokument shranijo v obliki *.DOC le v primeru, ko morajo ti zmanjšati velikost datoteke in so v dokumentu uporabljeni kompleksni makro ukazi. V vseh ostalih primerih morajo biti dokumenti shranjeni v obliki *.RTF.
2. Vključitev zaščite pred makro virusi v aplikacijah MS Office.
3. Nastavite WordPad ali WordView kot privzete programe za dokumente tipa *.DOC.
4. Izogibajmo se dvojnemu kliku na priponke v prispeli elektronski pošti. Če dobimo v elektronski pošti dokument ali razpredelnico, ki bi ga radi pregledali, ga ročno odpremo z WordPadom, WordViewem ali s kakšno drugo aplikacijo. Če se priponka izkaže kot izvršilni program (EXE, COM itd.) je nikoli ne zaženemo, čeprav nam to

svetuje sporočilo. Zapomniti si velja, da ne odpiramo priponk na sporočilih, ki jih ne pričakujemo.
5. Uporabljajmo protivirusne hevristične kontrole (kjer so omogočene).
6. Nastavite lastnosti za datoteke tipa *.EXE *.DLL v sistemskih mapah, da je omogočeno le branje teh datotek (read only). Sistemske mape so navadno C:\WINDOWS (za Win 98 in Win XP) in c:\WINNT (za Win 2000 in Win NT).
7. Nastavimo protivirusni program naj onemogoči oziroma obvesti ob vsakem poskusu spreminjanja lastnosti datotek pri katerih je omogočeno le branje(read only).

Nastavitve poštnih odjemalcev:
1. **Outlook (Microsoft)**:
    a. Nastavite varnostne nastavitve Internet Explorerja (IE) na visoka (high) varnost.
    b. Izklopite ActiveX in aktivno skripto v IE nastavitvah, oziroma odkljukajte, naj vas o uporabi teh prej vpraša za dovoljenje. (Opomba: Vse verzije Outlook-a z izjemo Outloka 97 se navezujejo na varnostne nastavitve Internet Explorer-ja (Tools, Internet Options, Security). V Outlook-u je omogočena le izbira med dvema možnostima (Tools, Options, Security). Privzeta nastavitev je običajno spletno območje, lahko pa izberemo omejena spletna mesta, kar je bolj varno.)
    c. V Outlook-u 98 je pomembno, da se izklopi možnost predogleda (privzeta nastavitev) za vse mape.
2. **Outlook Express (Microsoft)** – Izključite možnost predogleda (možnost, ki omogoča predogled le prvih treh vrstic, je sprejemljiva).
    a. Prva nastavitev je enaka kot za Outlook – IE visoka varnost.
    b. Možnost predogleda se izklopi v meniju Lokalne Mape (Local Folders) – Pogled (View) – Ureditev (Layout) – možnost predogled ne sme biti obkljukana.
3. **Netscape** – Izključite Java Skripto za elektronsko pošto in novice v meniju Urejanje (Edit) - Izbire (Preferences) – Napredno (Advanced).

Priporočljiva je tudi uporaba naslednjih nastavitev za poštne odjemalce:
1. Izklopitev avtomatičnega odpiranja priponk.
2. Odpiranje le običajnih tekstovnih dokumentov (Plain text)
3. Onemogočanje odpiranja izvršilnih datotek, datotek tipa *.doc, *.xls in *.ppt.
4. Izklopitev možnosti dvojnega klika na priponkah.
5. Ločeno shranjevanje elektronskih naslovov.

5. PROTIVIRUSNI PROGRAMI

Računalniški virusi so postali velika grožnja za računalniške uporabnike in prav zato so podjetja razvila protivirusne programe, ki poskrbijo za odpravljanje virusov in za preprečevanje okužbe računalnikov z njimi. Protivirusni programi so aplikacije, ki so narejene z namenom, da odkrivajo viruse. To storijo tako, da primerjajo programe (viruse) z bazo poznanih virusov, ki jo protivirusni programi vsebujejo, oziroma iščejo neko specifično vedenje, ki je značilno za večino virusov. V tem primeru protivirusni program ne pozna virusa in ga tako tudi ne more poimenovati, lahko ga pa vseeno nevtralizira. Protivirusni programi z leti vse bolj pridobivajo na pomenu, saj je vse večji delež poslovanja podjetij odvisen od računalnikov in elektronskega izmenjevanja podatkov med temi, zato je izbor optimalnega protivirusnega programa za podjetje primarnega pomena.

