UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

POSLOVNA ŠKODA KOT POSLEDICA RAČUNALNIŠKIH VIRUSOV

Ljubljana, september 2004 MIRAN VARGA

IZJAVA

Študent Miran Varga izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Aleša Groznika in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis: _____

KAZALO

1. UVOD

Računalniški virusi, hekerji, vdori, internetni kriminal. Vsi našteti pojmi polnijo naslovnice dnevnega časopisja in povzročajo ogromno gospodarsko škodo. Preventiva in odpravljanje posledic pustošenja računalniških virusov imata namreč svojo ceno – merjeno v milijonih. Milijonih evrov, naj dodam.

Brez dvoma so posledice hude. Zamislimo si samo, kaj se nam lahko zgodi na delovnem mestu ali doma. Predstavljajmo si situacijo, ko imamo nameščen protivirusni program, ki ga več mesecev nismo posodobili/osvežili. Ko končno posodobimo protivirusno bazo, ugotovimo, da so naše tabele in razpredelnice okužene z virusom, ki naključno spreminja podatke (števila) v datotekah. Seveda smo ves čas shranjevali tudi varnostne kopije, toda tudi te so že več mesecev okužene. Kako bomo vedeli, katerim rezultatom zaupati?

Naslednji primer. Na spletu se pojavi nov virus, ki se širi z elektronsko pošto. Naše podjetje prejema enormne količine okuženih e-poštnih sporočil, zato se odločimo da poštni strežnik za nekaj ur popolnoma izključimo in pri tem izgubimo nujno naročilo pomembnega poslovnega partnerja. Ali pa je podjetje primorano za nekaj ur izključiti delovanje več ključnih datotečnih strežnikov. Zaposlenim tako pade produktivnost, vse skupaj pa podjetje stane večje vsote denarja.

Na delovnem mestu imamo z virusom okužen računalnik. Poslovnemu partnerju pošljemo nekaj dokumentov, ki vsebujejo virus. Se bo slednji še čutil varnega in posloval z nami?

Nekaj primerov iz domačega okolja. Predstavljajmo si, da smo skorajda končali s pisanjem diplomskega dela. Otroci, ki tudi uporabljajo isti računalnik, namestijo novo igro. Le-ta je okužena z virusom, ki pobriše celotno vsebino trdega diska skupaj z našimi dokumenti. Koliko trdega dela je izgubljenega?

Prijatelj nam po elektronski pošti pošlje nekaj zanimivih datotek, ki jih je našel na spletu. Ko jih poženemo, računalnik okužimo z virusom, ki vsem našim kontaktom iz imenika priljubljenega poštnega odjemalca razpošlje naše zaupne datoteke. Skrajno neprijetno.

Vsi navedeni primeri oziroma incidenti so se že zgodili in ponovili. V vsakem od naštetih primerov bi lahko okužbo in širjenje virusa preprečili z nekaj enostavnimi ukrepi.

Škoda, ki nastane ob okužbi računalnika oziroma računalnikov z računalniškim virusom, torej še zdaleč ni zanemarljiva. Prav nasprotno. Zgornji primeri nazorno kažejo, da smo računalniškim virusom izpostavljeni povsod, zato je pomembno, da se te nevarnosti zavedamo in proti njej ustrezno ukrepamo. Namen tega diplomskega dela je prikazati problematiko računalniških virusov in njihove posledice. Pri napadih računalniških virusov nastaja tudi ogromna poslovna/ekonomska škoda, tako med domačimi uporabniki kot tudi v podjetjih. Žal je njeno merjenje težje izvedljivo, saj imajo računalniških virusi kopico neposrednih in posrednih učinkov. V svetu tako ne obstajajo globalne študije na to tematiko, razna priznana analitična podjetja zgolj podajajo svoje ocene. Še najbližje se obravnavani tematiki približa vsakoletna študija laboratorijev ICSA Labs o razširjenosti računalniških virusov. Omenjeni strokovnjaki že devet let vestno spremljajo 300 srednjih in velikih ameriških podjetij ter njihova soočenja z računalniškimi virusi. V zadnjih letih pri svojem delu poizvedujejo tudi po višini poslovne škode, ki jo povzročajo virusni napadi. Številke so iz leta v leto večje, kljub dejstvu, da se tudi stopnja zaščite veča.

Sorodno raziskavo zadnja leta opravlja tudi ameriški inštitut za računalniško varnost[1] v sodelovanju s preiskovalnim uradom FBI[2]. Njihova analiza temelji predvsem na podanih prijavah kršenja računalniške varnosti. Žal za Evropo podobna študija ne obstaja kakor tudi ne za Slovenijo. Stanje v Sloveniji bo v tem delu prikazano skozi oči strokovnjakov protivirusnih podjetij na domačem trgu, ki so privolila v sodelovanje. Za njihovo pomoč se jim na tem mestu tudi najlepše zahvaljujem. Menim, da bo prikaz stanja na domačem trgu na ta način kar najbolj realen.

2. RAČUNALNIŠKI VIRUSI

Sredi 80. let 20. stoletja sta brata Basit in Amjad Alvi iz Pakistana ugotovila, da ljudje nelegalno razmnožujejo njuno programsko opremo. Odzvala sta se tako, da sta napisala prvi računalniški virus, imenovan Brain. Program je namestil sebe in sporočilo o avtentičnosti vsebine na vsako izdelano kopijo diskete s programsko opremo bratov Alvi. Iz teh preprostih začetkov se je razvila celotna kultura računalniških virusov. Danes se novi virusi uspejo razmnožiti po računalniških sistemih širom sveta v vsega nekaj urah. Naslovnice časopisov so polne senzacionalnih naslovov o nevarnih virusih ter črvih, ljudje so šokirani nad posledicami, a prepogosto slabo informirani.

2.1 KAJ JE RAČUNALNIŠKI VIRUS?

Za veliko uporabnikov interneta je postalo izrazoslovje, ki opisuje zlonamerne programske kode, nekoliko zmedeno, saj se izraza »virus« ali »črv« pogosto uporabljata kot sinonima. Vendar pa sta to različni vrsti zlonamernih kod, vsaka s svojimi značilnostmi in svojim nazivom.

Če govorimo na splošno, vse zlonamerne programske kode spadajo pod precej širši koncept računalniških nevšečnosti (ang. malware). Slednje lahko definiramo kot katerikoli program, dejanje, sporočilo ali dokument, ki je sposoben povzročiti negativne posledice uporabnikom informacijskih sistemov.

Strokovna literatura računalniške programe, ki so namenoma napisani za ustvarjanje škode, deli na štiri skupine (Ahuja, 1997, str. 18–19):

- računalniški virusi,
- črvi,
- trojanski konji,
- programske bombe.

Računalniški virusi in trojanski konji se od črvov in programskih bomb razlikujejo po tem, da za svoje širjenje potrebujejo gostitelja, ostala dva pa ne, saj sta samostojna programa. Kot gostitelj računalniškemu virusu lahko služi izvršilna ali podatkovna datoteka, zagonski sektor na disketi, trdem disku ali drugem pomnilniškem mediju[3]. Značilno za računalniške viruse in

[1] Computer Security Institute (CSI).
[2] FBI je kratica za Federal Bureau of Investigation.
[3] Zagonski sektor premorejo različni pomnilniški mediji – diskete, trdi diski, optični mediji, USB pomnilniške naprave in drugi.

črve je tudi, da se razmnožujejo sami. Trojanski konji in programske bombe se navadno same ne razmnožujejo, čeprav obstajajo tudi t. i. virusni hibridi[4], ki se znajo samodejno širiti.

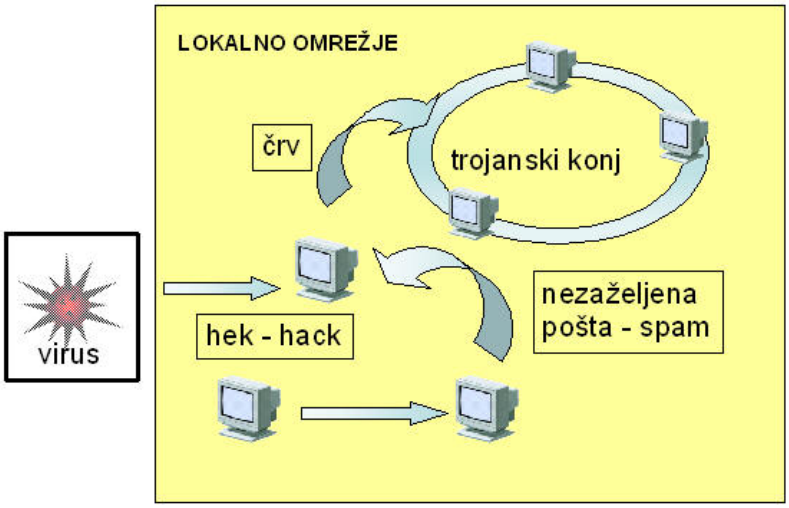
2.1.1 Računalniški virusi

Računalniški virus je računalniški program, ki ustvarja lastne kopije in se širi po drugih računalnikih in omrežjih, običajno brez uporabnikove vednosti. Virusi imajo lahko tudi škodljive stranske učinke. Slednji se pojavljajo v različnih oblikah – od nadležnih sporočil do brisanja vseh podatkov na računalniku. Virusi veljajo za samorazmnoževalne programe, ki lahko okužijo in uničujejo druge programe. Zanje je značilno, da se ob vsaki okužbi množijo.

Danes se največ računalniških virusov širi preko elektronske pošte (v obliki priponk elektronskih sporočil) in neposredno preko interneta. Slednja vrsta virusov ne potrebuje gostitelja, da bi se razširila iz enega na drug računalnik. Strategija virusa, ki se širi preko internetnega omrežja, je poiskati nezaščitena komunikacijska vrata, da bi prišel v računalnik, ne da bi uporabnik to opazil.

Poznamo več vrst računalniških virusov.

Slika 1: Primer nevarnosti v lokalnem omrežju



Vir: Varovanje informacijskega premoženja, 2004.

2.1.1.1 Virusi na zagonskem sektorju

Virusi na zagonskem sektorju (ang. boot sector viruses) disket ali trdih diskov so bili med prvimi oblikami virusov. Širijo se s spremembami zagonskega sektorja, dela diskete ali trdega diska, v katerem je zapisan program, ki omogoča zagon računalnika in operacijskega sistema.

Ko prižgemo računalnik, strojna oprema poišče program za zagon operacijskega sistema. Ta program se običajno nahaja na trdem disku, seveda pa ga je moč najti tudi na disketah ter

[4] Virusni hibrid je skupek škodljive kode, ki v sebi premore več programskih lastnosti – lahko je hkrati virus in trojanski konj, računalniški črv in programska bomba ali pa druga kombinacija naštetih oblik.

cedejih. Program se požene in naloži v pomnilnik računalnika. Virusi na zagonskem sektorju spremenijo program za zagon računalnika s svojo modificirano različico. Ob naslednjem zagonu sistema se uporabi okuženi zagonski sektor ter aktivira virus.

Okužba z virusom na zagonskem sektorju je mogoča le v primeru, ko smo računalnik zagnali (ang. boot up) z disketnega pogona, v katerem je bila z virusom na zagonskem sektorju okužena disketa. Takšne zagone smo opravljali pred desetletjem, ko je bil širše uporabljan operacijski sistem DOS, danes pa to početje zasledimo le redkeje.

Z leti je zagonski sektor postal vse bolj zaščiten, zato je tudi tovrstnih virusov čedalje manj. Večina virusov na zagonski sektor je bilo napisanih za operacijski sistem DOS, zato se v danes zelo razširjenih Windows okoljih ne širijo, jih pa včasih uspejo vsaj malo ohromiti in jim preprečiti normalen zagon.

Med bolj znana virusa na zagonskem sektorju štejemo virusa »Form« in »Parity Boot«.

2.1.1.2 Parazitski virusi (datotečni virusi)

Parazitski virusi, bolj znani kot datotečni virusi, so svoje poimenovanje dobili zaradi lastnosti samopripenjanja programom oziroma izvršilnim datotekam (ang. executables).

Ko zaženemo program, okužen z virusom, se virus požene prvi, zatem pa požene še želeni program. S tem virus skrije svojo dejavnost. Operacijski sistem namreč virus prepozna kot del programa, ki smo ga pognali in mu zato dodeli enake pravice dostopa do sistemskih sredstev. S pridobljenimi pravicami se lahko virus razmnoži, torej kopira samega sebe na druge datoteke, v sistemski pomnilnik in izvede vse druge škodljive operacije.

Parazitski virusi obstajajo že od samih začetkov virusnih okužb in še danes predstavljajo vrsto nevarnosti. S pojavom interneta so namreč ti virusi dobili idealno pomoč pri svojem širjenju, saj je prenos datotek preko spleta močno razširjena oblika komuniciranja med uporabniki. Posledično je tudi možnost okužbe z virusom velika.

2.1.1.3 Virusi, ki se sami posodabljajo

Kot posebno vrsto virusov lahko opredelimo tudi viruse, ki se sami posodabljajo. Take zlonamerne programske kode, kot je na primer virus Win32/Opaserv, lahko naložijo svoje izboljšane različice z interneta. Na srečo in po zaslugi podpore številnih ponudnikov internetnih storitev pa take spletne strani, ki hranijo posodobitve, običajno hitro ugasnejo.

2.1.1.4 Drugi virusi

Obstajajo tudi številni drugi primeri zlonamernih kod, ki ne sodijo v obstoječo klasifikacijo. Takšen primer je virus Win32/Sobig.B (imenovan tudi Palyh), ki med drugim poskuša povečati dostope do določene spletne strani; Lentin, ki ga je indijska skupina uporabila za vzpostavitev napada DoS[5] na pakistanske spletne strani ali CodeRed.F, narejen za napad na spletno stran Bele hiše.

[5] Pri t.i. DoS napadu gre za zavračanje storitev (ang. Denial of Service).

2.1.2 Računalniški črvi

Računalniški črvi (ang. worm) so podobni računalniškim virusom, od slednjih se razlikujejo le po tem, da za svoje širjenje ne potrebujejo prenašalca (kot je na primer datoteka, zagonski sektor diska ipd.). Črvi namreč naredijo svojo kopijo in za širjenje uporabljajo komunikacijsko povezavo med dvema računalnikoma, najpogosteje elektronsko pošto ter internet. Črv zaganja druge programe, ne spreminja pa datotek ali sektorjev na diskih. Za črve je značilno, da običajno ne napadajo drugih programov[6], vendar pa lahko zasedejo veliko količino računalniških virov in tako ohromijo računalniški sistem.

Črvi so trenutno najbolj razširjena vrsta računalniških virusov. Večina se jih širi z uporabo elektronske pošte, običajno v datoteki, pripeti k sporočilu. Ko se datoteka zažene, se bo črv poslal na vse naslovnike v imeniku uporabnikovega računalnika ali na druge naslove, ki jih najde v drugih aplikacijah ali datotekah.

Ker pa so uporabniki sčasoma postali pametnejši in spregledali te osnovne tehnike, so ustvarjalci črvov spoznali, da morajo postati bolj zviti, če želijo, da se njihove kreacije še naprej širijo po internetu. Zato so spremenili programske kode, tako da lahko dosežejo veliko število računalnikov. Glede na način, kako dosežejo uporabnika, lahko črve klasificiramo v naslednje skupine:

- Črvi, ki uporabljajo tehnike »socialnega inženiringa«, da pretentajo uporabnike in jih navedejo k temu, da sami poženejo datoteke, ki vsebujejo zlonamerne kode. LoveLetter je bil verjetno najbolj učinkovit virus te vrste. S samo tremi angleškimi besedami – »I Love You« – je uspel premamiti uporabnike in posledično okužiti sto tisoče računalnikov po vsem svetu.

- Črvi z vgrajenimi funkcijami za protokol SMTP[7]. To zlonamernim kodam omogoča, da se iz prizadetega računalnika razpošljejo same, ne da bi uporabnik sploh vedel za to in ne da bi pustil za sabo kakršnekoli sledi svojih aktivnosti. Uporabljajo lahko poštni strežnik, ki ga uporabnik prizadetega računalnika običajno uporablja, ali privzeti strežnik, ki ga določi avtor črva. Črvi tega tipa vključujejo virus Lentin.L, ki se ne glede na bralca sporočila razpošlje na naslove, ki jih najde v imenikih operacijskega sistema Microsoft Windows, aplikacijah MSN Messenger, .NET Messenger ter Yahoo Pager in vse tiste, ki jih najde v HTM datotekah na računalniku.

- Črvi, ki izkoriščajo ranljivosti v najbolj razširjenih programih. Ti so narejeni za izkoriščanje varnostih lukenj v najbolj uporabljanih programih, kot so poštni odjemalci, internetni brskalniki itd. Pri tem lahko izvedejo vrsto akcij, vključno z možnostjo, da se avtomatično zaženejo. V tej skupini sta najbolj znana črva Nimda in Klez.I, ki izkoriščata ranljivost v brskalniku Internet Explorer. Lahko se samodejno zaženeta, ko se sporočilo, ki prenaša črva, prikaže v predoglednem oknu.

V zadnjih letih se vse več črvov širi preko aplikacij za izmenjavo datotek, ali krajše P2P (ang. peer-to-peer). Priljubljenost tovrstnih aplikacij, ki so narejene za to, da uporabnikom interneta omogočajo enostavno medsebojno izmenjavo datotek, so programe, kot so KaZaA ali iMesh,

[6] Nekateri sodobni računalniški črvi skušajo onemogočiti protivirusne programe ter dostop do spletnih strani s protivirusno vsebino. Eden takšnih črvov je Win32/Klez.

[7] SMTP je angleška kratica za Simple Mail Transfer Protocol, torej protokol, ki ga računalniški programi uporabljajo za pošiljanje elektronske pošte.

spremenile v odlična sredstva za prenašanje zlonamernih programskih kod. Da bi izkoristili te programe, črvi ustvarijo datoteke v deljenih imenikih in jim dajo imena, ki zavedejo uporabnike, da jih naložijo na svoje računalnike – imena priljubljenih računalniških iger, programov, filmov, glasbe in podobno. Redisto.B ali Fizzer sta primera te vrste črvov.

2.1.3 Trojanski konji

Trojanski konji ali trojanci se imenujejo po mitološkem trojanskem konju – velikem lesenem konju, ki so ga Grki pustili pred vrati Troje po dolgi bitki. Misleč, da se je grška vojska umaknila, so Trojanci odvlekli konja v svoje mesto. Vendar pa so Grki, ko je padla tema, izstopili iz konja in napadli mesto ter ga tako lahko uničili.

V računalništvu so trojanski konji na videz neškodljivi programi, ki potem, ko dosežejo računalnik, izvedejo vrsto akcij, ne da bi uporabnik to opazil. Programi namreč izvajajo ukaze, ki niso navedeni v njihovih specifikacijah. Uporabnik tako požene domnevno običajen program, le-ta pa skrivno izvaja druge, največkrat škodljive operacije.

Trojanski konji so včasih uporabljani tudi kot sredstvo za okužbo računalnika z drugim virusom. Za razliko od drugih zlonamernih kod se trojanski konji ne razmnožujejo na način, da okužijo druge računalnike. Njihova možnost širjenja je zato omejena, vendar pa so v zadnjih letih pogosti primeri hibridov med črvi in trojanskimi konji, katerih metode razmnoževanja so številne.

Glede na akcije, ki jih trojanski konji izvedejo na prizadetem računalniku, jih delimo v naslednje skupine:

- Uničevalni trojanski konji so narejeni za brisanje določenih datotek, formatiranje trdega diska ali izvajanje drugih uničevalnih akcij. Primer izredno škodljivega trojanskega konja je bil Troj/Zulu. Program se je predstavljal kot popravek milenijskega hrošča (ang. millenium bug), v resnici pa je prepisal vsebino lokalnega trdega diska.

- Trojanski konji za odpiranje stranskih vrat (ang. backdoor Trojans) so narejeni, da odprejo stranska vrata do računalnika, preko katerih lahko napadalci (običajno hekerji) vstopijo in prevzamejo nadzor nad računalnikom. Sestavljeni so iz dveh sestavin: strežnika, nameščenega na napadenem računalniku, in odjemalca, ki ga napadalec uporablja za nadzor nad okuženim računalnikom. Napadalec (upravljavec) lahko na daljavo skrivno upravlja žrtvin računalnik, torej ustvarja, poganja, kopira ali briše datoteke ter programe, nadzoruje strojno opremo itd.

- Trojanci, ki lovijo udarce na tipkovnici (ang. keylogger Trojans), so programirani za lovljenje pritiska tipk uporabnika na tipkovnico. Na ta način lahko pridobijo zaupne informacije uporabnika, kot so gesla, številke kreditnih kartic ipd. Te informacije hranijo v posebnem dnevniku, do katerega lahko dostopa napadalec.

- Lažni trojanci po zagonu računalnika prikažejo lažna sporočila o napakah in napeljujejo uporabnike k vnosu uporabniških imen in gesel. Le-ta se nato pošljejo ustvarjalcu zlonamerne kode.