5.1 Izbor optimalnega protivirusnega programa za podjetje

Na trgu je veliko število protivirusnih programov in vsi obljubljajo nezgrešljivost pri odkrivanju in preprečevanju okužbe z virusi. Komu gre zaupati pri izbiri in na kaj naj bo kupec pozoren, pa je odvisno od podjetja in potreb, ki jih ima. V glavnem si pri odločitvi o nakupu protivirusnega programa velja zapomniti naslednje smernice:

1. Protivirusni program se mora ujemati s potrebami podjetja. To pomeni, da je v primeru podjetja, ki si izmenjuje veliko število Wordovih dokumentov ključnega pomena, da izbere protivirusni program, ki ponuja 100% zaščito pred makro virusi. Spet drugo podjetje, ki si izmenjuje elektronska sporočila z raznovrstnimi priponkami, mora izbrati protivirusni program, ki ponuja dobro zaščito pred črvi. Če podjetje ne opravlja prej navedenih opravil v velikem obsegu, je lahko najprimernejša aplikacija z dobro celovito zaščito.
2. Podjetje naj izbere takšen protivirusni program, ki je primeren za sposobnosti in znanje zaposlenih. Za dobro zaščito elektronskega poslovanja mora biti protivirusni program enostaven za namestitev, konfiguracijo, upravljanje in bistveno je, da ustreza tehničnemu znanju zaposlenih. Tudi najboljši protivirusni program bo nekoristen, če ga ne bomo znali primerno nastaviti, posodabljati in pravilno uporabljati. Ta vidik je še posebej pomemben za manjša podjetja, ki nimajo dovolj virov za polno zaposlitev visokokvalificiranega varnostnega administratorja. V takih podjetij to delo običajno opravlja eden izmed zaposlenih, ki običajno nima primerne kvalifikacije za takšno delo. To pomeni, da se mora podjetje pri nakupu ozirati prav na sposobnosti teh kadrov.
3. Koristen je tudi pregled testov protivirusnih programov, ki jih lahko dobimo v različnih računalniških revijah in na spletnih straneh. Računalniške revije nam ne povedo celotne zgodbe, saj v večini uporabljajo majhno bazo virusov, s katerimi preizkušajo protivirusne programe, so pa zato zelo koristne za oceno enostavnosti uporabe in cene programov. Za strokovnejše mnenje učinkovitosti protivirusnih programov si velja ogledat spletne strani kot so Icsa.net

(http://www.icsalabs.com/html/communities/antivirus/certification/certprod.shtml), virusbulletin.com (http://www.virusbulletin.com/vb100/archives/index.xml) in av-test.org. Organizacija TruSecure (ICSA.net) opravlja preizkušanje protivirusnih programov (98% vseh na trgu) že 13 let. Če protivirusni program uspešno opravi preizkuse, dobi njihov certifikat. Vsake tri mesece preizkušajo vse programe in v primeru, da certificiran protivirusni program ne opravi testov uspešno, obvestijo proizvajalca, ki ima možnost v sedmih dneh odpraviti napake, v nasprotnem primeru mu odvzamejo certifikat. Na podobnem principu temeljijo tudi ocene ostalih spletnih strani.

4. Ko se na podlagi testov odločimo, katerim protivirusnim aplikacijam velja zaupati, je priporočljivo, da najprej preizkusimo njihove preizkusne različice. Večina proizvajalcev nam danes to omogoča vsaj za tridesetdnevni rok. Le na tak način se lahko prepričamo, da je protivirusni program dovolj enostaven in primeren za naše sposobnosti uporabe.
5. Velik vpliv k odločitvi o nakupu prinese tudi zmožnost in pogostost posodabljanja baze poznanih virusov, ki jo protivirusni program ima.
6. Ko vse to pretehtamo, nam ostane le še zadnji faktor, ki vpliva na izbiro protivirusnega programa. To je cena programa in cena vsakoletnih posodobitev.

5.2 Glavne karakteristike nekaterih najbolj znanih protivirusnih programov

Protivirusni programi so si z leti čedalje bolj podobni, saj imajo že skoraj vsi osnovne karakteristike, ki vključujejo pregledovanje zagonskih datotek ob vklopu računalnika, komunikacijo s centralnim strežnikom za posodabljaje baze virusov in avtomatizirano nameščanje programa. Kljub podobnim karakteristikam protivirusnih programov pa ostajajo razlike v izvedbi teh opravil. Prav te razlike nam odpirajo vprašanje, kateri protivirusni program naj uporabljajo moderne korporacije. Odgovor bom poskušal podati z analizo štirih produktov vodilnih proizvajalcev na tem področju. To so podjetja Sophos, McAfee/Network Associates, Symantec in F-Secure. Poleg teh poznamo še veliko kakovostnih protivirusnih programov, ki imajo v primerjavi z zgoraj navedenimi določene prednosti in slabosti. Rezultati raziskave, ki jih je opravila organizacija AV-Test.org (www.AV-test.org), kažejo na to, da je hitrost odzivnosti z ustreznimi popravki hitrejša pri nekaterih novejših programih, ki imajo še relativno manjši tržni delež. Naj omenim sledeče: Kaspersky, BitDefender, Virusbuster, F-Prot, RAV, Trend Micro, Norman, Panda. Največja razlika v povprečnem času odzivnosti na popravke za viruse Dumaru.Y, MyDoom.A, Beagle.A in Beagle.B je med omenjenimi programi znašala celo 21 ur (Symantec 27:10 ur, Kaspersky 6:51 ur) (Računalniške novice, 2004, str. 17).

Norton Anti-Virus Corporate Edition 7.6 podjetja Symantec ponuja kombinacijo enostavnosti in fleksibilnosti uporabe, saj uporablja Microsoftovo konzolo kot uporabniški vmesnik, kar nedvomno pripomore k hitrejšemu uvajanju v aplikacijo. Po testih podjetja »InfoWord test center« so za namestitev aplikacije na strežnik in nekaj odjemalcev porabili zgolj 45 minut,

kar je nedvomno zelo kratek čas. Symantecov izdelek ponuja tipično arhitekturo, kjer odjemalec poroča centralnemu strežniku. Program ponuja tudi izredne možnosti za nameščanje aplikacij (odjemalec) na daljavo in posodabljanje baze poznanih virusov, kjer strežnik prejme bazo novih virusov s spleta in ta zatem razpošlje to do vseh odjemalcev. Pohvalna lastnost je tudi učinkovita administratorska kontrola nad določanjem tega, kaj lahko in kaj ne morejo početi uporabniki na svojih računalnikih s protivirusnim programom. Med slabosti programa lahko štejemo predvsem velikost (60MB) programa (odjemalec) in obremenitev (upočasnitev) sistema ob pregledovanju računalnika za virusi (full system scan).

McAfee Total Virus Defense Suite je naslednji od vodilnih protivirusnih programov na tržišču. Primeren je za organizacije, ki potrebujejo nadgradljivo in hkrati zelo fleksibilno protivirusno rešitev. Tudi tu imajo administratorji popolno kontrolo nad vsemi vidiki uporabe programa na odjemalčevem računalniku. Pozitivna lastnost tega programa leži v zelo majhnem (2MB) odjemalčevem programu in v zelo majhni obremenitvi računalnika pri pregledovanju datotek. Med slabosti pa lahko štejemo predvsem togost (zahtevnost) uporabniškega vmesnika pri uporabi za administratorja.

F-Secure Anti-Virus for Workstations 5 spada tudi med visokokakovostne protivirusne izdelke in je primeren za širok spekter podjetij. Odlikujejo ga enostavnost uporabniškega vmesnika za administratorje in relativna majhnost paketa na strani odjemalca (9MB). Tudi pri pregledovanju sistema pred virusi so ob zagonu ostalih aplikacij opazne le manjše zakasnitve.

Sophos Anti-Virus se lahko pohvali z zelo učinkovitim pregledovalnikom datotek, ki uporablja posebno tehnologijo (InterCheck) pri pregledovanju datotek, prav ta pa zagotavlja, da je sistem pri tem opravilu skoraj popolnoma neobremenjen. Po testih podjetja »InfoWord test center« se je izkazalo, da so lahko uporabljali različne aplikacije ob hkratnem pregledovanju datotek brez opaznih zakasnitev. Tudi za enostavnost namestitve programa in uporabe uporabniškega vmesnika je poskrbljeno zelo dobro. Sophos je tudi dobro poskrbel za podporo različnim operacijskim sistemom, saj podpira Windows-e, Unix, Linux, Macintosh in ostale operacijske sisteme. K pomanjkljivostim pa velja omeniti predvsem nezmožnost avtomatskega posodabljanja baze poznanih virusov (podjetje napoveduje prihod popravka v kratkem).