2.1.4 Programske bombe

Programske bombe so samostojni programi, sicer namenjeni opravljanju nekega koristnega dela, ki pa imajo nekje v svojem jedru skrito škodljivo kodo, ki se aktivira, ko so izpolnjeni določeni pogoji. Glede na tip teh pogojev jih delimo na časovne in logične. Napisane so lahko zaradi maščevanja, izsiljevanja ali pa zgolj iz nagajivosti. Bombe se ob izpolnitvi določenega pogoja (logične bombe) ali pa ob določenem času (časovne bombe) sprožijo in povzročijo uporabniku podatkovno škodo ali pa mu onemogočajo normalno delo z nagajanjem v obliki prikazovanja izskočnih oken, zapiranja programov, ponovnega zagona računalnika itd.

Zanimiv je primer, ko je podjetje odpustilo delavca, ta pa je namestil virus – logično bombo, ki se je sprožila po njegovem odhodu in naredila preko 10 milijonov dolarjev škode[8].

2.1.5 Druge nevarnosti

Računalniški virusi so del vse večje skupine, v katero sodijo vse vrste IT varnostnih groženj. Med temi sta na primer tudi neželena e-pošta (ang. spam) in oprema za vohunjenje (ang. spyware), katerih učinki so lahko prav tako uničujoči kot po napadih virusov.

2.1.5.1 Neželena elektronska pošta

Ena največjih nevarnosti interneta danes je tudi »spam« ali neželena komercialna pošta, saj lahko povzroča škodo na več različnih ravneh. Izraz »spam« naj bi izviral iz skeča Montyja Pythona[9]. Prizor se dogaja v restavraciji, kjer vse jedi na jedilniku vključujejo mesni obed v konzervi SPAM. Ko natakarica predstavlja jedilnik, skupina Vikingov poje napev "spam, spam, spam ..." vse glasneje in preglasi ves pogovor. Izraz se je bržkone začel uporabljati za opis neželene komercialne pošte, ker preglasi pravo pošto.

Finančna škoda, ki jo povzročajo tovrstne nevšečnosti, se lahko vrednoti s številom delovnih ur, ki jih uporabniki izgubljajo vsak dan, ko morajo brisati taka sporočila, ne da bi jih sploh prebrali. Če vzamemo za primer omrežje s 500 delovnimi postajami in vsaka na dan prejme 10 tovrstnih sporočil ter uporabnik porabi minuto za brisanje le-teh, je lahko preračunati, koliko delovnih ur je izgubljenih na leto zaradi ukvarjanja z neželeno elektronsko pošto. Še več, če je naslov sporočila dovolj privlačen, da privabi uporabnika, da ga le-ta prebere ali se poveže na spletni naslov, naveden v sporočilu, se število izgubljenih ur drastično poveča.
Poslovno škodo, ki jo utrpi podjetje zaradi neželene pošte, meri tudi poseben kalkulator – t. i. Spam cost calculator na spletni strani Computer mail services. Podatki oziroma izračuni, ki se nahajajo v tabeli 1, temeljijo na predpostavki, da posamezni zaposleni v podjetju na dan prejme pet neželenih elektronskih sporočil, za katerih brisanje porabi vsega tri sekunde. Škoda vključuje izgubljene delovne ure zaradi odpravljanja posledic in finančno izgubo ali strošek zaradi onemogočanja poslovanja podjetja.

[8] Gupta, 2000, str. 337.
[9] Vir: Hari Murčehajič: Nove grožnje z interneta, Ribera, d. o. o., 2003, [URL: www.ribera.si]; 21. 6. 2004

Tabela 1: Prikaz odvisnosti stroškov podjetja od števila prejetih neželenih sporočil

Število zaposlenih	Število dnevno prejetih neželenih sporočil	Število izgubljenih ur na leto	Letna izguba (v USD)
100	500	152	2.400
300	1.500	456	7.200
500	2.500	760	12.000

Vir: Computer mail services: Spam cost calculator, 2004.

Neželena pošta sproža tudi druge nevarnosti. Tako sporočilo lahko, čeprav ne zelo pogosto, prenaša virus ali druge zlonamerne programske kode, morebiti celo vsebuje povezave na spletne strani, narejene za pretakanje datotek, ne da bi se uporabnik tega sploh zavedal. Prav takšno metodo je uporabljal virus Win32/Sobig.F, ki se je globalno razširil najhitreje v zgodovini računalništva.

V borbi pred neželeno komercialno pošto imajo uporabniki veliko prednost, saj ima večina tovrstnih sporočil določene značilnosti, po katerih jih je lažje identificirati. Skoraj vsa neželena sporočila poskušajo uporabnika z uporabo podobnih »močnih« besed prepričati, da kupi določen proizvod. Zato lahko posebni programi naredijo profil e-pošte, kategorizirajo ta sporočila kot neželena in jih izbrišejo, še preden se naložijo na poštni strežnik ali poštni nabiralnik prejemnika. Najboljša zaščita pred neželeno pošto je prav gotovo previdnost pri tem, komu vse razkrivamo svoj elektronski naslov.

Neželene pošte ne bomo prejemali tudi ob upoštevanju naslednjih napotkov (Shimmin, 1997, str. 217):

- ne odgovarjajmo na verižna pisma,
- ne odgovarjajmo na reklamna sporočila,
- ne vključujmo predogleda neželenih sporočil, ki so v obliki HTML, saj s tem potrdimo veljavnost svojega naslova,
- Pri naročanju na biltene z novicami (ang. newsletters) uporabljajmo po možnosti kak brezplačen naslov in ne svojega zasebnega,
- na svojih spletnih straneh ne objavljajmo osebnih elektronskih naslovov in
- čim manj obiskujmo in se zadržujmo na pornografskih in piratskih straneh.

2.1.5.2 Programska oprema za vohunjenje

Programska oprema za vohunjenje (ang. spyware) je ena bolj pogostih vrst računalniških nevšečnosti v obtoku. Kot je razvidno iz imena, so tovrstni programi narejeni za vohljanje po aktivnostih uporabnikov, predvsem takrat, ko so povezani v svetovno medmrežje[10]. Ker katerakoli vrsta programske opreme za vohunjenje bistveno prizadene zaupnost na računalniku shranjenih podatkov, se šteje za potencialno nevarnost, ki je ne gre spregledati.

Vohunske aplikacije zbirajo in pošiljajo informacije o spletnih straneh, ki jih uporabniki najpogosteje obiskujejo, čas povezav itd. Prav tako zbirajo podatke o računalniku, na katerem so nameščeni: o operacijskem sistemu, procesorju, pomnilniku itd.

[10] Internet.

Obstajajo tudi programi za vohunjenje, ki lahko odkrijejo in poročajo, če je nameščena programska oprema na računalniku legalna ali ne.

Ti programi so postali zelo razširjeni, v veliki meri zaradi skupka značilnosti, kot so (Murčehajič, 2003, str. 10):

- Skoraj popolne tehnike zakrivanja: programska oprema za vohunjenje je običajno nameščena skupaj z drugimi aplikacijami: odjemalskimi P2P aplikacijami, orodji za trdi disk itd.

- Neopazna imena datotek, ki »vohunom« omogočajo, da se jih ne opazi tako kot ostale datoteke, ki pripadajo aplikaciji.

- Ker niso virusi in ne uporabljajo nobenih rutin, ki bi jih povezovale z virusi, jih protivirusni programi ne opazijo, razen če niso bili posebej programirani za ta namen.

- Na računalniku ne kažejo nobenih vidnih znakov, niti ko so nameščeni niti ko tečejo. Zato uporabniki običajno ne skrbijo o tem, ali so tovrstne aplikacije nameščene na njihovih računalnikih ali ne. Posledično se lahko programska oprema za vohunjenje skrije na sistemih za dolgo časa.

2.2 KAKO VIRUSI OKUŽIJO RAČUNALNIK?

Z virusom okuženi program mora biti aktiviran, preden okuži računalnik. Virusi poznajo več načinov aktiviranja. Tako so lahko pripeti drugim programom ali pa skriti v programski kodi, ki se požene samodejno ob odpiranju določenih tipov datotek, predvsem izvršilnih. Z virusom okužene datoteke lahko prejmemo na več načinov – na pomnilniških medijih (diskete, USB ključi, trdi diski …), kot priponko elektronskim sporočilom ali pa jih nevede naložimo z interneta. Takoj ko okuženo datoteko poženemo, se aktivira tudi virus. Nato se virus lahko prenese, okuži tudi druge datoteke na računalniku.

Najpogostejše virusne okužbe izvirajo iz naslednjih medijev:

- ***Svetovni splet / internet***
  Programi ali dokumenti, ki jih zvlečemo z interneta, so lahko okuženi.

- ***Programi***
  Programi, okuženi z virusom, lahko okužijo naš računalnik, takoj ko jih poženemo.

- ***Elektronska pošta***
  Elektronska sporočila lahko vsebujejo priponke, ki so okužene z virusom. Ob odprtju okužene priponke tako tvegamo okužbo z virusom. Nekatera elektronska sporočila vsebujejo tudi skripte, ki se poženejo v trenutku, ko začnemo prebirati vsebino sporočila.

- ***Dokumenti in razpredelnice***
  Dokumenti in razpredelnice se lahko okužijo s t. i. makro virusi, ki lahko okužijo vse tekstovne dokumente in razpredelnice ter spremenijo ali poškodujejo podatke v njih.

- ***Diskete, cedeji in drugi mediji***
  Računalniške diskete so lahko okužene z virusom v zagonskem sektorju ali pa se virus skriva v zapisanih datotekah. Prav tako so lahko okužene tudi datoteke na cedejih ali devedejih ter drugih medijih.

Učinki računalniških virusov so zelo različni. V tabeli 2 so navedene zmožnosti virusov.

Tabela 2: Učinki računalniških virusov

Učinki	Primer
Sporočila	Virusi lahko izpisujejo nadležna sporočila na računalniški zaslon. Primer takega virusa je virus WM97/Jerk.
Nagajanje	Virus Yankee vsak dan ob 17. uri zaigra določeno skladbo.
Onemogočanje dostopa	Virus WM97/NightShade z geslom zaklene okužene dokumente na petek 13.
Kraja podatkov	Trojanski virus Troj/LoveLet-A preko e-pošte odpošlje podatke o uporabniku in računalniku na določen naslov na Filipinih.
Poškodovanje podatkov	Virus XM/Compatable spreminja podatke v MS Excel razpredelnicah.
Brisanje podatkov	Zloglasni virus Michelangelo 6. marca prepiše dele trdega diska.
Poškodovanje strojne opreme	Virus CIH oziroma Chernoyl (W95/CIH-10xx) na dan 26. 4. skuša prepisati BIOS računalnika in tako onemogočiti le-tega.

Vir: Oldfield, 2001, str. 11.

2.3 PREPREČEVANJE OKUŽB Z RAČUNALNIŠKIMI VIRUSI

Z upoštevanjem nekaj enostavnih pravil lahko zmanjšamo nevarnost okužbe z računalniškim virusom na minimum, oziroma ustrezno ukrepamo v primeru okužbe.

2.3.1 Izobraževanje uporabnikov

Zaposlene v podjetju je potrebno seznaniti z nevarnostmi, ki jih prinašajo okužbe z računalniškimi virusi. Pri tem je potrebno opredeliti delo z izmenljivimi mediji, delo z elektronsko pošto ter delo v omrežju oziroma medmrežju (internetu). Za podjetje je tudi priporočljivo, da ima izdelano varnostno politiko na delovnih mestih, ki jasno opredeljuje, kaj so virusne nevarnosti, kako se pred njimi zaščititi ter kaj storiti v primeru okužbe. Dober način izobraževanja uporabnikov so tudi seminarji in delavnice, kjer se zaposlenim virusno problematiko podrobneje predstavi.

2.3.2 Protivirusna programska oprema

Protivirusni programi skrbijo za zaznavo in odpravo virusov. Svoje delo pa lahko učinkovito opravljajo le v primeru, ko so pravočasno/redno posodobljeni, saj le ažurna protivirusna baza nudi ustrezno rešitev. Če protivirusni program virusa ne pozna, ga običajno tudi ne zazna in ga posledično tudi ni moč odstraniti, zato je redno posodabljanje nuja. Večina protivirusnih programov omogoča avtomatsko samoposodabljanje in tako ne potrebuje velike pozornosti uporabnika. Protivirusni program je potrebno tudi pravilno nastaviti. Ob povprečni relativno visoki zmogljivosti današnjih računalnikov protivirusna podjetja priporočajo, da uporabnik nastavi protivirusni program tako, da ta v realnem času pregleduje sistem za virusi.

2.3.3 Arhiviranje datotek

Arhiviranje operacijskih sistemov, elektronske pošte ali posameznih datotek je zelo priporočljivo. Za datoteke in sisteme, ki so kritični za uspešno delovanje podjetja, je obvezna izdelava ene ali več varnostnih kopij dnevno. Varnostnih kopij tudi ne hranimo vseh na istem mestu.

2.4 KRATKA ZGODOVINA VIRUSOV

V tabeli 3 se nahaja krajši kronološki opis ključnih dogodkov, pomembnih s stališča računalniških virusov in varnosti. Kot lahko vidimo, osnovne ideje sodijo že v konec prve polovice 20. stoletja, medtem ko se pravo dogajanja začne razvijati po letu 1986, ko je tudi napisan prvi računalniški virus. Pravi razmah pa digitalna kuga doživi konec 20. stoletja in svoj škodljivi vpliv vedno bolj širi v kasnejših letih.

Tabela 3: Kratka zgodovina virusov

Leto	Dogodek
1949	Matematik John von Neumann predlaga reprodukcijo računalniških programov.
1950	Podjetje Bell Labs razvije igro, v kateri igralci uporabljajo škodljive programe za napad drugih računalnikov.
1975	John Brunner, avtor znanstveno fantastičnih del, obravnava tematiko računalniškega črva, ki bi se širil preko raznih omrežij.
1984	Fred Cohen predstavi izraz »računalniški virus« v svojem znanstvenem delu o programih.
1986	Brata Alvi napišeta prvi računalniški virus Brain.
1987	Črv, imenovan »božično drevesce« (Christmas tree), ohromi IBM-ovo svetovno omrežje.
1988	Internetni črv (internet worm) se razširi skozi ameriško omrežje DARPA.
1990	Mark Washburn napiše virus imenovan 1260. Gre za prvi polimorfični virus, ki mutira (spreminja svojo obliko) z vsako novo okužbo.
1992	Svet preplaši virus Michelangelo, čeprav je okuženih relativno malo računalnikov.
1994	Pojavi se prva obsežnejša potegavščina (hoax) »Good times«.
1995	Pojavi se prvi makro virus, imenovan Concept. Istega leta je napisan prvi virus za operacijski sistem Windows 95.
1998	»CIH oziroma Chernobyl« postane prvi virus, ki paralizira/poškoduje strojno opremo.
1999	Pojavi se virus »Melissa«, ki se zna sam širiti preko elektronske pošte. Sledi mu virus »Bubbleboy«, prvi virus, ki okuži računalnik zgolj ob branju elektronske pošte.
2000	»Love Bug« postane najuspešnejši virus, ki se širi preko elektronske pošte. Pojavi se prvi virus za operacijski sistem Palm OS.
2001	Začenja se obdobje črvov. Udarijo črvi Sircam, Code Red, Nimda ter Klez. Pokaže se velika ranljivost svetovnih računalnikov, saj črvi uspejo ohromiti internet, čeprav samo začasno.
2003	Poskusi rušenja interneta se nadaljujejo. Črv SQL slammer napade Microsoft SQL temelječe strežnike. Jeseni črva Sobig in Blaster onemogočita milijone računalnikov z operacijskim sistemom Microsoft Windows. Stroški odprave posledic so gromozanski.
2004	Pojavi se virus »Cabir«, ki okuži prenosne naprave z operacijskim sistemom Symbian OS. Sledi mu virus »WinCE4.Dust«, ki okuži operacijski sistem Windows CE. Korporacija Microsoft tako nima več virusno varne platforme. Poplavi s črvi ni videti konca, pojavijo se številni črvi MyDoom, Sasser in drugi.

Vir: Oldfield, 2001, str. 18–19; Wikipedia, 2004; lasten vir.

3. STANJE PO SVETU

Za razliko od Slovenije se v tujini z virusnimi analizami ukvarjajo bolj podrobno. Tako je moč zaslediti več posameznih raziskav po različnih državah, a so slednje zelo omejene glede ciljnih namer. Splošno stanje v širšem gospodarskem okolju tako prikazuje le vsakoletna študija ICSA Labs, neodvisnega oddelka ameriške korporacije TruSecure. Slednja se ukvarja z reševanjem varnostnih problemov, predvsem na področju računalništva in informatike.

3.1 RAZISKAVA ICSA LABS O RAZŠIRJENOSTI VIRUSOV

Omenjeno podjetje tako že od leta 1995 spremlja posledice novodobne kuge – računalniških virusov – po večjih ameriških podjetjih in vsako leto pripravi obširno poročilo ter večdnevni seminar na to temo. Zato velja njihovo letno poročilo o razširjenosti računalniških škodljivcev, imenovano Computer Virus Prevalence Survey, za najbolj detajlno raziskavo na tem področju. Takšna raziskava seveda zahteva obilo sredstev in časa, sodelovanja s strani podjetij in sprotno spremljanje dogajanja v svetu računalniških virusov. Obdelati je namreč potrebno ogromne količine podatkov in iz njih izluščiti bistvo ter raziskati razloge in vzroke za postavljene zaključke.

3.1.1 O raziskavi

Raziskava laboratorija ICSA Labs o razširjenosti virusov (ang. Computer Virus Prevalence Survey) vsako leto zbere in obdela podatke o razširjenosti računalniških virusov ter drugih škodljivih kod (ang. malware) v srednjih in velikih ameriških podjetjih. Zadnja objavljena raziskava je že deveta zapovrstjo in obravnava razširjenost računalniških nevarnosti v letu 2003. V raziskavi so sodelovala podjetja in vladne agencije, ki so izpolnjevale naslednje kriterije: organizacija premore 500 ali več računalnikov, dve ali več lokalnih omrežij (LAN) ter dve ali več oddaljenih omrežij. Podjetja so po varni povezavi podatke o okužbah in reševanju virusnih vprašanj posredovala laboratorijem ICSA Labs vsak mesec, od januarja do decembra 2003. V laboratoriju so podatke zbrali, jih normalizirali in analizirali. Letno poročilo opisuje aktualno problematiko računalniških nevarnosti v obravnavanem letu, odkriva trende in druga gibanja virusnega širjenja ter smeri okužb.

Za analizo virusnega širjenja in posledično povzročeno škodo, ki jo obravnava to delo, sem uporabil tudi podatke preteklih letnih poročil ICSA Labs, torej od leta 1996 naprej. Ker gre za sistematično vsakoletno študijo razširjenosti virusov, so podatki med posameznimi letnimi poročili primerljivi. Seveda pa bo največja pozornost namenjena prav virusnim trendom zadnjih nekaj let, saj se le-ti močno razlikujejo od starejših metod in načinov okužb, ki so jih uporabljali virusi desetletje ali dve nazaj.

3.2 LETO 2003

3.2.1 Splošni pregled

3.2.1.1 Mnenja udeležencev raziskave

Anketa, ki jo je konec leta 2003 izpolnilo 300 ameriških podjetij, ki so sodelovala v raziskavi ICSA Labs, jasno izraža mnenje, da je virusna problematika postala bolj pereča glede na prejšnje leto (2002). Namreč kar 88 odstotkov anketiranih podjetij meni, da se je virusna problematika nekoliko ali močno poslabšala, medtem ko preostalih 12 odstotkov podjetij odgovarja, da je imelo z virusi enako ali manj težav kot prejšnje leto. Velja dodati, da je leto 2003 tako veljalo za najslabše ocenjeno leto v zadnjem desetletju glede virusnih nevarnosti.

3.2.1.2 Pogostost virusnih okužb

Raziskovalci so leta 2003 obravnavali več kot 2,7 milijona virusnih incidentov na več kot 900 tisoč delovnih postajah, strežnikih ter omrežnih vozliščih. V povprečju je torej bil kar 201 poskus okužb na tisoč računalnikov vsak mesec v obdobju od začetka januarja do konca decembra 2003 in 108 dejanskih virusnih okužb na 1.000 računalnikov na mesec.

3.2.1.3 Lastnosti virusnih katastrof

V letnem poročilu je obravnavan tudi pojav virusnih katastrof. Za virusno katastrofo se šteje epidemijo, v kateri je virus ali škodljiva koda istočasno okužila 25 ali več osebnih računalnikov ter strežnikov oziroma je bila povzročena velika škoda ali finančna izguba organizaciji. Pri zadnjem kriteriju so anketirani tudi opisali razsežnost virusne katastrofe kot: število okuženih računalnikov, izgubo podatkov, izgubo produktivnosti, izgubo dohodka itd. Po teh definicijah je virusno katastrofo v letu 2003 prijavilo 92 od 300 obravnavanih podjetij.