Tabela 6: Primerjalna tabela z ocenami od 1 do 10, kjer 1 predstavlja najslabšo oceno in 10 najboljšo oceno

Produkt	**F-Secure Anti-Virus 5**	**McAfee Total Virus Defense Suite**	**Norton Corporate Edition 7.6**	**Sophos Anti-Virus**
Cena(100 mest)	32$/odjemalca	43.50$/odjemalca	17.90$/odjemalec 19.40$/strežnik	31$/odjemalec
Posodabljanje baze	Avtomatsko	Avtomatsko	Avtomatsko	Ročno
Podpora OS na strani odjemalca	Windows, Linux	Windows	Windows	Windows, Solaris, Liuux, Unix, Macintosh
Podpora OS na strežniku	Windows NT/2000	Windows NT/2000	Windows NT/2000	Windows NT/2000
Velikost odjemalca	9MB	2MB	60MB	8MB
Enostavnost uporabe	7	5	6	7
Izvedba	7	6	8	7
Inovativnost	7	7	8	9
Povezljivost	8	6	8	9
Nadgradljivost	8	9	9	7
Varnost	8	6	7	9
Primernost	7	8	8	7
Podpora	7	7	6	9
Izobraževanje	7	7	7	7
Vrednost	8	7	9	8
Celota	7	6	7	7
Za	+Stabilnost, enostavnost uporabe	+Fleksibilnost, nadgradljivost	+Uporabniški vmesnik	+Zelo učinkovit pregledovalnik, podpora
Proti	-Nadgradljivost	-Uporabniški vmesnik	-Obremenjevanje sistema – Velikost/odjemalca	-Ročno posodabljanje -Ne popolnoma centralizirano upravljanje
Podjetje	F-Secure; www.fsecure.com	McAfee; www.mcafee.com	Symantec; www.symantec.com	Sophos; www.sophos.com

Vir: Andress, 2002, str. 27.

Izbira protivirusnega programa je na koncu odločitev podjetja in načina, kako želi podjetje aplikacijo upravljati. Vseeno pa so opazne nekatere ključne razlike med aplikacijami, ki lahko pripomorejo k izbiri protivirusnega programa. Če podjetje od protivirusnega programa pričakuje veliko stopnjo nadgradnje in centraliziranega upravljanja, potem je Symantecov izdelek najprimernejši. Za podjetje, ki ima med prioritetami velikost odjemalne aplikacije in hitrost delovanja računalnika je priporočljiva aplikacija podjetja McAfee. V primeru, da

organizacija išče aplikacijo, ki ji bo nudila najboljšo varnost, performance, tehnično podporo in kompatibilnost z različnimi operacijskimi sistemi je zmagovalec Sophos Anti-Virus.

6. SKLEP

Pričujoče delo nas seznanja s vse bolj aktualno in perečo problematiko računalniških virusov, katerih posledice so lahko ogrožajočega pomena za nemoteno in učinkovito uporabo informacijskih tehnologij, na katerih temelji večji del ali pa celotno poslovanje sodobnih podjetij. Predstavil sem razvojne generacije, ki so zaznamovane predvsem z načinom okužbe z virusi. Tako so za prvo generacijo značilni predvsem virusi startnega zapisa, ki so bili aktualni v časovnem obdobju od leta 1985 tja do leta 1994. Temu je sledilo obdobje makro virusov, ki so prevladovali od leta 1995 do leta 1999. Nato je prišlo obdobje virusov elektronske pošte za katere je bilo značilno, da so se sami razpošiljali na nove elektronske naslove, ki so jih našli v okuženem računalniku (1999-2001). V četrto generacijo virusov štejemo večdelne viruse in viruse, ki izkoriščajo programske pomanjkljivosti operacijskih sistemov in ostalih programov (2001-?). O peti generaciji virusov lahko le špekuliramo, da jo bodo zastopali raznovrstni virusi, ki bodo iz osebnih računalnikov vse pogosteje prehajali v prenosne telefone, dlančnike in ostale naprave, ki se bodo posluževale masovnih operacijskih sistemov.