3.2.1.4 Posledice virusnih katastrof

92 virusnih katastrof v letu 2003 je zastrašujoč podatek, saj je daleč najslabši v zadnjih letih. Leto 2002, ki je veljalo za izredno slabo, je postreglo z 80 prijavami virusnih katastrof. Leto 2003 so tako zaznamovali številni izbruhi virusnih incidentov. Začelo se je že v januarju, s črvom W32/Slammer in posnemovalci. Slammer je bil mrežni črv, ki se je samodejno razširil po svetovnem spletu v vsega 15 minutah! Medmrežni promet, ki ga je ustvaril črv Slammer pri iskanju računalnikov za okužbo, je povzročil veliko upočasnitev v delovanju interneta ter drugih napadenih komunikacijskih poti. Slammerju je v letu 2003 sledilo še veliko drugih izbruhov in incidentov.

Leto 2003 je bilo tudi prvo leto, ko so v laboratoriju ICSA Labs vsak mesec zabeležili virusno katastrofo. Tudi čas, potreben za odpravo virusne katastrofe, se je povečal, čeprav le za malo. Tako so v letu 2003 za odpravo posledic virusne katastrofe v podjetjih v povprečju potrebovali 24 posameznih delavnikov, medtem ko so leto poprej uspeli posledice odpraviti en delavnik prej. Zato pa so se bistveno bolj povečali stroški odprave posledic virusnih katastrof, ki so v letu 2003 narasli za kar 23 odstotkov v primerjavi z letom 2002. Tako je

posamezna virusna katastrofa podjetje v povprečju stala skorajda sto tisoč ameriških dolarjev. Na podlagi preteklih izkušenj odgovorni v laboratoriju ICSA Labs menijo, da so pridobljeni podatki o virusni škodi podcenjeni. Tehnično osebje, odgovorno za virusno reševanje in preprečevanje v podjetjih, naj bi tako poročalo o zgolj neposrednih stroških virusnih katastrof. Dejanski zneski naj bi bili ob upoštevanju neposrednih in posrednih stroškov virusnih katastrof višji za faktor sedem ali osem.

3.2.1.5 Uporaba protivirusne zaščite

Skorajda vsa podjetja (98 odstotkov) so potrdila uporabo protivirusne programske opreme na vsaj 90 odstotkih svojih računalnikov. Večina anketiranih podjetij uporablja protivirusne rešitve podjetij Network Associates Inc. ter Symantec Corporation.

Boljša je tudi zaščita strežnikov za elektronsko pošto, med katerimi jih je 94 odstotkov zaščitenih s protivirusno programsko opremo. Obenem pa preseneča še vedno relativno nizka stopnja zaščite požarnih zidov (zaščitenih je polovica vseh) in proxy strežnikov, saj le 58 odstotkov slednjih varuje protivirusna programska oprema. Podjetja se torej najbolj zavedajo nevarnosti, ki jih prinaša elektronska pošta, saj kar 88 odstotkov anketiranih podjetij elektronska sporočila in priponke filtrira (blokira, odpravlja viruse, zavrača neželeno pošto …).

3.2.1.6 Cilji analize

Cilji vsakoletnega projekta laboratorija ICSA Labs so ugotoviti razširjenost računalniških virusov in škodljivih kod v srednjih in velikih podjetjih, opisati virusne nevarnosti ter rešitve v računalniških omrežjih, požarnih zidovih, vozliščih ter tudi delovnih postajah in strežnikih. Strokovnjaki vsako leto opazujejo trende in gibanja virusnih okužb, različne metodologije okužb ter načine širjenja škodljivih kod. Območje raziskave zajema računalnike na Intel in ne-Intel platformah[11] v podjetjih, ki imajo skupno več kot 500 računalnikov, več lokalnih in oddaljenih omrežij. V raziskavi sodelujejo podjetja iz industrijskih, trgovskih in vladnih logov.

3.2.1.7 Raziskava in njena metodologija

Zaupanje

Podatki so zbrani iz 300 kvalificiranih podjetij, ki izpolnjujejo predpisane pogoje. Velikost vzorca nudi ±6-odstotno natančnost odgovorov, ki se nanašajo na celoten vzorec.

Zaokroževanje

Občasno so podani podatki o odstotkih, ki presegajo mejo 100 odstotkov. Slednje se pojavi zaradi možnosti več odgovorov. V nekaterih primerih, vrsticah ali stolpcih v preglednicah, znaša vsota 99 ali več kot 100 odstotkov zaradi zaokroževanja. Prav tako lahko v posameznih primerih tabele in grafikoni izražajo vrednosti manjše od 100 odstotkov zaradi izključitve odgovorov tipa »ne vem«, »odklanjam odgovor« in »drugo«.

[11] Manjše število zbranih podatkov, upoštevanih v raziskavi, je zbrano tudi iz Macintosh ter ne-Intel platform. Njihov delež pa je praktično zanemarljiv.

3.3 OSNOVNE UGOTOVITVE

3.3.1 Statistični podatki

Raziskava ICSA Labs o razširjenosti virusov za leto 2003 je obsegala 962.278 delovnih postaj, strežnikov in vozlišč. V povprečju je imelo posamezno podjetje 3.027 osebnih računalnikov (mediana 1.872) in 181 podatkovnih in drugih strežnikov (mediana 68).

3.3.1.1 Kako pogosto se pojavljajo virusi?

Vsa podjetja, ki so sodelovala v raziskavi leta 2003, so v omenjenem letu naletela na vsaj eno z virusi povezano težavo.

Raziskovalci so tako v letu 2003 obravnavali več kot 2,7 milijona virusnih incidentov na več kot 900 tisoč delovnih postajah ter strežnikih. V povprečju je bil torej kar 201 poskus okužb na tisoč računalnikov vsak mesec v obdobju od začetka januarja do konca decembra 2003 in 108 dejanskih virusnih okužb na 1.000 računalnikov na mesec. Omenjene številke potrjujejo trend rasti virusnih okužb v zadnjih letih. Najbolj očitno je prav povečanje razmerja med poskusi okužb in dejanskimi virusnimi okužbami. Strokovnjaki to pripisujejo filtriranju in blokiranju sumljivih oziroma škodljivih vsebin že na vstopu v lokalno omrežje. Računalniški virusi in škodljive kode, ki to zaščito prebijejo, ponavadi tudi okužijo osebne računalnike in strežnike v lokalnih omrežjih.

Pri primerjavi podatkov posameznih raziskav med leti 1996 in 2003 je opaziti določene trende virusnih okužb. V tabeli 4 lahko vidimo, da so med leti 1996 in 1998 strokovnjaki zabeležili povprečno rast 12 okužb z računalniškimi virusi na 1.000 računalnikov vsak mesec, enaka zakonitost se je nato pojavila v obdobju med leti 1999 in 2001. Rast virusnih okužb se je po letu 2001 upočasnila in znaša okoli 3 virusne okužbe na tisoč računalnikov na mesec. Za primerjavo med posameznimi leti služi obdobje med mesecem novembrom in decembrom, saj pretekli podatki kažejo, da je zanesljivost podatkov/odgovorov v tem obdobju najvišja (ima najmanj nihanj).

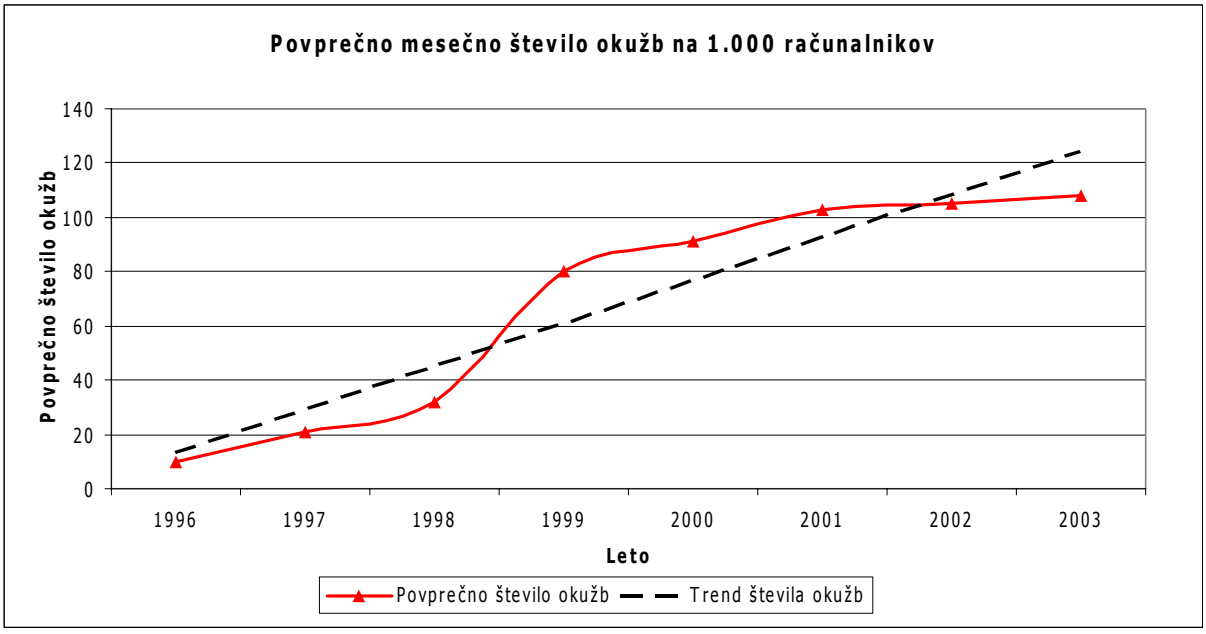
Tabela 4: Povprečno mesečno število okužb na 1.000 računalnikov

Leto raziskave	nov.–dec.
1996	10
1997	21
1998	32
1999	80
2000	91
2001	103
2002	105
2003	108

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 2 grafično prikazuje povprečno število virusnih okužb in njihovo rast v obdobju med letoma 1996 in 2003. Velik porast števila okužb med letoma 1998 in 1999 gre pripisati virusu W32/Melissa, ki je izbruhnil leta 1999 in okužil izjemno veliko število računalniških sistemov s svojim masovnim razpošiljanjem preko elektronske pošte.

Slika 2: Povprečno mesečno število okužb z računalniškimi virusi na 1.000 računalnikov



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

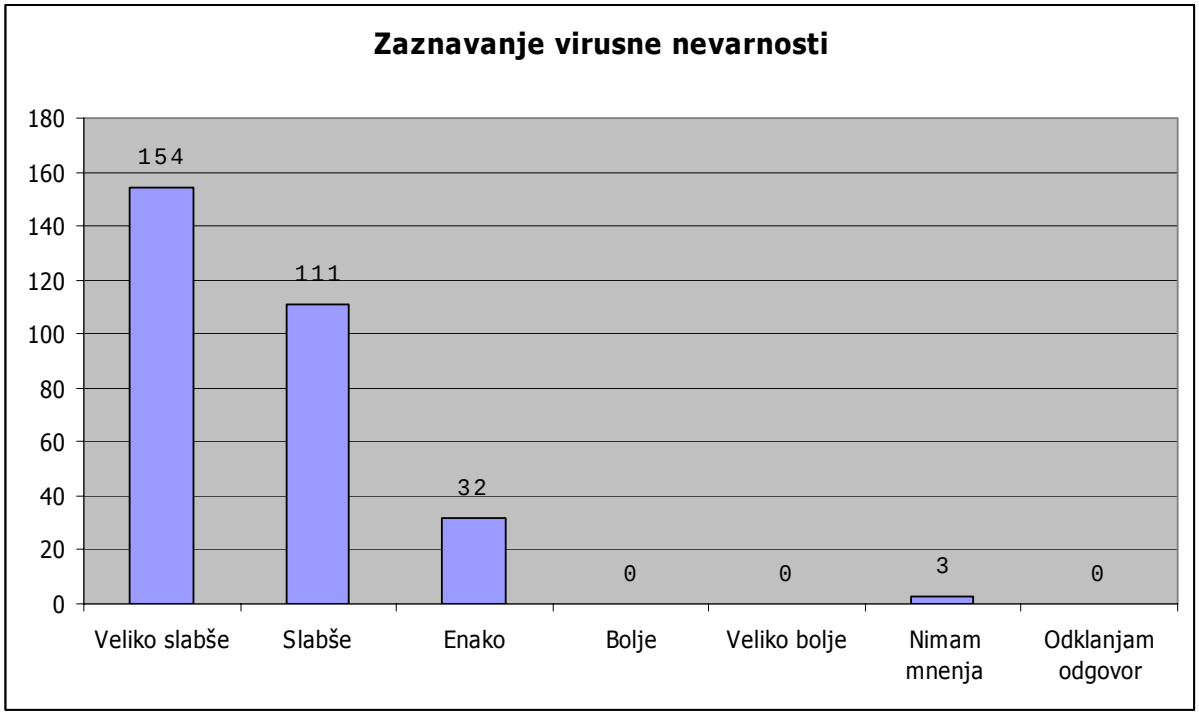
3.3.1.2 Možnosti virusne katastrofe

Za virusno katastrofo se šteje epidemijo, v kateri je virus ali škodljiva koda istočasno okužila 25 ali več osebnih računalnikov ter strežnikov oziroma je bila povzročena velika škoda ali finančna izguba organizaciji. Pri zadnjem kriteriju so anketirani tudi opisali razsežnost virusne katastrofe kot: število okuženih računalnikov, izgubo podatkov, izgubo produktivnosti, izgubo dohodka itd. Po teh definicijah je virusno katastrofo v letu 2003 prijavilo 92 od 300 obravnavanih podjetij.

3.3.1.3 Zaznavanje virusne nevarnosti

Anketirani so izražali tudi lastno zaznavanje splošne virusne nevarnosti v letu 2003 glede na preteklo leto. Lestvica odgovorov je bila razdeljena na odgovore od »veliko slabše« do »veliko boljše«. Na sliki 3 so predstavljeni odgovori anketiranih, ki v veliki večini (88 odstotkov) menijo, da je splošno stanje virusne nevarnosti veliko slabše kot v predhodnem letu, le 12 odstotkov podjetij namreč meni, da se stanje ni poslabšalo ali da se je izboljšalo. Slednji odstotek je najnižji v vseh letih, odkar svoje letne raziskave izvaja laboratorij ICSA Labs.

Slika 3: Zaznavanje virusne nevarnosti v letu 2003



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.4 PODROBNE UGOTOVITVE

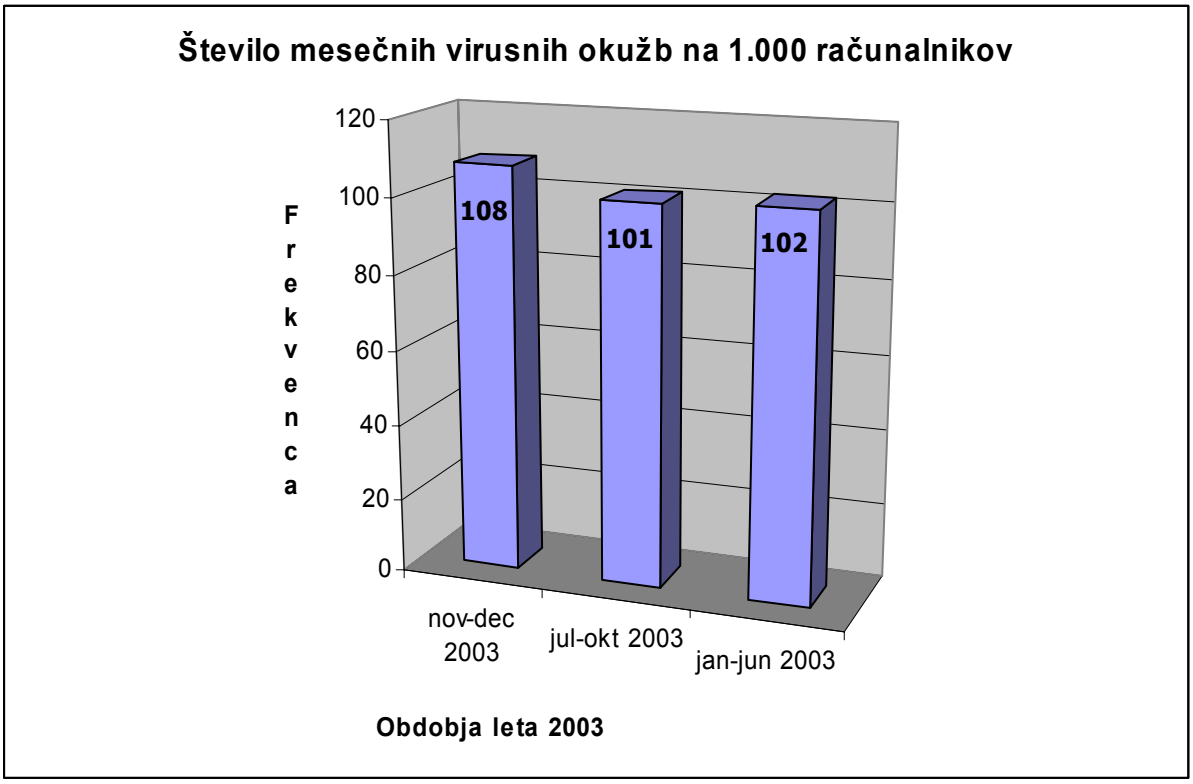
3.4.1 Spremenljivi vidiki razširjenosti računalniških virusov

Primarni cilj vsakoletnega dela raziskovalcev skupine ICSA Labs je odgovoriti na vprašanje, kako se razširjenost računalniških virusov spreminja skozi čas. Končne ugotovitve vsako leto razkrijejo veliko novosti, pomembnih za razumevanje virusnih problemov in ključnih za njihovo odpravljanje. Trendi kažejo vsakoletno rast okužb z računalniškimi virusi in škodljivimi kodami, zaskrbljujoč podatek pa predstavljajo vedno hujše posledice na poslovanje podjetja in povzročena škoda. Virusne nevarnosti se moramo zavedati in proti njej ukrepati z vsemi možnimi sredstvi in prijemi, saj tudi novodobni virusi pri svojih napadih/izbruhih ne prizanašajo in se poslužujejo vseh možnih načinov okužb in širjenja.

3.4.2 Virusne okužbe

Kot rečeno, raziskava ICSA Labs vsako leto poroča o porastu virusnih okužb. Tudi obdobje med januarjem in decembrom 2003 te ugotovitve potrjuje. Na sliki 4 je predstavljeno povprečno število okužb v obravnavanih mesecih.

Slika 4: Povprečno mesečno število virusnih okužb na 1.000 računalnikov v letu 2003



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.4.3 Lestvica najpogostejših virusov

Računalniški virusi se med seboj lahko zelo razlikujejo glede na razširjenost. Lastnosti računalniških virusov, ki vplivajo na razširjenost, so naslednje: vrsta virusa, možnosti okužb in virusna škoda. Virusi, ki se širijo preko elektronske pošte, v zadnjih letih močno prevladujejo po razširjenosti, medtem ko so preprosti makro virusi v upadanju, virusi na zagonskih sektorjih pa so popolnoma izginili iz statistik novega tisočletja. Obravnavana podjetja so poročala o svojih okužbah z računalniškimi virusi. Zaradi velikega števila računalniških virusov ter še večjega števila različic[12] in ob pomanjkanju standardiziranega identifikacijskega sistema[13] anketirani v določenih primerih niso mogli podati gotovih podatkov o virusni okužbi. V teh primerih so raziskovalci ICSA Labs iz delnih podatkov o imenih ter posledicah virusne okužbe skušali razbrati, za katero vrsto virusa gre oziroma vsaj v katero družino virusov okužba sodi.

Leto 2003 je postreglo z opaznim povečanjem hudih virusnih okužb, zvrstili so se številni virusni izbruhi. Še več, številni novi virusi so dosegli širše okužbe, ki bi jih v prejšnjih letih postavile na lestvico najpogostejših 10 virusov, a jih v tokratni lestvici ni. To samo priča o

[12] Poznanih je več kot 70.000 virusnih različic.

[13] Leta 1991 je skupina varnostnih strokovnjakov iz organizacije CARO (Computer Anti-Virus Research Organization) razvila shemo poimenovanja virusov, ki jo je še istega leta predstavila na konvenciji NVNC '91 (New Virus Naming Convention). Predstavljeno shemo in formuliranje poimenovanja računalniških virusov po vzorcu »Družina_virusov.Skupina_virusov.Različica« danes uporablja večina podjetij in strokovnih ustanov. Konsistentnost podatkov je tako v zadnjih letih vse večja, a dejstvo je, da standardiziranega identifikacijskega sistema poimenovanja računalniških virusov v vsej protivirusni industriji preprosto ni.

nevarnostih, ki jih novi virusni izbruhi prinašajo – vsak nov virus je še bolj dodelan, bolj škodljiv, težje izsledljiv in odstranljiv. V tabeli 5 je predstavljenih 10 najpogostejših virusnih okužb v letu 2003. Podatki za okužbe na lestvici od 1 do 10 veljajo za 1.000 računalnikov.

Tabela 5:

Lestvica 2003	Virus	Število okužb
1	W32/Yaha	32
2	W32/Klez	29
3	W32/Mimail	22
4	W32/BugBear	18
5	W32/SirCam	12
6	W32/Sobig	7
7	W32/Dumaru	6
8	W32/Swen	5
9	W32/Lovgate	4
10	W32/Blaster	2

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Velja omeniti, da se kar 9 izmed 10 virusov, ki se nahajajo na lestvici najpogostejših virusov v letu 2003, širi preko elektronske pošte. Edina izjema je črv W32/Blaster, ki se samodejno širi preko lokalnih omrežij ter interneta.

3.4.4 Virusne katastrofe

Anketirana podjetja so na vprašanje »Ali je vaše podjetje doživelo virusno katastrofo v letu 2003?« v 92 primerih (31 odstotkov) odgovorila pritrdilno. Podrobnosti o odgovorih so v tabeli 6.

Tabela 6: Podatki o virusnih katastrofah v letu 2003

Odgovor	Frekvenca
Da	92
Ne	192
Ne vem	16
Odklanjam	0
Skupaj	300

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.4.4.1 Časovni okvir virusnih katastrof

Raziskava je merila tudi pogostost virusnih katastrof po posameznih mesecih. Tabela 7 obravnava njihovo frekvenčno porazdelitev v koledarskem letu 2003.

Tabela 7: Časovna porazdelitev virusnih katastrof

Mesec zadnje virusne katastrofe	Odgovor	Odstotek
januar 2003	11	12
februar 2003	3	3
marec 2003	2	2
april 2003	1	1
maj 2003	4	4
junij 2003	2	2
julij 2003	2	2
avgust 2003	39	42
september 2003	3	3
oktober 2003	8	9
november 2003	7	8
december 2003	10	11

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Kot je razvidno iz tabele 7, so raziskovalci zaznali vsaj eno virusno katastrofo v vsakem mesecu leta 2003, kar se je pripetilo prvič, odkar ICSA Labs izvaja svojo vsakoletno raziskavo. Opazni sta dve večji odstopanji (špici), in sicer v mesecu januarju ter avgustu 2003. Januarsko odstopanje gre pripisati izbruhu črva W32/Slammer ter pojavu prvih različic črvov Lirva ter SoBig. Mesec avgust je bil s stališča virusnih katastrof eden najslabših doslej. Med glavne škodljivce v avgustu so se vpisale različice črvov Blaster, Nachi, SoBig ter Mimail.

3.4.4.2 Virusi, ki so povzročili zadnje virusne katastrofe

Podjetja so strokovnjakom ICSA Labs posredovala tudi podatke o virusih, ki so povzročili virusne katastrofe (večje okužbe). V tabeli 8 so navedeni najbolj aktivni virusi, frekvenca njihovih okužb ter domet – število okuženih računalnikov.

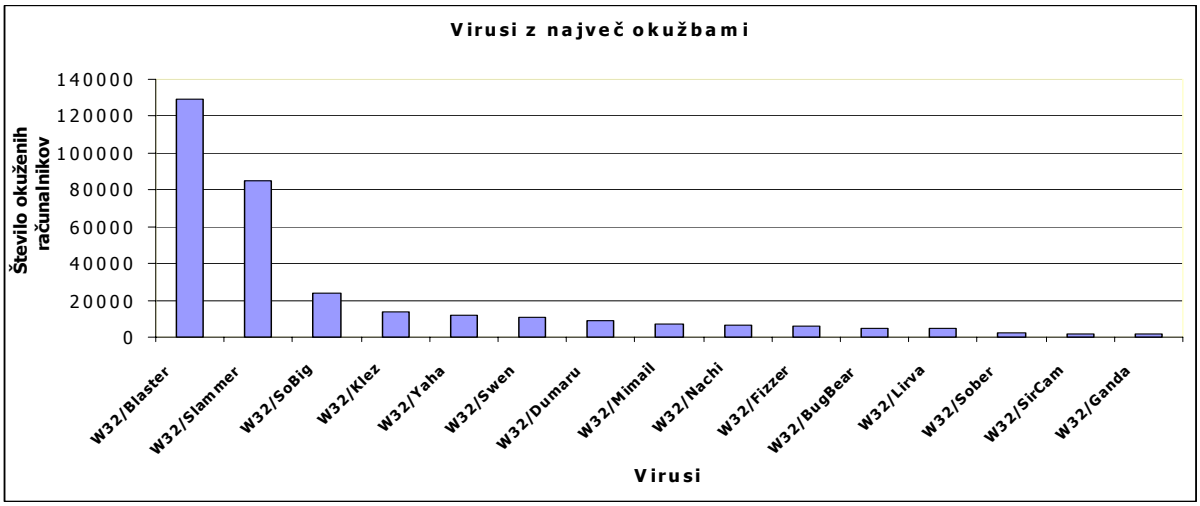
Tabela 8: Virusi z največ okužbami v letu 2003

Virus	Frekvenca okužb	Število okuženih računalnikov
W32/Blaster	12	129087
W32/Slammer	16	84921
W32/SoBig	6	23761
W32/Klez	10	13997
W32/Yaha	5	11799
W32/Swen	7	10760
W32/Dumaru	4	8697
W32/Mimail	9	7011
W32/Nachi	3	6325
W32/Fizzer	2	5768
W32/BugBear	5	4987
W32/Lirva	2	4732
W32/Sober	2	2106
W32/SirCam	8	2091
W32/Ganda	1	1893

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Na sliki 5 si oglejmo še grafični prikaz vrednosti iz tabele 8. Skupno število v virusnih katastrofah okuženih računalnikov je v letu 2003 znašalo 317.935.

Slika 5: Virusi z največ okužbami v letu 2003



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Računalniški virus W32/Blaster, znan tudi pod vzdevki MSBlast, Lovsan ter Poza, je torej v letu 2003 okužil največ računalnikov v ameriških podjetjih pa tudi drugod po svetu. Virus izkoristi napako prekoračitve pomnilnika (ang. buffer overrun) in na računalnikih z nameščenim operacijskim sistemom MS Windows XP ali Windows 2003 začne izvajati proces ponovnega zagona, na sliki 5 je tudi grafična ponazoritev izpisanega sporočila o napaki. Izpiše se naslednje obvestilo o napaki (v angleškem jeziku): »This system is being shut down in 60 seconds by NT Authority/System due to an interrupted Remote Procedure Call (RPC)«. Besedilo je izpisano v jeziku operacijskega sistema Microsoft Windows.

Slika 6: Proces ponovnega zagona zaradi napake prekoračitve pomnilnika

Vir: F-Secure: Opisi virusov, 2004.

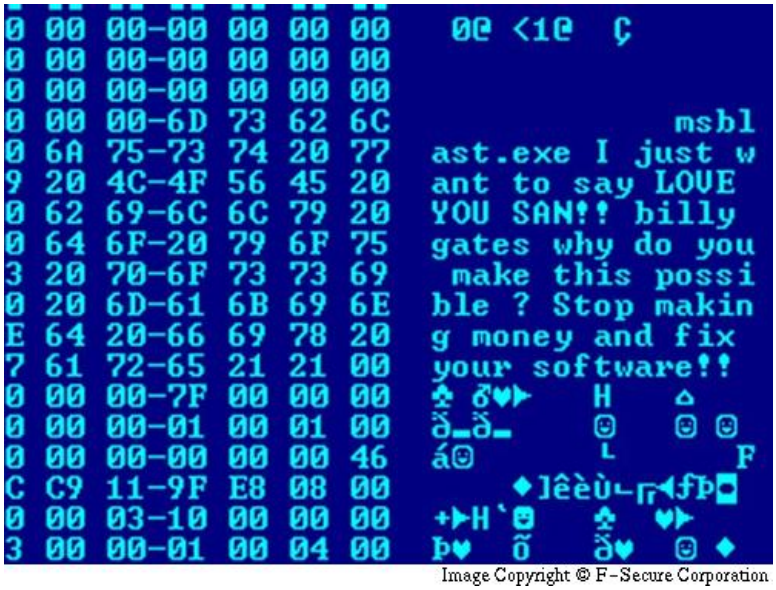
Zanimiv je tudi način širjenja omenjenega virusa. Virus namreč okuži računalnike na zaporednih naslovih z naključno izbranim začetnim naslovom. Algoritem daje prednost računalnikom z IP naslovi v bližini okuženega računalnika. IP naslovi so naslednje oblike: A.B.C.D. Virus najprej prebere IP naslov okuženega računalnika. Zatem se z izbiro naključne številke med 1 in 20 odloči ali bo okužil lokalne ali naključno izbrane računalnike. Če je naključno izbrana številka večja ali enaka 12, uporabi lokalno številko. Če je C večji od 20, od številke odšteje 20. D je vedno 0. Če virus izbere naključno številko, se A, B in C generirajo naključno v območjih: A od 1 do 254, B od 0 do 253, C od 0 do 253, D pa je vedno 0. Z uporabo teh naslovov Blaster prične pregledovati računalnike, po 20 zaporednih računalnikov hkrati. Poizkusi se povezati na vrata 135 vseh 20 računalnikov in preverja, če je bila povezava uspešna. Za širjenje preko napake DCOM uporablja dva načina, enega za Windows 2000 in drugega za Windows XP. Če uspe izkoristiti napako, odpre na napadenem računalniku povezavo in z uporabo protokola TFTP (ang. Trivial File Transfer Protocol) prekopira svojo kodo. Zatem se na napadenem računalniku požene.

Računalniki, okuženi z virusom Blaster, pošiljajo velike količine prometa na naslov windowsupdate.com. Pakete dolžine 40 znakov pošiljajo vsakih 20 tisočink sekunde na vrata 80. To lahko povzroči nedelovanje napadenega strežnika. Microsoft je zato 15. avgusta 2003 spletni naslov windowsupdate.com ukinil, tako da virus ne bo mogel napasti Microsoftovih strežnikov. To priča o moči, ki jo avtorji škodljivih kod dejansko imajo. Z virusom Blaster so avtorji dobesedno prisilili velikana iz Redmonda[14], da je ukinil svoje spletno mesto windowsupdate.com in začel z novim izboljšanim projektom prenove portala za vzdrževanje in posodabljanje svojih operacijskih sistemov MS Windows. Najnovejša, v tem trenutku peta različica portala je dostopna na spletnem naslovu http://v5.windowsupdate.microsoft.com.

Virus Blaster vsebuje besedila kot na primer:
»I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!«

Grafična ponazoritev sporočila kot dela virusne kode se nahaja na sliki 7.

Slika 7: Primer sporočila virusa Blaster, različica Lovsan



Vir: F-Secure: Opisi virusov, 2004.

[14] Microsofta.

3.4.5 Posledice virusnih katastrof

Virusi lahko povzročijo številne negativne posledice. Virusna okužba lahko povzroči nedosegljivost strežnikov, kar ima za posledico paralizirano delovanje večine procesov in aktivnosti v podjetju. V primeru, da strežniki niso dosegljivi zunaj niti znotraj organizacije, nastajajo veliki stroški, še posebej pri današnjih »spletnih podjetjih« (ang. dot com). Tu se podjetja soočajo predvsem s stroški izgubljenih priložnosti, zmanjšanega ugleda, zaradi nedosegljivosti strežnika/ov pa ostanejo začasno brez dela tudi zaposleni. Stroški neaktivnosti zaposlenih so lahko še kako visoki, a težko merljivi. Padec produktivnosti je še ena izmed negativnih posledic virusnega napada. Pri odstranjevanju okužbe z računalniškimi virusi nastajajo stroški dela. Virusne okužbe lahko privedejo tudi do izgube podatkov ali razkritja zaupnih podatkov tretjim osebam. To pa lahko za posamezno podjetje pomeni tudi splošno katastrofo in v najhujših primerih tudi prenehanje delovanja, propad. Občutek varnosti, tudi pred računalniškimi virusi, se še kako pozna na organizacijski klimi v podjetju.

3.4.5.1 Nedosegljivost strežnikov

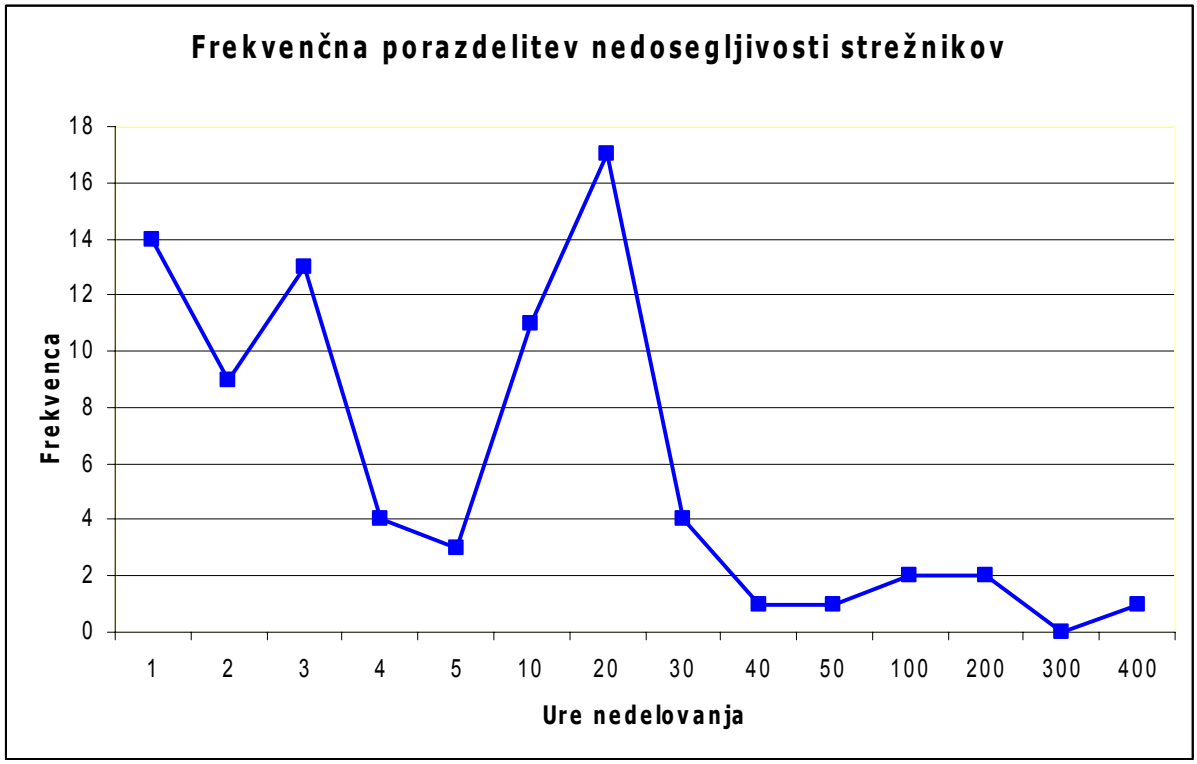
Srednja in velika ameriška podjetja niso imuna na virusne napade. Tudi sama neredko doživijo in preživijo virusno katastrofo. Po podatkih raziskave ICSA Labs je najbolj pereča težava sistemskih administratorjev v podjetjih ob virusnih napadih nedosegljivost strežnikov, ki dobesedno paralizira poslovanje posameznega podjetja. Nedosegljivost strežnikov kot posledico virusnega napada je namreč navedlo kar 82 podjetij. V tabeli 9 in na sliki 8 je predstavljen vzorec odgovorov na vprašanje o času nedosegljivosti strežnikov. V povprečju so bili strežniki v letu 2003 nedosegljivi 17 ur, v dobrih dveh tretjinah prizadetih podjetij pa so strežnike povrnili v prvotno stanje v manj kot desetih urah.

Tabela 9: Frekvenčna porazdelitev nedosegljivosti strežnikov

Ure nedelovanja	Frekvenca	Kumulativa (%)
1	14	17
2	9	28
3	13	44
4	4	49
5	3	52
10	11	66
20	17	87
30	4	91
40	1	93
50	1	94
100	2	96
200	2	99
300	0	99
400	1	100
Skupaj	**82**	**100**

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 8: Frekvenčna porazdelitev nedosegljivosti strežnikov



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.4.5.2 Stroški dela, nastali kot posledica virusnih katastrof

Podjetja, ki jih je v letu 2003 doletela virusna katastrofa, so tudi ovrednotila stroške dela, ki so nastali v procesu odpravljanja virusnih okužb. Pri tem je bilo dejavno predvsem osebje, ki v podjetjih skrbi za brezhibno delovanje informacijskega sistema. Podatki, podani v tabeli 8, so merjeni v številu posameznih delavnikov, ki jih je podjetje potrebovalo za odpravo težav, povzročenih s strani računalniških virusov. Za posamezni delavnik se šteje povprečno število delovnih ur delavca v podjetju, v ZDA ga merijo s kriterijem »person-day«. Ustrezni slovenski kriterij bi bil delavec-dan, torej posamezni delavnik v obsegu 8 delovnih ur.

Podatke o nastalih stroških odprave virusnih okužb je posredovalo 82 podjetij ali 89 odstotkov vseh podjetij, ki so potrdila, da so leta 2003 doživela virusno katastrofo. Kot je razvidno iz tabele 9, je polovica podjetij potrebovala do deset posameznih delavnikov za odpravo nastalih težav, v povprečju pa so podjetja iz ZDA potrebovala dobrih 24 posameznih delavnikov (mediana je znašala 11 posameznih delavnikov). To pomeni, da je bilo v povprečju potrebno pokriti stroške dela 24 delavcev (informatikov), ki so probleme, nastale z okužbami računalniških virusov, rešili v enem dnevu.

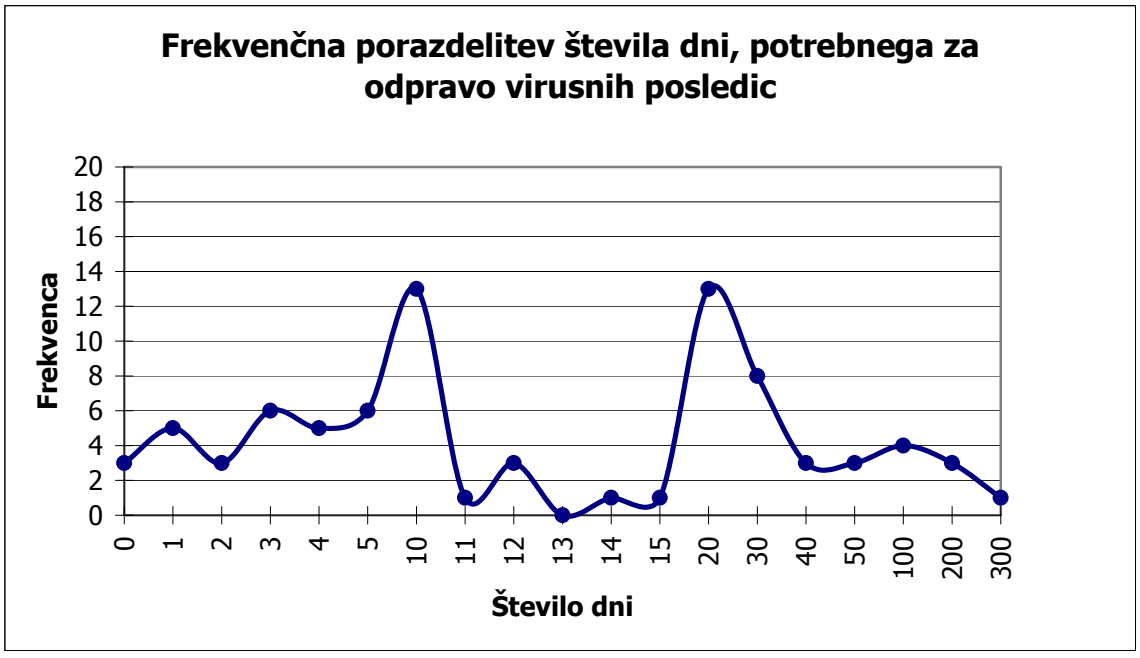
Tabela 10: Frekvenčna porazdelitev števila dni, potrebnih za odpravo virusnih posledic

Število dni	Frekvenca	Odstotek
0	3	4
1	5	6
2	3	4
3	6	7
4	5	6
5	6	7
10	13	16
11	1	1
12	3	4
13	0	0
14	1	1
15	1	1
20	13	16
30	8	10
40	3	4
50	3	4
100	4	5
200	3	4
300	1	1
Skupaj	**82**	

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Na sliki 9 je frekvenčna porazdelitev števila dni, potrebnih za odpravo virusnih posledic, prikazana še v grafični obliki. Najbolj opazni sta odstopanji (špici) pri vrednostih 10 in 20 posameznih delavnikov.

Slika 9: Frekvenčna porazdelitev števila dni, potrebnih za odpravo virusnih posledic



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.4.5.3 Stroški organizacije zaradi računalniških virusov

Enako so raziskovalci pri ICSA Labs poizvedovali o oceni vseh stroškov, ki jih je podjetje oziroma organizacija utrpela zaradi posameznega (zadnjega) virusnega napada. Ker gre za skupne stroške, vanje sodijo težave s strojno opremo, stroški odpravljanja virusov, stroški »neaktivnosti« ostalih zaposlenih, padec produktivnosti, izgubljene priložnosti itd. Ocene, ki so jih posredovala podjetja v ZDA, se nahajajo v tabeli 11.