Med najbolj pereče probleme računalniških virusov sodijo zagotovo velike izgube, ki jih utrpijo podjetja in posamezniki, ko se srečujejo z virusi. Kljub temu, da se je zavedanje problema virusov v zadnjih leti zelo povečalo, je škoda, ki jo povzročijo virusi, vsako leto še vedno zelo velika. To potrjujejo tudi raziskave, ki kažejo, da se je v letu 2002 število uničenih, poškodovanih in izgubljenih dokumentov znatno povečalo glede na pretekla leta in škoda, ki so jo utrpela podjetja, je kot posledica tega zelo narasla. Vse to se je zgodilo kljub povečani uporabi protivirusnih programov in sprotnem ažuriranju baze poznanih virusov v protivirusnih aplikacijah. Dejstvo je, da se v današnjih časih porabi več časa in energije, kot v preteklosti za boj proti virusom, a trend naraščanja okužb z virusi še vedno ne pojenja. Glavni razlog za to so nove generacije internetnih virusov, ki se vse hitreje širijo in že v nekaj urah okužijo zelo veliko število računalnikov v korporaciji. V preteklosti je vse to potekalo veliko počasneje, saj so virusi potrebovali več mesecev, da so lahko ogrozili poslovanje organizacije. Zaradi tako hitrega širjenja novih virusov se je bistveno povečal pomen zaščite pred novimi in neznanimi virusi. Pred časom je veljalo, da je lahko reaktivna politika zadoščala za temeljito zaščito pred virusi, danes pa je to lahko le osnova. Podjetja morajo zagotavljati zaščito tudi pred novimi neznanimi virusi in to lahko dosežejo le z uporabo aplikacij, ki se poslužujejo hevrističnih metod, detektorjev sprememb, filtriranja in podobnih postopkov.
Kljub povečani uporabi protivirusnih aplikacij v organizacijah, so se stroški odprave posledic okužb v zadnjem letu povečali. To izhaja predvsem iz dejstva, da so protivirusni programi nujni element zaščite, ne pa tudi zadostni. Podjetja morajo uporabljati celovito politiko zaščite, ki mora vključevati tudi generične tehnike zaščite in predvsem bi tukaj poudaril

izobraževanje zaposlenih. Zaposleni morajo imeti vsaj osnovno znanje o dejavnikih, ki lahko povzročijo motnje v delovanju sistema, in seznanjeni morajo biti s tem, kako uporabljati računalnik glede na različne namene! K temu pa v veliki meri pripomore jasno izoblikovana in zapisana protivirusna politika podjetja, ki bi morala biti temelj vseh varnostnih prizadevanj podjetja. Le z dobro zasnovano varnostno politiko, ki zagotavlja celovit pristop do zaščite podjetja in z dobrim poznavanjem, oziroma aplikacijo te s strani zaposlenih, se lahko organizacija celovito zaščiti pred virusi in s tem zmanjša stroške podjetja.

7. LITERATURA

1. Andress Mandy: Preventive medicine. [URL: http://www.infoworld.com/article/02/03/01/020304neantivirus_1.html], 1.3.2002.
2. Bontchev Vesselin: Methodology of Anti-Virus Research: Faculty of Informatics, University of Hamburg, 1998. 83 str.
3. Bridwell Larry: Computer Virus Prevalence Survey 2002: ICSA Labs, a Division of TrueSecure Corporation. [URL: http://www.icsalabs.com], 2003. 56 str.
4. Brunnstein Klaus: From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour. [URL: http://www.csrc.nist.gov/nissc/1999/proceeding/papers/p12.pdf], 23.7.1999.
5. Cohen Fred: Computer Viruses. Los Angeles: University of Southern California, 1986. 57 str.
6. Coulthard A., Vuori T.A.: Computer Viruses: a quantitative analysis. [URL: http://emeraldinsight.com/0957-6053.htm], 10.12.2003.
7. Helenius Marko: A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities. Tampere: University of Tampere, 2002. 92 str.
8. Jackson Chris: Virus Security for Small Enterprises. [URL: http://www.securityfocus.com/infocus/1281], 28.2.2001.
9. Mrhar Peter: Računalniški Virusi. Nova Gorica: Flamingo, 1995. 107 str.
10. Resne pomanjkljivosti protivirusnih programov. Računalniške novice, Ljubljana, 2004, 5/IX, str. 17.
11. Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretville: The Norman Book on Computer Viruses [http://download.norman.no/manuals/eng/BOOKON.PDF], 8.1.2004
12. Sophos: Computer viruses demystified. [URL:http://www.sophos.com/sophos/docs/eng/comviru/viru_ben.pdf], 2001. 73 str.
13. White Steve R., Chess David M., Chengi Jimmy K.: Coping with Computer Viruses and Related Problems. Los Angeles: IBM Thomas J. Watson Research Center, 1989. 27 str.