Tabela 11: Ocena stroškov virusnega napada

Stroški v USD	Frekvenca	Odstotek
2.500	2	2
3.000	0	0
5.000	12	15
10.000	19	23
20.000	9	11
30.000	9	11
40.000	6	7
50.000	5	6
100.000	8	10
200.000	4	5
300.000	1	1
400.000	1	1
500.000	1	1
1.000.000	3	4
>1.000.000	2	2

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

V povprečju so ameriška srednja in velika podjetja ob virusnem napadu v letu 2003 utrpela za 99.000 ameriških dolarjev škode, oziroma stroškov. Mediana zbranih podatkov znaša 11.000 USD, medtem ko je bilo največ podjetij, ki ocenjujejo, da jih je zadnji virusni napad olajšal za 10 tisoč ameriških dolarjev. Grafična ocena stroškov virusnih napadov je na sliki 10.

Glede na prejšnja leta stroški povezani z virusnimi izbruhi naraščajo, leta 2002 so povprečni stroški virusnega napada po ocenah podjetij znašali 81 tisoč USD. Povečalo se je tudi število podjetij, ki so utrpela največjo škodo, torej milijon dolarjev ali več. Omenjeni podatek kaže na dejstvo, da je v organizacijah z veliko računalniki in več omrežji potrebno vložiti tudi veliko več napora ter sredstev v odstranjevanje računalniških virusov v primeru, če pride do okužbe. Strokovnjaki so tudi mnenja, da bodo stroški virusnih katastrof v bodoče še naraščali, vse do uvedbe novih varnostnih ukrepov na področju strojne in programske opreme. Novejši računalniški virusi so namreč vse bolj kompleksni in jih je tudi vse težje odstraniti, pa tudi posledice, ki sledijo okužbam so bistveno bolj hude kot pred desetletjem (Bennet, 2004).

Slika 10: Ocena stroškov virusnega napada

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.5 VPLIVI VIRUSOV NA POSLOVANJE PODJETJA

V naslednjih tabelah je navedenih nekaj neposrednih in posrednih stroškov, ki so posledica virusnih katastrof. Nekateri izmed njih so težko merljivi, druge pa le redke analize in študije upoštevajo pri svoji kvazi celoviti oceni. Študija ICSA Labs upošteva kar najširši spekter vplivov virusov na poslovanje podjetja, čeprav sami strokovnjaki opozarjajo, da so odgovori, ki jih prejemajo od podjetij, večkrat podcenjeni.

3.5.1 Učinki napada virusov na poslovanje

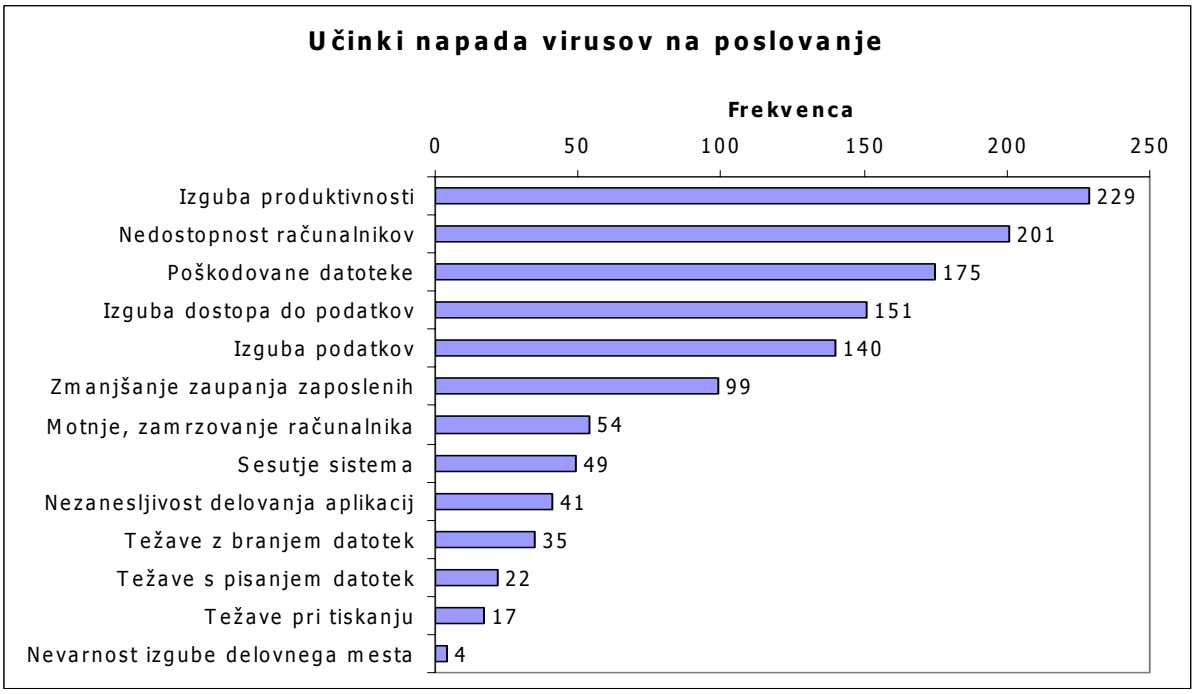
Virusne katastrofe in razvejanost incidentov ter okužb z raznimi črvi kažejo svoje posledice povsod. V denarju oziroma stroških, na zaposlenih ter tudi organizacijski klimi v podjetju. Po izkušnjah ameriških podjetij se posledice napada virusov odražajo predvsem v nižji produktivnosti, nedostopnosti računalnikov in izgubi podatkov. Podrobnejša razdelitev se nahaja v tabeli 12, podjetja pa so lahko v svojih odgovorih navedla več učinkov, pač tiste, za katere so opazila, da so se pojavili tudi pri njih.

Tabela 12: Učinki napada virusov na poslovanje

Učinek	Frekvenca	Odstotek
Izguba produktivnosti	229	76
Nedostopnost računalnikov	201	67
Poškodovane datoteke	175	58
Izguba dostopa do podatkov	151	50
Izguba podatkov	140	47
Zmanjšanje zaupanja zaposlenih	99	33
Motnje, zamrzovanje računalnika	54	18
Sesutje sistema	49	16
Nezanesljivost delovanja aplikacij	41	14
Težave z branjem datotek	35	12
Težave s pisanjem datotek	22	7
Težave pri tiskanju	17	6
Nevarnost izgube delovnega mesta	4	1

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 11: Učinki napada virusov na poslovanje



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6 PROTIVIRUSNA ZAŠČITA

Boj z računalniškimi virusi bijejo protivirusni programi. Kot namiguje že njihovo ime, protivirusni programi odkrivajo in odstranjujejo vse vrste omenjenih zlonamernih kod, ki predstavljajo grožnjo računalnikom. Zaradi vse bolj prefinjenih tehnik računalniških virusov se morajo protivirusni programi razvijati na enak način kot tehnologija, ki ustvarja zlonamerne programske kode. Zato je bistvenega pomena, da protivirusni programi dnevno posodabljajo datoteke z opisi virusov in redno nadgrajujejo pregledovalni stroj. Novi načini, na katere se virusi širijo, in vse večje grožnje hekerskih napadov so prav tako dejavniki, ki govorijo v prid uporabi protivirusnih programov. Protivirusni programi v kombinaciji s požarnim zidom so namreč najbolj sposobni preprečevati te nevarnosti.

3.6.1 Izvor računalniških virusov

Raziskovalci ICSA Labs že od svoje prve raziskave iz leta 1996 sledijo izvoru virusnih okužb. Podjetja tako izpolnijo vprašalnik, ki jim nudi več možnosti odgovorov, kako je do okužbe z računalniškim virusom prišlo. Zaradi tega so tudi vsote posameznih let večje od 100 odstotkov. V tabeli 13 je podana primerjava izvora virusov od leta 1996 do leta 2003.

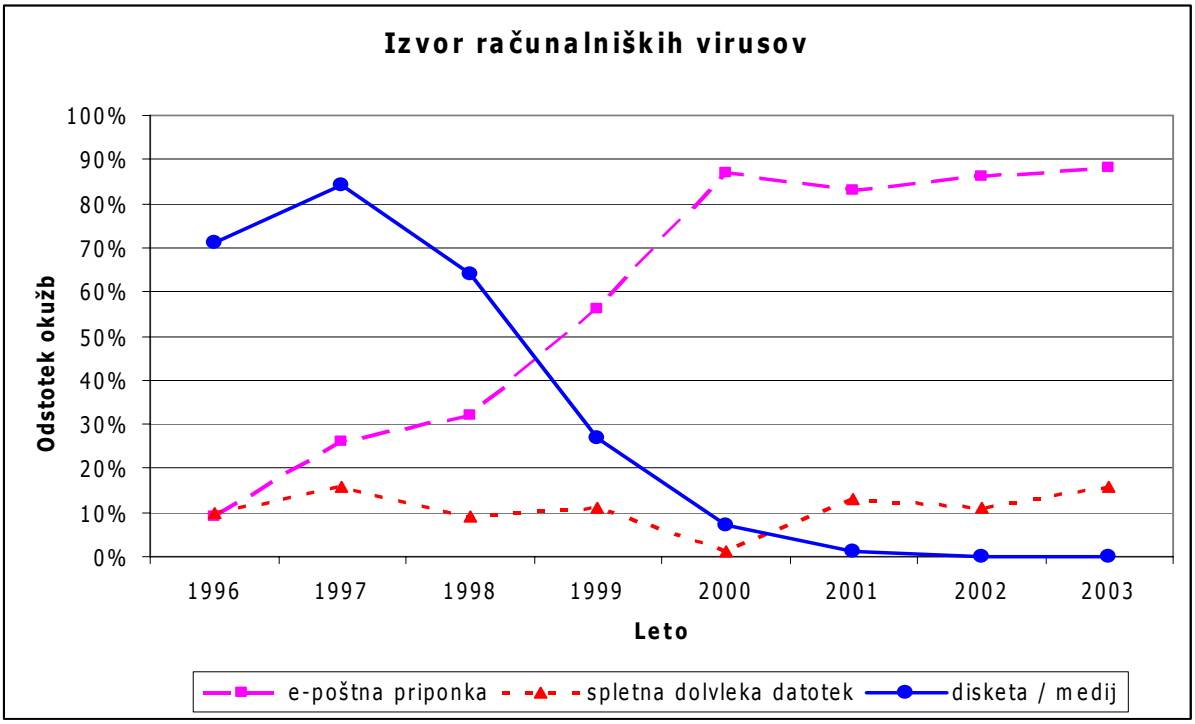
Tabela 13: Izvor računalniških virusov ter odstotek posameznih okužb po letih

Izvor virusa / Leto	1996	1997	1998	1999	2000	2001	2002	2003
e-poštna priponka	9	26	32	56	87	83	86	88
spletna dolvleka datotek	10	16	9	11	1	13	11	16
brskanje po spletu	0	5	2	3	0	7	4	4
neznan	15	7	5	9	2	1	1	3
drug izvor	0	5	1	1	1	2	3	11
distribucija programov	0	3	3	0	1	2	0	0
disketa	71	84	64	27	7	1	0	0

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Močno opazen je trend rasti virusnih okužb, ki se širijo z datotekami, pripetimi elektronskim sporočilom. Tovrstne okužbe močno dominirajo na lestvici najpogostejših virusnih okužb že od leta 2000. V porastu so tudi okužbe z računalniškimi virusi, ki so povezane s spletno dolvleko datotek. Slednje gre pripisati porastu programov za spletno izmenjavo datotek P2P (ang. peer-to-peer). Ta trend je pri domačih uporabnikih še veliko bolj očiten kot v podjetjih. V zadnjih letih se je močno zmanjšalo število okužb, ki so se v računalnik naselile s pomočjo diskete ali drugega pomnilniškega medija. Kljub temu virusna statistika občasno še zazna določene viruse na zagonskih sektorjih, a je njihovo število v globalnem merilu praktično zanemarljivo (nično). Na sliki 12 so tako zbrana najbolj očitna gibanja računalniških virusov, oziroma njihov izvor v zadnjem desetletju.

Slika 12: Izvor računalniških virusov



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6.2 Uporaba protivirusne zaščite

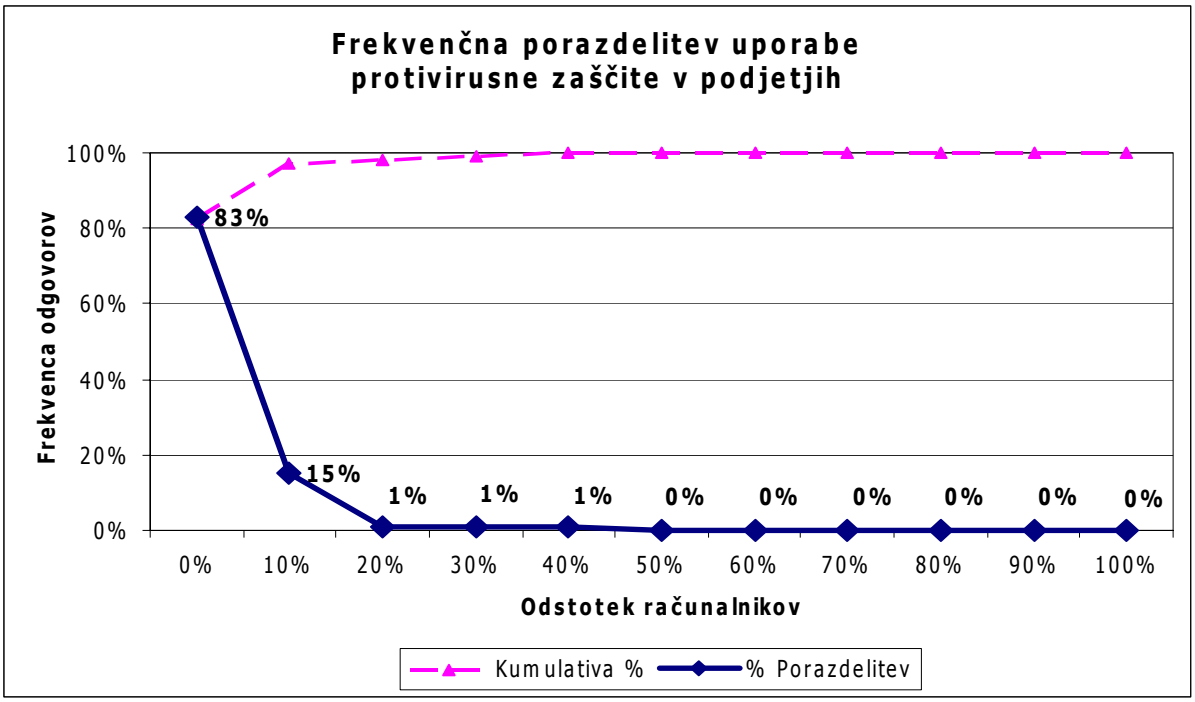
Podjetja se vedno bolj zavedajo pomena ustrezne protivirusne zaščite, ki jih varuje pred škodljivimi vplivi računalniških virusov. Večino zaščite predstavlja ustreza protivirusna programska oprema, predvsem protivirusni programi specializiranih varnostnih podjetij. Po podatkih raziskave ICSA Labs Computer Virus Prevalence Survey iz leta 2003 je kar 83 odstotkov izmed 300 podjetij imelo na vseh delovnih postajah nameščeno protivirusno programsko opremo. 90- ali večodstotno zaščito s protivirusnimi programi pa je javilo kar 98 odstotkov vseh podjetij. V tabeli 14 se nahaja frekvenčna porazdelitev uporabe protivirusne zaščite v podjetjih.

Tabela 14: Frekvenčna porazdelitev uporabe protivirusne zaščite v podjetjih

Porazdelitev	Frekvenca	Odstotek
0 %	249	83
10 %	45	15
20 %	2	1
30 %	2	1
40 %	2	1
50 %	0	0
60 %	0	0
70 %	0	0
80 %	0	0
90 %	0	0
100 %	0	0

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 13: Uporaba protivirusne zaščite na delovnih postajah



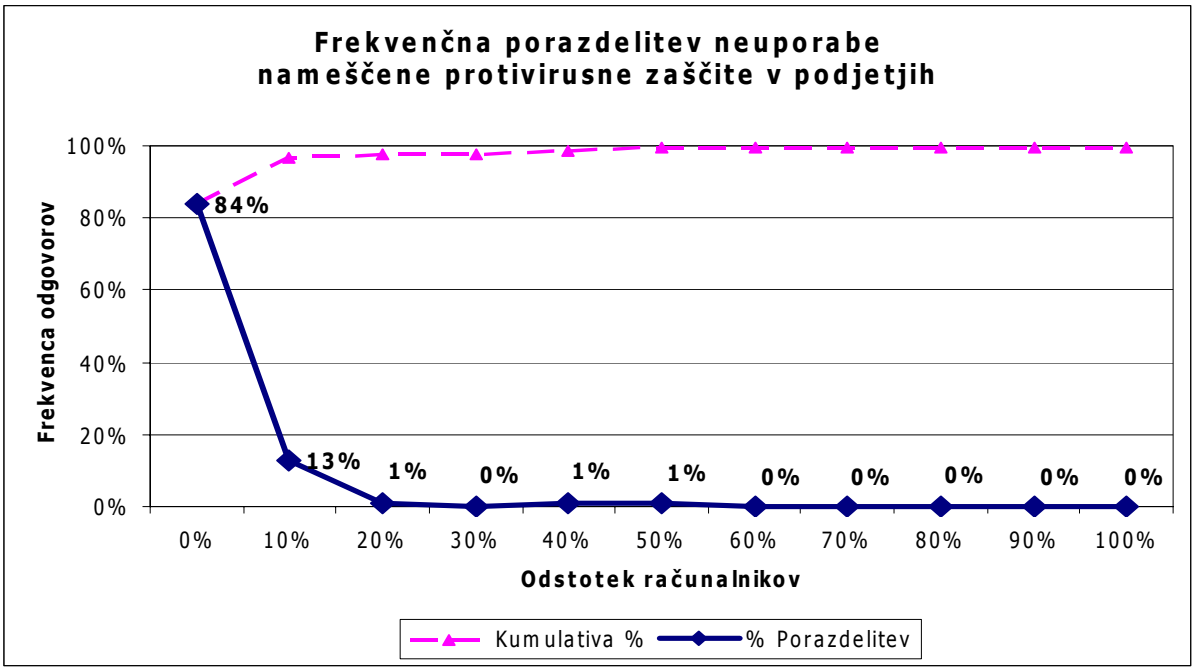
Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6.3 Neuporaba protivirusne zaščite

Raziskovalci so tudi leta 2003 preverjali morebitno neuporabo protivirusne programske opreme, torej število računalnikov, ki so sicer imeli nameščen protivirusni program, a le-ta zaradi različnih razlogov ni deloval. Zbrani podatki kažejo, da je le peščica računalnikov v podjetjih, ki ustrezajo omenjenemu kriteriju. Tako naj bi bilo računalnikov, ki sicer imajo nameščeno protivirusno programsko opremo, a le-ta ni aktivna, le manjši odstotek. Namreč kar 97 odstotkov podjetij meni, da je takšnih računalnikov v njihovi organizaciji manj kot desetina, 84 odstotkov podjetij pa je prepričanih, da so vsi njihovi računalniki ustrezno

zaščiteni s protivirusno programsko opremo in da le-ta brezhibno opravlja svoje delo. Rezultati iz leta 2003 tako kažejo bistveno izboljšanje glede na prejšnja leta, ko je bilo neustrezno opremljenih bistveno več računalnikov v podjetjih. Delno gre tak rezultat pripisati večjemu zavedanju in osveščenosti zaposlenih o virusnih nevarnostih, pa tudi sistemski administratorji so postali bolj pozorni na »sumljive« računalnike v svojih omrežjih. Nenazadnje je napredek očiten tudi pri proizvajalcih protivirusne programske opreme, ki so močno olajšali in izboljšali delo ter nadzor nad računalniki v podjetjih, tako da je spremljanje delovanja posameznih delovnih postaj veliko enostavnejše.

Slika 14: Neuporaba nameščene protivirusne zaščite na delovnih postajah



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6.4 Protivirusni programi na delovnih postajah

V tabeli 15 se nahajajo podatki o uporabi protivirusnih programov različnih proizvajalcev v podjetjih. Podatki o uporabi posameznih programov v podjetjih presegajo kumulativo 100 odstotkov, saj nekatera podjetja uporabljajo protivirusne programske rešitve različnih proizvajalcev.

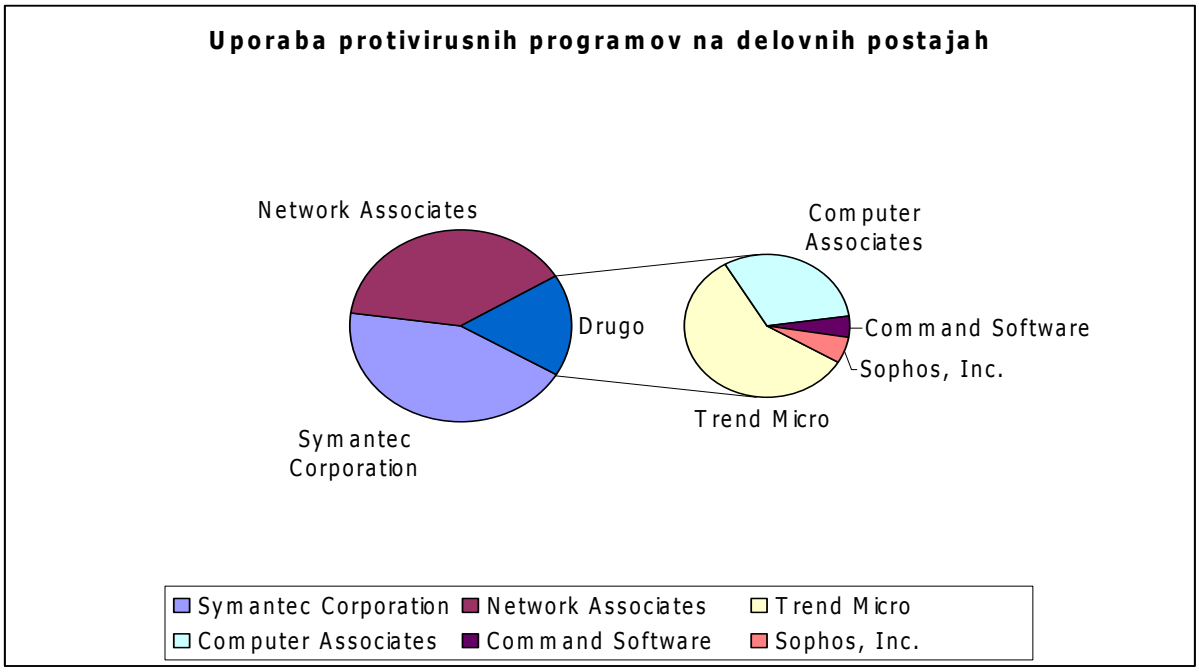
Tabela 15: Uporaba protivirusnih programov na delovnih postajah

Proizvajalec protivirusne programske zaščite	Število podjetij	Odstotek	Število delovnih postaj	Odstotek
Symantec Corporation	142	37	388698	43
Network Associates	131	34	355520	40
Trend Micro	47	12	89437	10
Computer Associates	41	11	47691	5
Command Software	11	3	7708	1
Sophos, Inc.	10	3	9103	1

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Kot je razvidno iz tabele 15, v ZDA prevladujejo predvsem protivirusne programske rešitve proizvajalcev Symantec Corporation (protivirusni program Norton Antivirus) ter Network Associates (protivirusni program McAfee VirusScan), ki si razdelita vsak dobrih 40 odstotkov namestitev po delovnih postajah. Stabilno tretji ostaja proizvajalec Trend Micro s protivirusnim programom PC-cillin, ki v ZDA pred računalniškimi virusi ščiti dobro desetino delovnih postaj v podjetjih. Omenjeni tržni deleži se z manjšimi spremembami ohranjajo že več let, kar kaže na dejstvo, da podjetja specializiranim varnostnim podjetjem zaupajo in ostajajo lojalna. Večjih migracij in zamenjav protivirusne programske zaščite med 300 obravnavanimi podjetji ni. Slika 15 predstavlja grafično ponazoritev podatkov iz tabele 15.

Slika 15: Uporaba protivirusnih programov na delovnih postajah v ZDA



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Raziskovalce ICSA Labs so seveda zanimali tudi načini ter metode zaščite, ki jih protivirusni programi omogočajo. V tabeli 16 so navedene najpogostejše metode varovanja pred računalniškimi virusi.

Tabela 16: Načini zaščite pred računalniškimi virusi v podjetjih

Način zaščite	Frekvenca
Uporabniki pregledujejo diskete ter datoteke	81
Protivirusni program preišče trdi disk ob vsakem zagonu	278
Protivirusni program preišče trdi disk ob vsaki prijavi	225
Protivirusni program je venomer aktiven (išče viruse) v ozadju	295
Drugi periodični načini odkrivanja virusov	102
Drugi realnočasovni načini odkrivanja virusov	30

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Raziskava v letu 2003 je pokazala, da večina podjetij (89 odstotkov) uporablja realnočasovno spremljanje dogajanja na računalniku, saj večina novejših protivirusnih programov takšno zaščito tudi omogoča. Sodobni računalniki namreč premorejo dovolj procesorske moči, da takšno sprotno spremljanje delujočih procesov in dela z datotekami ne vpliva na delovno produktivnost zaposlenih v podjetjih. Kar 74 odstotkov podjetij preišče morebitne virusne okužbe svojih računalnikov že ob zagonu.

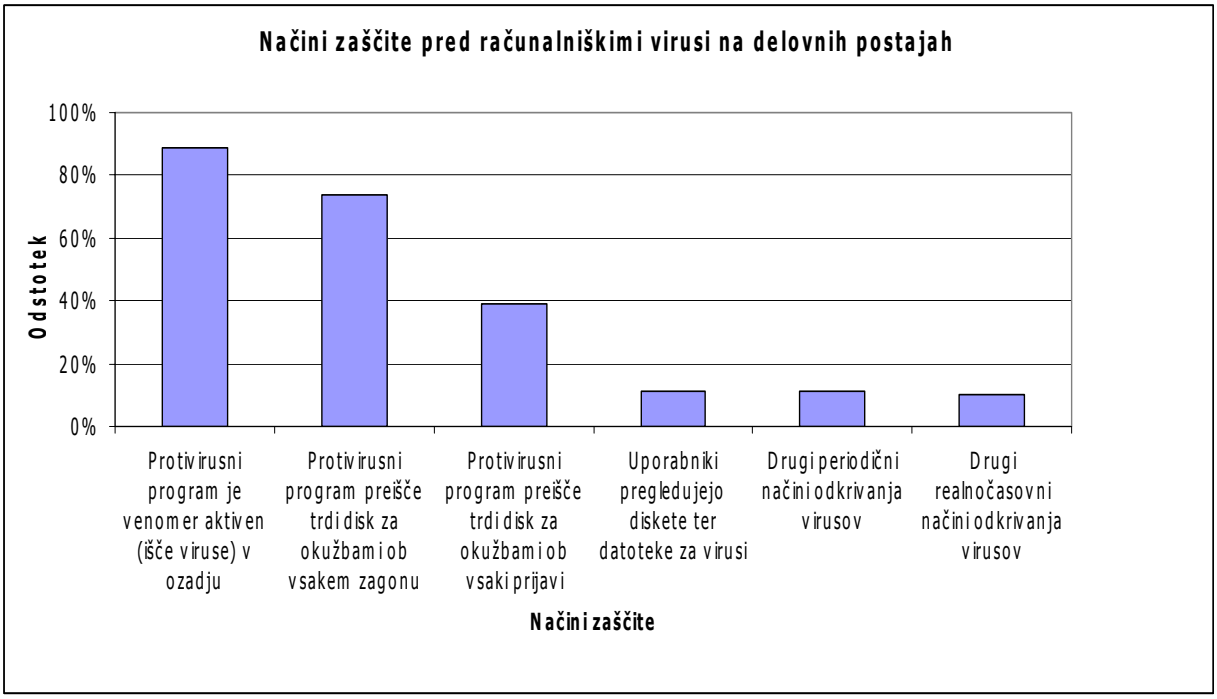
Še bolj zanimiv podatek kot število organizacij, ki uporablja posamezne načine zaščite pred virusnimi okužbami, je podatek o številu računalnikov, na katerih se izvajajo posamezne metode za preprečevanje okužb z računalniškimi virusi. V tabeli 14 so tako zbrani podatki o številu računalnikov, ki uporabljajo posamezno vrsto zaščite ter njihov odstotek med vsemi obravnavanimi računalniškimi sistemi v raziskavi ICSA Labs Computer Virus Prevalence Survey 2003. Podatki iz tabele 17 so za lažjo orientacijo grafično prikazani še na sliki 16.

Tabela 17: Načini zaščite pred računalniškimi virusi na delovnih postajah

Način zaščite	Število delovnih postaj	Odstotek
Protivirusni program je venomer aktiven (išče viruse) v ozadju	835979	89
Protivirusni program preišče trdi disk ob vsakem zagonu	695083	74
Protivirusni program preišče trdi disk ob vsaki prijavi	366328	39
Uporabniki pregledujejo diskete ter datoteke	103323	11
Drugi periodični načini odkrivanja virusov	103323	11
Drugi realnočasovni načini odkrivanja virusov	93930	10

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 16: Načini zaščite pred računalniškimi virusi na delovnih postajah

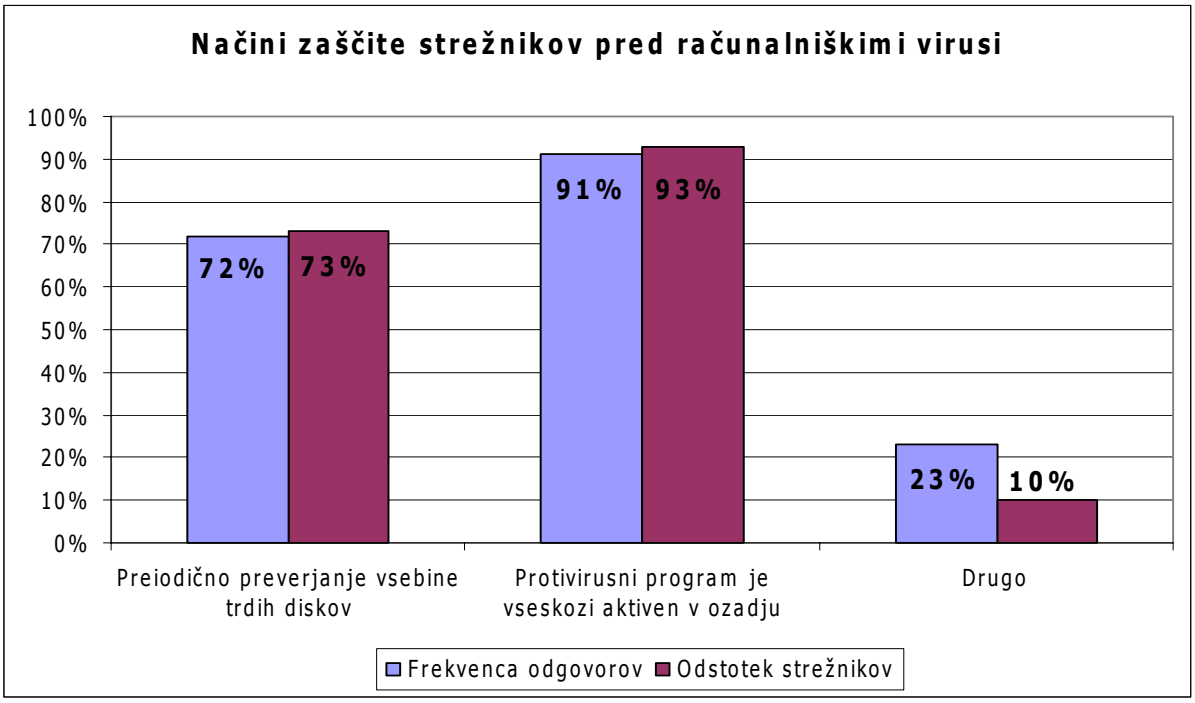


Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6.5 Protivirusni programi na strežnikih

Strežniki so za nemoteno delovanje podjetja bistveno pomembnejši od delovnih postaj. Na njih tečejo aplikacije in so shranjeni podatki, do katerih dostopa večje število delovnih postaj v podjetju. Če postane strežnik zaradi virusnega napada nedosegljiv, to pomeni, da so za čas do odprave težav neproduktivni tudi zaposleni na delovnih postajah, ki komunicirajo s tem strežnikom, saj ne morejo uporabljati vitalnih podatkov ter aplikacij. Podjetja se vse bolj zavedajo nevarnosti, ki grozijo strežnikom, zato je nivo zaščite le-teh vsako leto višji. Informatiki v podjetjih so raziskovalcem ICSA Labs posredovali tudi podatke o zaščiti strežnikov. Leta 2003 je tako velika večina podjetij, in sicer kar 93 odstotkov vseh podjetij, na svojih strežnikih uporabljala realnočasovno protivirusno zaščito. Ostali podatki o zaščiti strežnikov so predstavljeni na sliki 17.

Slika 17: Načini zaščite strežnikov pred računalniškimi virusi



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.6.6 Protivirusni programi na vstopnih točkah

Računalniki in oprema, ki se nahaja med posameznimi omrežji in je mejnik med internim omrežjem podjetja ter zunanjim svetom, je za delo podjetja ključna. Viruse je namreč potrebno zaustaviti že na vhodu, čeprav je slednje povezano z velikimi stroški. Toda stroški okužbe so lahko še večji, kot smo navedli v enem izmed zgornjih primerov. Strežniki za elektronsko pošto, proxy strežniki ter požarni zidovi so tako najbolj izpostavljeni zunanjim nevarnostim. V tabeli 18 je navedena stopnja zaščite posameznih točk/strežnikov.

Tabela 18: Frekvenčna porazdelitev zaščite vstopnih točk

Zaščita v odstotkih	E-poštni strežniki	Proxy strežniki	Požarni zidovi
100	281	177	151
90	11	14	22
80	2	2	0
70	0	1	0
60	2	0	0
50	1	3	1
40	0	0	0
30	0	0	0
20	0	0	1
10	0	0	0
0	3	103	125

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

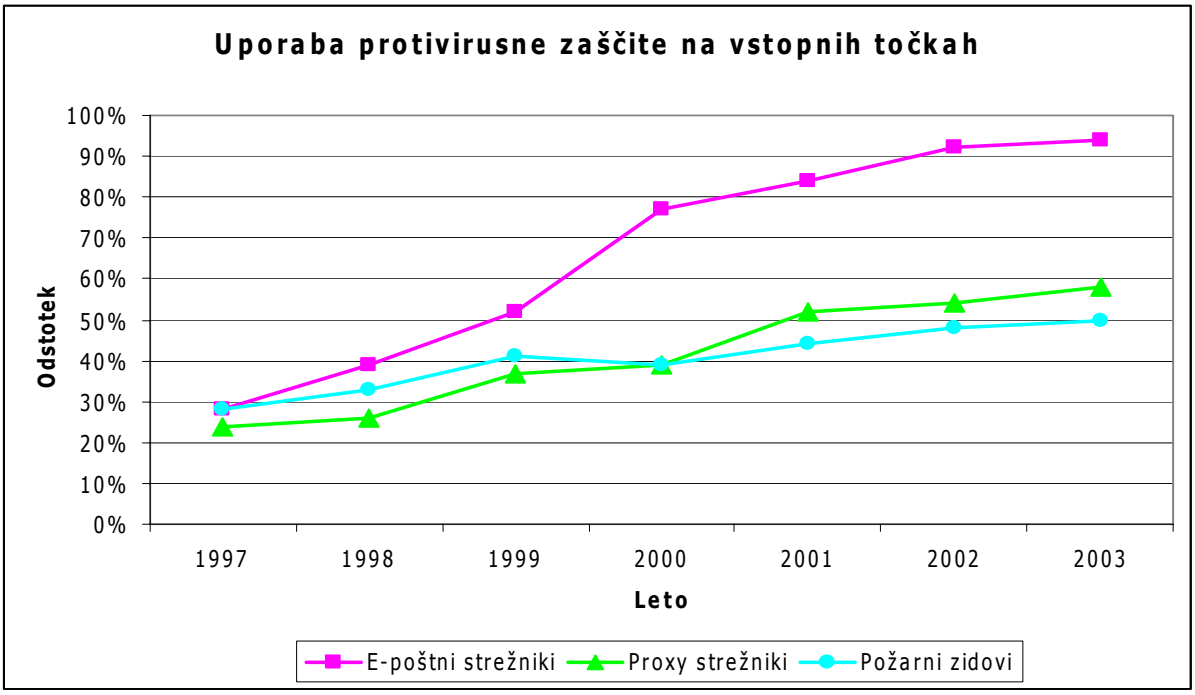
Podatki iz tabele 18 veljajo za leto 2003, a je enak dvoličen trend opazen že skozi vsa leta, kar ICSA Labs izvaja svojo raziskavo. Podjetja ali zaščitijo vse vstopne točke ali pa nobene, izjema so v zadnjem času le strežniki za elektronsko pošto, saj danes nedelujoč e-poštni strežnik za podjetje pomeni pravo katastrofo. Pri ostalih vstopnih točkah pa velja, da podjetij, ki bi imela stopnjo zaščite med 90 in 100 odstotki, skorajda ni.

Na sliki 18 je prikazana rast deleža protivirusne zaščite na vstopnih točkah od leta 1997 do 2003. Strokovnjaki so si že leta 1997 prizadevali za popolno zaščito vstopnih točk, njihova prizadevanja pa počasi, a vztrajno kažejo pozitivne rezultate. Zaradi številnih zlorab in virusnih napadov so bili prav strežniki za elektronsko pošto deležni večje protivirusne zaščite, ki je v zadnjih nekaj letih že presegla stopnjo 90 odstotkov vseh strežnikov. Leta 2002 je bilo tako ustrezno zaščitenih 92, leto kasneje pa že 94 odstotkov strežnikov za elektronsko pošto.

Počasneje, a kljub temu z vsakoletnim porastom, se podjetja odločajo namestiti protivirusno zaščito tudi na proxy strežnike ter požarne zidove. Ustrezno protivirusno opremljenih vstopnih točk je bilo v letu 2003 za več kot polovico, natančneje 50 odstotkov požarnih zidov ter 58 odstotkov proxy strežnikov je bilo varovano s protivirusno programsko opremo.

Kljub temu da zaščita vstopnih točk ni nadomestilo za zaščito lokalno lociranih strežnikov ter delovnih postaj, je eden ključnih nivojev celotne protivirusne zaščite in predstavlja pomembno mesto v načinu varovanja informacij v podjetju.

Slika 18: Uporaba protivirusne zaščite na vstopnih točkah



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

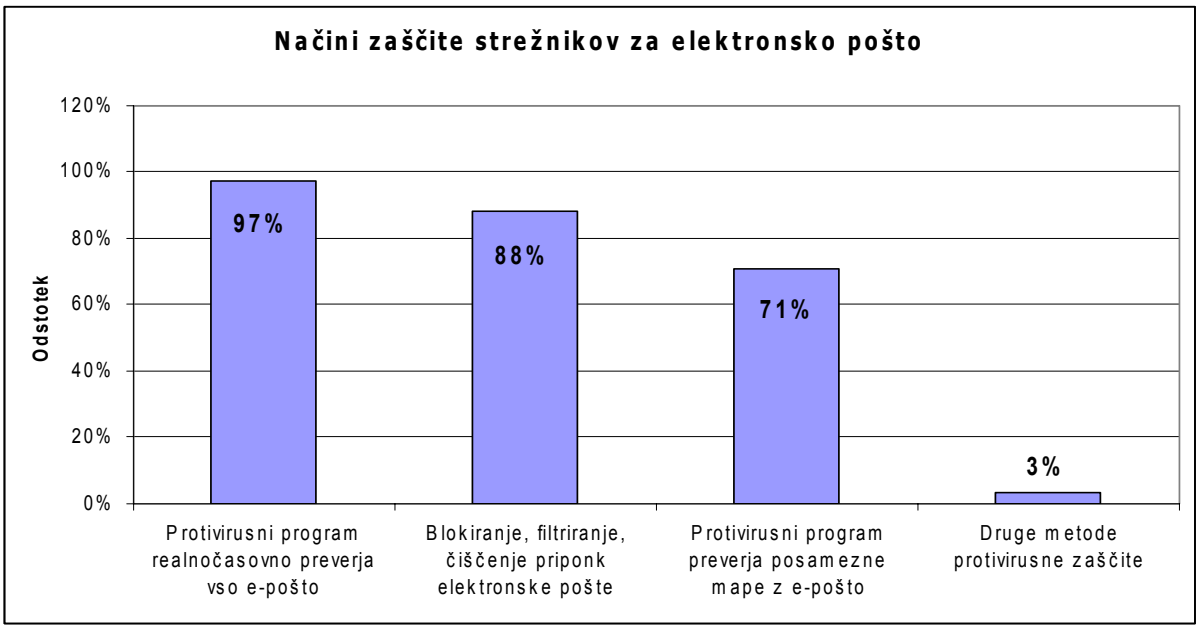
Podjetja so tudi objavila, na kakšne načine ščitijo svoje mejne strežnike pred nevarnostmi svetovnega spleta. V tabeli 19 se nahaja frekvenčna porazdelitev najpogostejših metod, ki se jih podjetja poslužujejo pri zaščiti strežnikov za elektronsko pošto pred virusnimi nevarnostmi. Grafična ponazoritev je prikazana na sliki 19.

Tabela 19: Načini zaščite strežnikov za elektronsko pošto

Način zaščite	Frekvenca
Protivirusni program realnočasovno preverja vso e-pošto	292
Blokiranje, filtriranje, čiščenje priponk elektronske pošte	264
Protivirusni program preverja posamezne mape z e-pošto	212
Druge metode protivirusne zaščite	10
Anketiranih podjetij	300

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 19: Načini zaščite strežnikov za elektronsko pošto



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

V tabeli 20 in na sliki 20 je enaka analiza kot v tabeli 19 in na sliki 19 opravljena za proxy strežnike v ameriških srednjih in velikih podjetjih. Proxy strežnik poganja program, narejen z namenom povečanja hitrosti dostopov, zmanjšanja zasedenosti povezav ter izboljšanja varnosti pri komunikacijah preko omrežja. Hitrost dostopov se poveča, ker uporabnik dobi datoteke iz proxy strežnika na najhitrejši možen način (lokalno omrežje). Zasedenost povezav se zmanjša, ker uporabniki dostopajo večinoma samo do proxy strežnika, manjša je obremenitev zunanjih povezav. Podatke o svojih proxy strežnikih in njihovi zaščiti je posredovalo 209 podjetij.

Tabela 20: Načini zaščite proxy strežnikov

Način zaščite	Frekvenca
Protivirusni program realnočasovno preverja ves promet	149
Blokiranje, filtriranje, čiščenje okuženih datotek	130
Druge metode protivirusne zaščite	11
Anketiranih podjetij	209

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Slika 20: Načini zaščite proxy strežnikov

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

Tabela 21 in slika 21 prikazujeta stopnjo zaščite požarnih zidov podjetjih. Požarni zid je vrsta sistemske rešitve, ki podrobno nadzira vse povezave/promet med lokalnim in globalnim omrežjem ter ustavi vsak prenos, ki ni v skladu z varnostnimi pravili[15]. Podatke o protivirusni zaščiti požarnih zidov je posredovalo 176 podjetij.

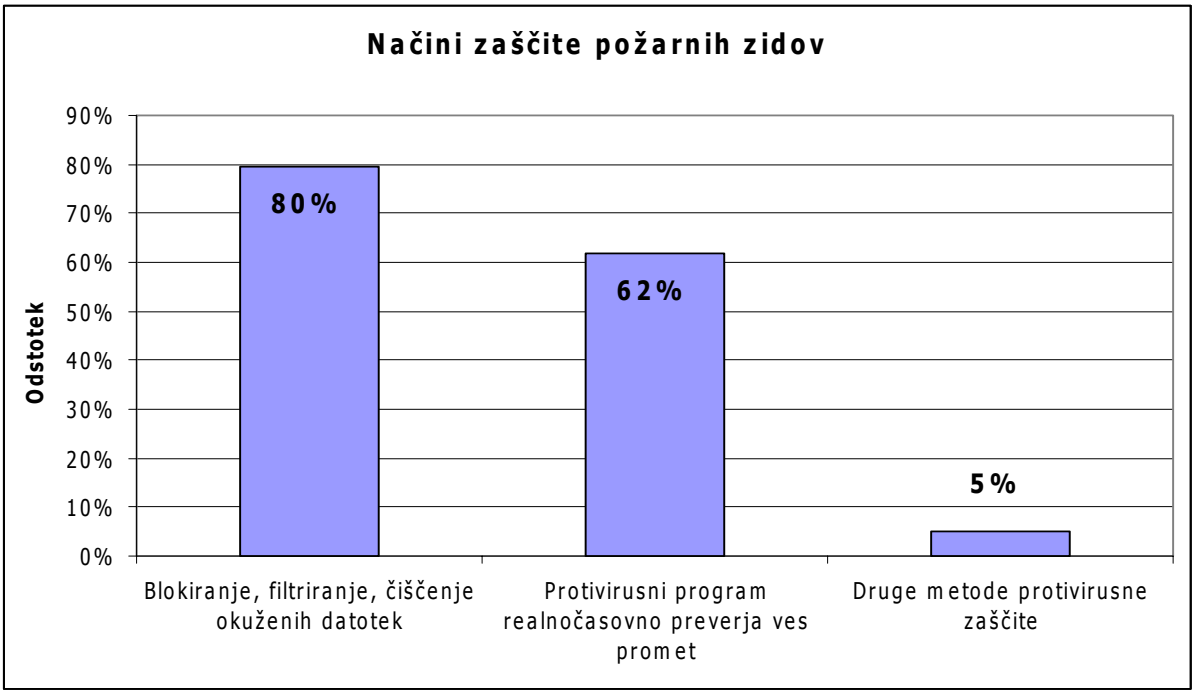
Tabela 21: Načini zaščite požarnih zidov

Način zaščite	Frekvenca
Blokiranje, filtriranje, čiščenje okuženih datotek	140
Protivirusni program realnočasovno preverja ves promet	109
Druge metode protivirusne zaščite	9
Anketiranih podjetij	176

Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

[15] Firewalls: a technical overview, 2004.

Slika 21: Načini zaščite požarnih zidov



Vir: ICSA Labs Computer Virus Prevalence Survey 2003, 2004.

3.7 KOMENTAR RAZISKAVE

Rezultati raziskave kažejo, da se virusni problemi poglabljajo, problematika računalniških virusov in črvov je vse bolj pereča. Večina obravnavanih podjetij (88 odstotkov) je namreč leto 2003 označila za najbolj kritično doslej, in to potem, ko so že prejšnja leta – od 2000 naprej – veljala za slaba.

Virusne okužbe, virusne katastrofe ter stroški odprave posledic virusnih napadov naraščajo iz leta v leto, čeprav se je rast zmanjšala na vsega nekaj odstotkov letno v zadnjih treh letih. Med leti 1996 in 1999 se je število virusnih okužb podvojilo. Velik porast okužb gre pripisati izbruhu računalniškega virusa Melissa marca 1999, ki se je samodejno širil preko elektronske pošte. Po letu 1999 se je letna rast virusnih okužb ustalila na okoli 15 odstotkih. Medtem ko virusne okužbe od leta 2001 do 2003 v povprečju okužijo vsak mesec nekaj več kot desetino vseh računalnikov (v letu 2001 so zaznali v povprečju 103 okužbe, leta 2003 pa 108 okužb na 1.000 računalnikov mesečno), je veliko bolj zaskrbljujoč podatek povišano število poskusov okužb. Slednje se je namreč dramatično povečalo v zadnjih letih, v letu 2002 je bilo tako zaznanih v povprečju 1,2 milijona poskusov okužb z računalniškim virusom vsak mesec, medtem ko podatki za leto 2003 prikazujejo povprečno 2,7 milijona poskusov virusnih okužb mesečno. Izjemno povečanje gre na račun velikega števila črvov, ki se širijo s pomočjo elektronske pošte, internetnih črvov ter kopice njihovih različic. Temu trendu v bližnji prihodnosti ni videti konca, tudi mnenja varnostnih analitikov so precej črnogleda.

Povečuje se tudi število virusnih katastrof. V letu 2003 je bilo namreč s strani podjetij prijavljenih kar 92 virusnih katastrof (leta 2002 jih je bilo 80), prvič se je tudi zgodilo, da je bil vsak mesec prijavljen vsaj en primer virusne katastrofe.

Kljub dejstvu, da število klasičnih računalniških virusov upada, pa se vse bolj povečuje delež okužb z raznimi računalniškimi črvi, ki se zelo hitro širijo preko elektronske pošte ter interneta. O tem priča tudi lestvica desetih najpogostejših virusov leta 2003, kjer se na prvih devetih mestih nahajajo črvi, ki se masovno širijo preko e-pošte, deseto mesto pa zaseda internetni črv Slammer.

Novi črvi so postali vse bolj trdoživi in se »v obtoku« obdržijo dlje časa, tudi po zaslugi več deset različic posameznega črva. Največja ovira pri preprečevanju virusnih okužb pa je zmožnost izjemno hitrega širjenja škodljivih kod. Podjetja so novim nevarnostim izpostavljena že v nekaj minutah oziroma najkasneje v nekaj urah po izbruhu. Virusi so včasih veljali za nadlogo, danes pa predstavljajo resnično nevarnost. Danes imajo praktično vsa podjetja povezavo v svetovni splet, od koder izbira večina škodljivih kod, ki se lahko razširijo v kratkem času. Poglejmo si nekaj zaskrbljujočih dejstev:

- Parazitski (datotečni) virusi so potrebovali mesece ali leta za masovne okužbe.
- Makro virusi so se razširili v nekaj tednih, največ mesecih.
- E-poštni virusi potrebujejo le nekaj dni, da obidejo planet.
- Virus Code Red je potreboval 12 ur.
- Črv Klez je »osvojil« svet v pičlih dveh urah in pol.

Povečujejo se tudi stroški odprave posledic virusnih okužb, povzročena škoda je iz leta v leto večja. Računalniški virusi in črvi so iz leta v leto bolj škodljivi, saj povzročajo več dejanske škode na računalniških sistemih in v njih shranjenih podatkih. Tega se vse bolj zavedajo tudi podjetja zato nivo protivirusne zaščite raste, še vedno pa ni povsem zadovoljiv, veliko rezerv pa ostaja prav na ključnih točkah – stičiščih lokalnih omrežij z zunanjim svetom, internetom. Podjetja s protivirusnimi programi so svoje izdelke v zadnjih nekaj letih močno izpopolnila, tako da so le-ti zmožni samodejnega zaznavanja virusov, posodabljanja virusnih definicij ter omogočajo lažje upravljanje in nadzor sistemskim administratorjem.

3.7.1 Virusni trendi

Zaznani virusni trendi raziskave ICSA Labs Computer Virus Prevalence Survey so naslednji:

- Najnovejši internetni ter e-poštni črvi razvijejo več različic in imajo daljšo obstojnost, posledično je nevarnost okužb večja.
- Visoka raven mesečnih okužb z računalniškimi virusi in črvi je prisotna vse leto. Podjetja bodo morala posvetiti več časa, sredstev ter osebja za vpeljavo najvišjih varnostnih mehanizmov v boju proti računalniški nesnagi. Trendi kažejo, da v primeru okužb z računalniškimi virusi, čas in stroški potrebni za odpravo težav naraščajo.
- Računalniški virusi in črvi postajajo vse težje izsledljivi. Večina e-poštnih virusov ponareja/prikriva svoj pravi izvor in se zelo hitro razmnožuje.
- Kot kaže, so pisci računalniških virusov in pošiljatelji neželene pošte združili svoje vrste oziroma vsaj uporabljajo iste tehnike za razširjanje škodljivih kod. Tako smo priča številnim sodobnim računalniškim črvom, ki zbirajo podatke (predvsem naslove elektronske pošte) iz raznih imenikov in znajo na okuženem računalniku postaviti lastni poštni in spletni strežnik za razpošiljanje svojih škodljivih vsebin.
- Stroški odprave posledic virusnih okužb rastejo in dosegajo visoke zneske.

4. STANJE V SLOVENIJI

V Sloveniji žal trenutno ne premoremo organizacije, inštituta, podjetja ali skupine, ki bi se namensko ukvarjala s splošno problematiko računalniških virusov v gospodarstvu, tako kot to počne ameriški laboratorij ICSA Labs. Zato sem se pri izdelavi diplomskega dela obrnil na podjetja, ki v Sloveniji distribuirajo protivirusne programe ter skrbijo za njihovo tehnično podporo in implementacijo. Izkazalo se je, da imajo le-ta še največ znanja in podatkov o stanju v domačem gospodarstvu – vsaj kar zadeva varnostno politiko, računalniške viruse ter protivirusno programsko opremo. Podatke o problematiki računalniških virusov v Sloveniji so tako prispevala naslednja podjetja, navedena v abecednem vrstnem redu: Alterna intertrade, d. d. (Network Associates – McAfee programska oprema), CHS, d. o. o. (izdelki Symantec), Parametica, d. o. o. (BitDefender ter eScan) ter Ribera, d. o. o. (Panda Software). Podatki v oklepajih označujejo, katere tuje protivirusne hiše zastopa posamezno podjetje.

Menim, da sodelujoča podjetja s svojimi proizvodi in storitvami pokrivajo okoli polovico trga protivirusne zaščite (programske opreme ter strojne opreme) v Sloveniji. Skupno število aktivnih licenc vseh obravnavanih protivirusnih programov presega več sto tisoč primerkov[16].

Slovenija pri napadih računalniških virusov ni nobena izjema in tudi v malo podalpsko deželo škodljive kode zelo hitro najdejo pot. Po podatkih domačih protivirusnih podjetij se ob večjih virusnih izbruhih prvi alarmi v Sloveniji začnejo pojavljati še isto uro kot drugod po Evropi.

Tudi Center Vlade RS za informatiko ima izdelane osnovne smernice in priporočila, kako poskrbeti za varnost informacij v podjetjih. Bolj kot na protivirusno zaščito – programsko in strojno – se v svojem dokumentu z naslovom »Priporočila za pripravo informacijske varnostne politike« osredotočajo na nadzor in kontrolo zaposlenih ter njihovega dela (Hajtnik, 2002).

Domači ponudniki protivirusne zaščite nudijo svoje rešitve podjetjem in domačim uporabnikom. Pri vseh ponudnikih je med aktivnimi licencami delež podjetij vsaj 70-odstoten ali višji, pri svoji analizi in izračunih sem tako upošteval samo podatke, ki se nanašajo na uporabo protivirusne zaščite v podjetjih. Komentar stanja protivirusne zaščite pri domačih uporabnikih bo podan na koncu tega poglavja.

4.1 SPLOŠEN OPIS STANJA PO PODJETJIH

Domača protivirusna podjetja so si enotna, da je stanje protivirusne zaščite po slovenskih podjetjih relativno dobro. Podjetja se namreč zavedajo nevarnosti in potencialnih škod, ki jih povzročajo računalniški virusi, veliko podjetij ima tudi slabe izkušnje z virusi iz preteklosti. Vsa podjetja se strinjajo, da je problematika računalniških virusov v zadnjih letih vse bolj pereča, poskusov okužb je iz leta v leto več.

Seveda je prostora za izboljšave še veliko, največje omejitve domačim podjetjem predstavljajo relativno ozko omejeni proračuni IT oddelkov glede na ostale oddelke v podjetjih. Zato je stopnja zaščite večkrat tudi kompromis med številom varnostnih mehanizmov ter vloženimi sredstvi. Vsa podjetja se sicer strinjajo, da je digitalna varnost eden ključnih elementov sodobnega poslovanja.

[16] Vir: Lastni izračuni. Zaradi nestrinjanja sodelujočih podjetij konkretnih podatkov ni moč objaviti.

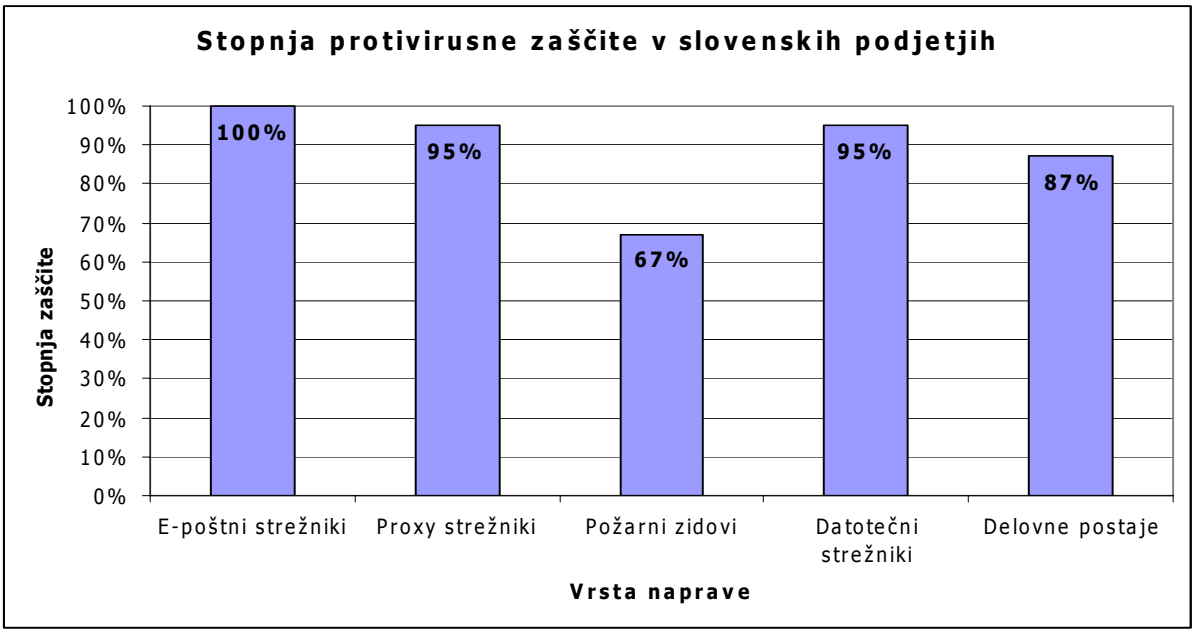
4.2 STOPNJA ZAŠČITE S PROTIVIRUSNIMI PROGRAMI

Protivirusni programi so najpogostejša oblika zaščite računalniških sistemov v slovenskih podjetjih. Tako ima večina domačih podjetij na veliko delovnih postajah nameščen protivirusni program[17] (podatki o tovrstni zaščiti se gibajo med 75 in 100 odstotki, tehtano povprečje znaša 87 odstotkov, pri datotečnih strežnikih in strežnikih za elektronsko pošto pa je stopnja zaščite še višja, protivirusna podjetja namreč poročajo o kar 95- oziroma 100-odstotni stopnji zaščite. Po prejetih podatkih imajo torej vsa domača podjetja na strežnikih za elektronsko pošto nameščen protivirusni program. Razlaga slednjega podatka je preprosta – manjša in nekaj srednje velikih podjetij namreč nima lastnih strežnikov za elektronsko pošto (imajo pa več elektronskih poštnih predalov pri svojem ponudniku internet dostopa), večja podjetja pa imajo vse svoje poštne strežnike zelo dobro zaščitene, saj se preko elektronske pošte danes prenaša vse več škodljivih kod. Ta trend potrjujejo tudi podatki domačih ponudnikov dostopa do interneta, več o tem v nadaljevanju.

Tudi zaščita požarnih zidov in proxy strežnikov je po podatkih domačih protivirusnih ponudnikov v Sloveniji malce nad ravnjo, izkazano v ameriški raziskavi laboratorija ICSA Labs. Tako je s protivirusnimi programi opremljenih dobri dve tretjini požarnih zidov, medtem ko je zaščita proxy strežnikov na ravni datotečnih strežnikov in strežnikov za elektronsko pošto, saj je kar 95-odstotna. Tudi tu je razlaga visoke stopnje zaščite enaka kot v primeru zaščite strežnikov za elektronsko pošto.

Na sliki 22 je prikazano tudi splošno stanje protivirusnih rešitev (predvsem protivirusnih programov) v slovenskih podjetjih. Podatki veljajo za prvo polovico leta 2004.

Slika 22: Povprečna stopnja protivirusne zaščite v slovenskih podjetjih



Vir: Lastni izračuni. Podatki veljajo za prvo polovico leta 2004.

[17] Vir: Lastni izračuni. Podatki veljajo za prvo polovico leta 2004.

4.3 POSLEDICE VIRUSNIH NAPADOV

Domača protivirusna podjetja sem povprašal tudi o najbolj pogostih posledicah, ki so jih njihove poslovne stranke sporočile ob virusnih napadih. V tabeli 22 se nahaja deset najbolj pogostih odgovorov, ki so jih posredovala slovenska podjetja.

Tabela 22: Deset najpogostejših posledic virusnih napadov

Mesto	Posledica virusnega napada
1.	Izguba produktivnosti
2.	Poškodovane datoteke
3.	Izguba podatkov
4.	Zmanjšanje zaupanja zaposlenih
5.	Motnje, zamrzovanje računalnika
6.	Izguba podatkov
7.	Sesutje sistema
8.	Nezanesljivost delovanja aplikacij
9.	Težave pri tiskanju
10.	Težave s pisanjem datotek

Vir: Interni podatki slovenskih protivirusnih podjetij, 2004.

Kot je razvidno iz tabele 22, se slovenska podjetja ob virusnih napadih soočajo s podobnimi težavami kot ameriška (podatki iz tabele 12). Na obeh lestvicah najpogostejših posledic napadov računalniških virusov najdemo navedeno izgubo produktivnosti, kar je seveda logično, saj virusni napad vsaj za določen časovni interval (krajši ali daljši) ohromi ali celo ustavi poslovanje podjetja. Zaposleni v Sloveniji se tako kot njihovi ameriški kolegi pogosto srečujejo tudi s poškodovanimi datotekami, večkrat podatke v datotekah tudi izgubijo. Nemalokrat je posledica napada računalniškega virusa tudi nezanesljivo delovanje sistema, ki v nekaterih primerih vodi tudi v samo sesutje in ponovni zagon. Vse to pa zahteva dragocen čas, tako obnavljanje sistema kot tudi neproduktivnost zaposlenih ob nedelujočem informacijskem sistemu. Presenetljivo visoko na domači lestvici posledic virusnih napadov je tudi odgovor o zmanjšanju zaupanja zaposlenih. Slednji pogosto izražajo strah pred računalniškimi virusi in nezaupanje v informacijski sistem podjetja – le-ta naj bi bil po njihovem mnenju preveč ranljiv.

4.4 IZVOR RAČUNALNIKIH VIRUSOV

Tudi v slovenskih podjetjih se kažejo enaki trendi kot v ameriških. Med izvori okužb z računalniškimi virusi tako daleč premočno vodi elektronska pošta pred spletno dolvleko datotek, medtem ko se virusi, ki se širijo z različnimi mediji, pojavljajo dokaj redko.

Kljub dejstvu, da podjetja najbolj pazijo prav na računalniške viruse, ki se širijo z elektronsko pošto, so le-ti v slovenskem prostoru najbolj pogosti. Neredko domače sistemske administratorje presenetijo tudi trdoživi omrežni črvi, ki v svojih več različicah napadajo omrežja tudi po mesec dni.

Svoj delež k statistiki dodajo še zaposleni, ki so v veliki večini primerov tudi krivci za okužbe z računalniškim virusom. Zaposleni, ki imajo neoviran dostop do interneta, prej ali slej zaidejo tudi na strani s sumljivo vsebino (najpogosteje so to pornografske strani in strani z

nelegalno programsko vsebino) in s spleta pretočijo z virusi, črvi ali trojanskimi konji okužene datoteke. Pogosto se v slovenskih podjetjih tudi zgodi, da se okuži računalnik, ki sicer ima nameščen protivirusni program. Razlog te okužbe je v največ primerih neposodabljanje virusnih definicij, kar je posledica izključitve s strani uporabnika (največkrat po pomoti). Glede na dejstvo, da večina sodobnih protivirusnih programov premore funkcijo samodejnega posodabljanja, bodo omenjene napake vse redkejše. K redkosti teh napak bo pripomogla tudi izboljšana administracija protivirusnih programov v velikih podjetjih, h kateri stremijo vsi proizvajalci varnostne programske opreme in napredek je že opazen.

4.5 POSLOVNA ŠKODA ZARADI VIRUSOV

Slovenska podjetja se zavedajo, da jim okužbe z računalniškimi virusi povzročajo precej poslovne škode. Žal uradnih statistik, ki bi merile višino povzročene škode kot posledice virusnih napadov, v podjetjih ne vodijo, prav tako mi s temi podatki niso mogla postreči niti domača protivirusna podjetja.

Najbolj pogosti odgovori o povzročeni poslovni škodi, ki je nastala zaradi virusnega napada, so se nanašali na padec produktivnosti v podjetju. Virus, ki uspe ohromiti informacijski sistem podjetja, povzroči veliko izgubo delovnega časa zaposlenih, ki so tako čakali, da informatiki v podjetju težavo odpravijo. Tudi delo slednjih je pogosto edino ovrednoteno kot merilo povzročene škode, čeprav še zdaleč ni tako. Neposrednih in posrednih stroškov je še veliko več.

4.6 ZAŠČITA PRED RAČUNALNIŠKIMI VIRUSI V PODJETJIH

Znotraj podjetja so računalniki ponavadi povezani v lokalno omrežje. Lokalno omrežje pa je na eni ali več straneh povezano še z drugimi omrežji ali internetom. Prav na teh stičnih točkah pa je ključnega pomena dobra zaščita. Najlažje je namreč računalniške viruse zaustaviti na vhodu v podjetje. Načini in zahtevnost varovanja pa se razlikujejo tudi od velikosti podjetja, njegovega omrežja ter tipologije in nivojev.

Za varovanje informacijskega premoženja so ključni naslednji postopki, ki morajo biti izpolnjeni za optimalni nivo zaščite informacij v podjetju (Varovanje informacijskega premoženja, 2004):

- Z varnostno politiko se določijo pravila in postopki varovanja in zaščite informacijskega premoženja.

- Z varnostno analizo se identificira celotno informacijsko premoženje podjetja in njihove lastnike, sočasno se preveri učinkovitost varnostnih in zaščitnih ukrepov določenih z varnostno politiko.

- Z oceno tveganja se določa še sprejemljivo poslovno tveganje. Določa se tveganje glede na ranljivost informacijskega premoženja in glede na grožnje, ki jim je to premoženje izpostavljeno. Identificira se tisto informacijsko premoženje, katerega uničenje, odtujitev ali sprememba lahko povzroči poslovno škodo večjo od še sprejemljive.

Slika 23: Model varovanja informacijskega premoženja

Vir: Varovanje informacijskega premoženja, 2004.

Informacijsko premoženje organizacije (Smart-Com, 2004) ali ustanove predstavljajo vsi podatki in vse informacije ter vse naprave in vsi prenosni sistemi, ki omogočajo izdelavo, prenos, obdelavo in hranjenje podatkov in informacij. Prav tako informacijsko premoženje vključuje vse lastninske in poslovne informacije, intelektualno lastnino (patenti, know-how, blagovna znamka ...), sredstva in objekte v lasti podjetja ter informacijsko premoženje tretjih oseb, do katerih ima podjetje dostop ter vsi podatki in informacije, katerih nepooblaščeno uničenje, spreminjanje ali razkritje izven podjetja lahko povzroči podjetju posredno ali neposredno škodo:

- napad na integriteto ali zaupanje v podjetje,
- finančno izgubo,
- poslovno škodo,
- izgubo položaja,
- zmanjšanje poslovanja,
- prekinitev pogodbe s tretjo osebo ali
- neprilagajanje zakonskim zahtevam.

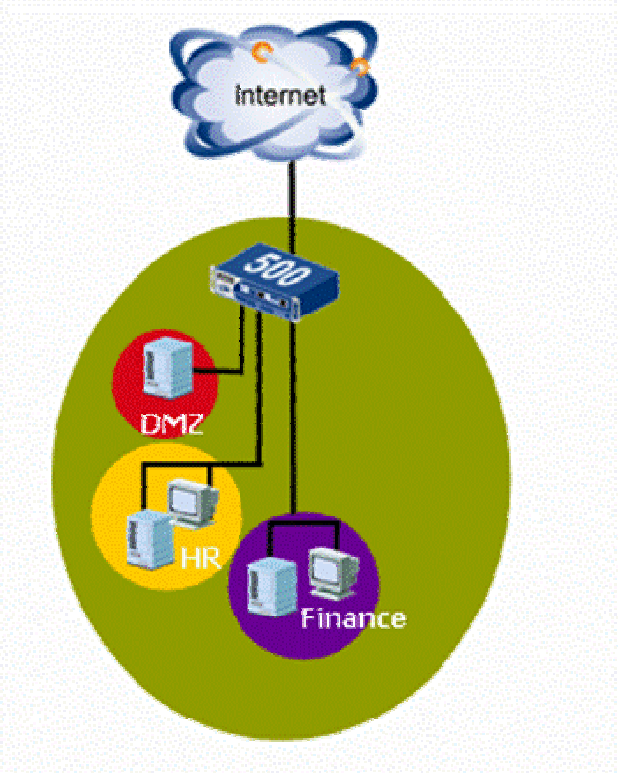
Varovati informacijsko premoženje pomeni zagotoviti zaupnost, celovitost in razpoložljivost informacij in podatkov. Varovanje lahko vključuje celotno informacijsko premoženje organizacije oz. ustanove ali samo en njen del. Varovanje in zaščita informacijskega premoženja je sistem in ne produkt, ker se stalno spreminja, dopolnjuje in nadgrajuje.

4.6.1 Varovanje malih omrežij

Mala podjetja so zelo odvisna od omrežja, saj je to ključno orodje za podporo izvajanju hitrega in učinkovitega poslovanja. Hkrati se povečujejo grožnje, ki bi lahko resno vplivale na zmanjšanje prihodkov in ugleda podjetja ter na zaupanje njihovih strank. Varno omrežno infrastrukturo je potrebno zasnovati na podlagi formalne varnostne politike. Načrtovanje varnega omrežja temelji na ugotavljanju pričakovanih groženj in metodah, ki bi le-te preprečile.

V mala omrežja lahko uvrstimo podjetja, ki imajo omrežje skoncentrirano na eni lokaciji in podjetja z do nekaj deset računalniki. Osnovne značilnosti zaščite takega omrežja se začno pri postavitvi požarnega zidu, s katerim omrežje zaščitimo pred zunanjimi vdori. Hkrati moramo zagotoviti segmentacijo omrežja, da ločimo strežnike z varnostno občutljivimi podatki od ostalih računalnikov. Priporočljivo je, da je brezžično omrežje, v kolikor je prisotno, povsem ločen segment. S pomočjo varnostne politike, ki jo nastavimo na požarni pregradi, dovolimo dostop do informacij samo upravičenim uporabnikom. Dodaten nadzor izvajamo s sistemom za odkrivanje in preprečevanje vdorov. Hkrati je pomembna protivirusna zaščita in zaščita pred neželeno pošto. Prav tako je možno filtriranje vsebin.

Slika 24: Primer zaščite malega omrežja

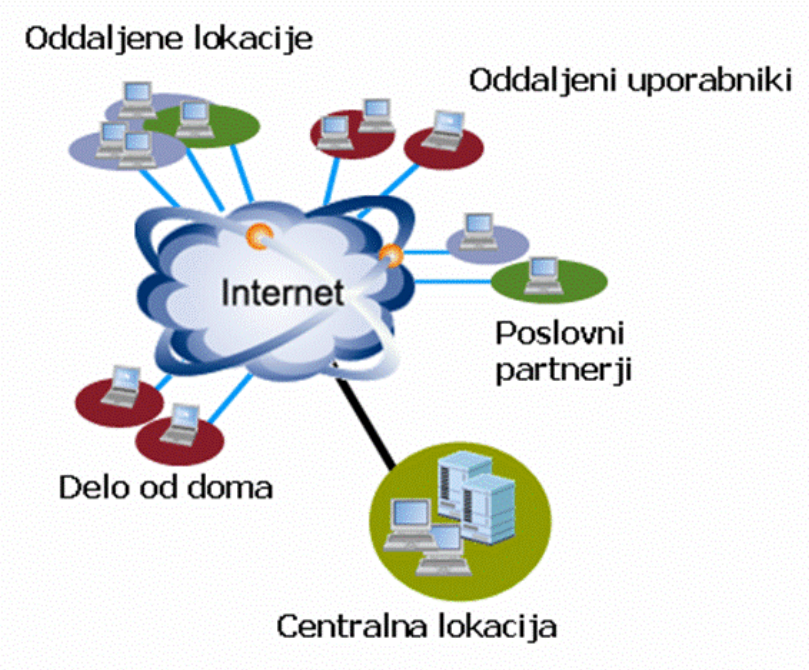


Vir: Varovanje informacijskega premoženja, 2004.

4.6.2 Varovanje velikih omrežij

V velika omrežja lahko uvrstimo podjetja, ki imajo poleg centralne lokacije več oddaljenih enot (poslovalnic). Podjetja morajo zagotoviti varno izmenjavo informacij med enotami. Temu je namenjen sistem razpršenega intraneta z uporabo varnih povezav. Hkrati podjetja ne smejo pozabiti na grožnje, ki prihajajo iz notranjosti omrežja. S požarnimi zidovi ter sistemi za odkrivanje in preprečevanje vdorov, ki so glavni gradniki sistema lokalni intranet, je omogočena večnivojska zaščita. VPN[18] naprave nudijo vzpostavitev varnih medsebojnih povezav, ki so lahko statične ali dinamične. Pri velikem številu lokacij je priporočljiva uporaba sistema za upravljanje in nadzor VPN omrežja. Zaradi nemotenega poslovanja je potrebno na osrednji lokaciji poskrbeti za podvojene naprave, ki v primeru izpada prevzamejo delo. Povezava v internet je prav tako ključnega pomena, zato mora biti podvojena. Poleg tega lahko zaposlenim zagotovimo tudi varen oddaljen dostop do lokalnega omrežja, ki ga omogoča sistem oddaljenega dostopa do intraneta.

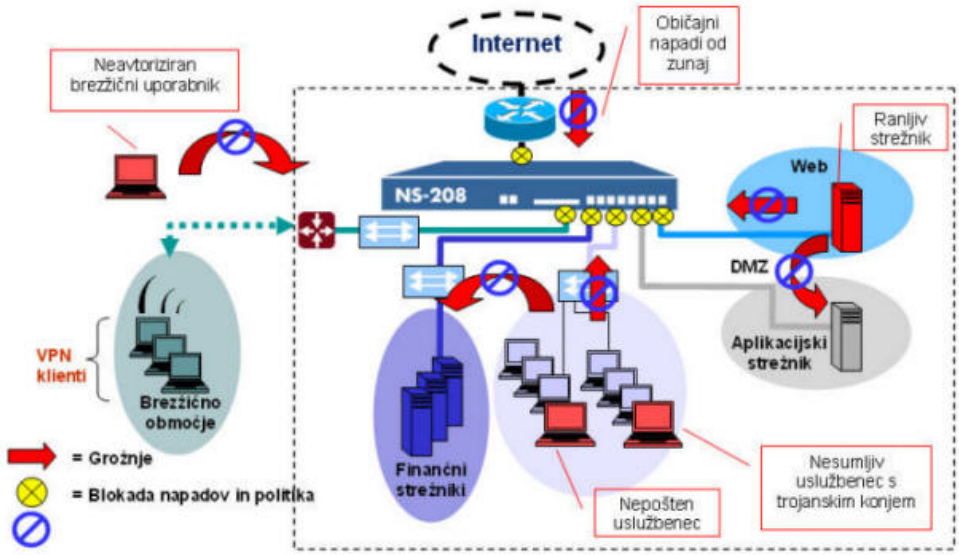
Slika 25: Primer zaščite velikega omrežja



Vir: Varovanje informacijskega premoženja, 2004.

[18] Kratica VPN pomeni Virtual Private Network, oziroma navidezno zasebno omrežje. Navidezna zasebna omrežja so temelj za varno komunikacijo med posameznimi lokacijami, nadgradljiva z velikim številom IP tehnologij, s katerimi podjetje na več lokacijah postane celovita enota.

Slika 26: Primer zaščite lokalnega omrežja



Vir: Varovanje informacijskega premoženja, 2004.

4.6.3 Implementacija varnostnih rešitev v slovenskih podjetjih

Sama implementacija varnostnih rešitev med slovenskimi podjetji se zelo razlikuje. Tista večja, uspešnejša, ki se tudi v celoti zavedajo nevarnosti in škod, ki jih lahko povzroči računalniški virus, so zelo dobro zaščitena. Taka podjetja svojim IT oddelkom, kamor pri večini tudi sodi skrb za digitalne varnostne rešitve, po podatkih slovenskih protivirusnih podjetij namenjajo od 7 do 10 odstotkov letnega proračuna. Pri tem je za varovanje informacijskega sistema v podjetju vrhunsko poskrbljeno – varovane so vse vstopne točke ter tudi posamezne delovne postaje in strežniki v podjetju. Dostop do posameznih nivojev v podjetju je omejen, prav tako podjetje izobražuje svoje zaposlene, poleg tega pa sistemski administratorji za vsak nivo uporabnikov določijo pravice, tako da zaposleni na svojih računalnikih ne morejo početi ravno vsega, kar se jim zljubi.

V večini domačih podjetij pa je slika informacijske varnosti vendarle drugačna, slabša, neredko tudi na meji delujočega. IT oddelki v takih podjetjih so zelo omejeni z letnimi proračuni in skrb za digitalno varnost zanje predstavlja kompromis. Tako vsako leto zakrpajo le nekaj lukenj ter posodobijo del strojne in programske opreme. Težava v teh podjetjih je v glavah nadrejenih, ki si informatiko predstavljajo kot skupek računalnikov in programov. Manj ali skoraj nič poudarka ne dajejo izobraževanju zaposlenih, tudi izdelana varnostna politika je prej izjema kot pravilo. Takšna podjetja utrpijo tudi največjo škodo ob virusnih napadih, saj nanje niso niti ustrezno pripravljena, zato se tudi slabo odzovejo. Medtem ko večina takih podjetij ščiti svoje vstopne točke, pa jim neredko zmanjka sredstev za zaščito lokalnega omrežja in delovnih postaj. Ker pa digitalna nevarnost danes preži na prav vsakem koraku, za pogoste okužbe poskrbijo kar zaposleni sami z odpiranjem neznanih datotek itd. Pri varnosti pač kompromisi ne smejo priti v poštev.

5. KAKO V PRIHODNJE?

Strokovnjaki na področju računalniških virusov in varnostni analitiki svarijo, da se virusna nevarnost ne bo kmalu polegla, še več, stanje naj bi postajalo čedalje slabše. Pisci virusov imajo po novem poleg standardnih motivov (dokazovanje znanja, koristoljubje …) še nov, politični motiv. Računalniški črvi postajajo vse bolj prikriti in vse bolj spretni – nekateri znajo celo onemogočiti protivirusne programe! Leto 2004 tako nadaljuje grozeče trende iz preteklosti oziroma jih še poglablja. Internetni črvi pustošijo praktično na tedenski osnovi, strežniki za elektronsko pošto se šibijo pod bremeni neželene elektronske pošte (ang. spam) in virusov.

Microsoft, največji svetovni proizvajalec operacijskih sistemov, ima med vsemi osebnimi računalniki na svetu kar 93,8-odstotni tržni delež pri operacijskih sistemih[19]. Obenem pa je grozljivo dejstvo, da nobena izmed njegovih platform ni virusno varna brez ustreznih dodatkov in popravkov (Thurrtott, 2004). To velja tudi za operacijske sisteme za dlančnike in druge mobilne naprave, katerih visoko prodajo gre pričakovati v prihodnjih letih. Pa ne le Microsoft, tudi drugi proizvajalci operacijskih sistemov za mobilne naprave, npr. Symbian, se soočajo z enakimi težavami – virusi.

5.1 ZAŠČITA NA STROJNEM NIVOJU

Več kot očitno je, da je »mečevanje« na nivoju programske opreme početje, ki se lahko vleče v neskončnost. Pisci virusov na eni strani in protivirusna podjetja na drugi praktično tekmujejo drug z drugim po hitrosti in odzivnosti – to je boj med dobrimi iz zlimi silami. Nekateri napadi "zlobne" programske opreme so rezultat ranljivosti programov in operacijskih sistemov, ki dovoljujejo pretok prevelike količine podatkov na določena mesta fizičnega pomnilnika. Rezultat je tako imenovana prekoračitev pomnilnika (ang. buffer overrun) in vrivanje škodljive kode vanj. Prav tak način so izbrali računalniški črvi Sasser, MSBlast ter Welchia. Pravzaprav nobena tehnologija ne more preprečiti takšnega početja, toda Microsoft se z obilico posameznih tehnologij trudi problem omiliti, in sicer na več načinov. Prvi je prenova oz. vnovično prevajanje komponent, ki imajo neposredni vpliv na jedro samega operacijskega sistema, drugi pa prizadevanje Microsofta[20], da bi s pomočjo izdelovalcev mikroprocesorjev uveljavil novo tehnologijo NX (no-execute – NX). Ta bo strojno preprečila takšno početje, kar bo znatno ublažilo posledice.

Praktično vsi proizvajalci procesorjev so se hitro in pozitivno odzvali. Tako bo NX strojni nivo zaščite vgrajen v bodoče mikroprocesorje proizvajalcev AMD, IBM, Intel, Transmeta, VIA in drugih, nekateri procesorji pa že sedaj premorejo omenjeno zaščito (primer: AMD Athlon 64 ter Opteron, Intel Itanium ter Itanium 2). Ukaz NX uporabi sam mikroprocesor, s katerim vsili ločitev programske kode in podatkov. Tako prepreči, da aplikacija oziroma komponenta operacijskega sistema izvrši programsko kodo, ki jo računalniški črv ali virus preneseta na področje pomnilnika, namenjeno zgolj podatkom. Zaščita je aktivna na dveh nivojih – v samem jedru ter na uporabniškem nivoju. To tudi posledično prisili razvijalce

[19] Po podatkih raziskave Worldwide Client and Server Operating Environment Market Forecast and Analysis, 2002–2007. [URL: http://www.winnetmag.com/Article/ArticleID/40481/40481.html], 11. 7. 2004

[20] Zaščita pred izvajanjem škodljivih kod (ang. Execution protection).
[URL: http://msdn.microsoft.com/security/productinfo/XPSP2/memoryprotection/execprotection.aspx], 28. 8. 2004

programske opreme, da se izogibajo izvrševanja programske kode izven podatkovnih strani, brez da bi le-te prej označili kot izvršilne. Tako podpirajo tudi dobro pisanje programskih osnov za vse razvijalce programske opreme in gonilnikov.

Zaščita NX, ki jo bodo vsebovali praktično vsi bodoči procesorji, pa ni omejena zgolj na Microsoftove operacijske sisteme. Tudi na Linux jedru temelječi operacijski sistemi, ki v zadnjih letih vse bolj rinejo v ospredje, že omogočajo takšno sožitje strojne in programske opreme.

5.2 IZBOLJŠAVE PROGRAMSKE OPREME

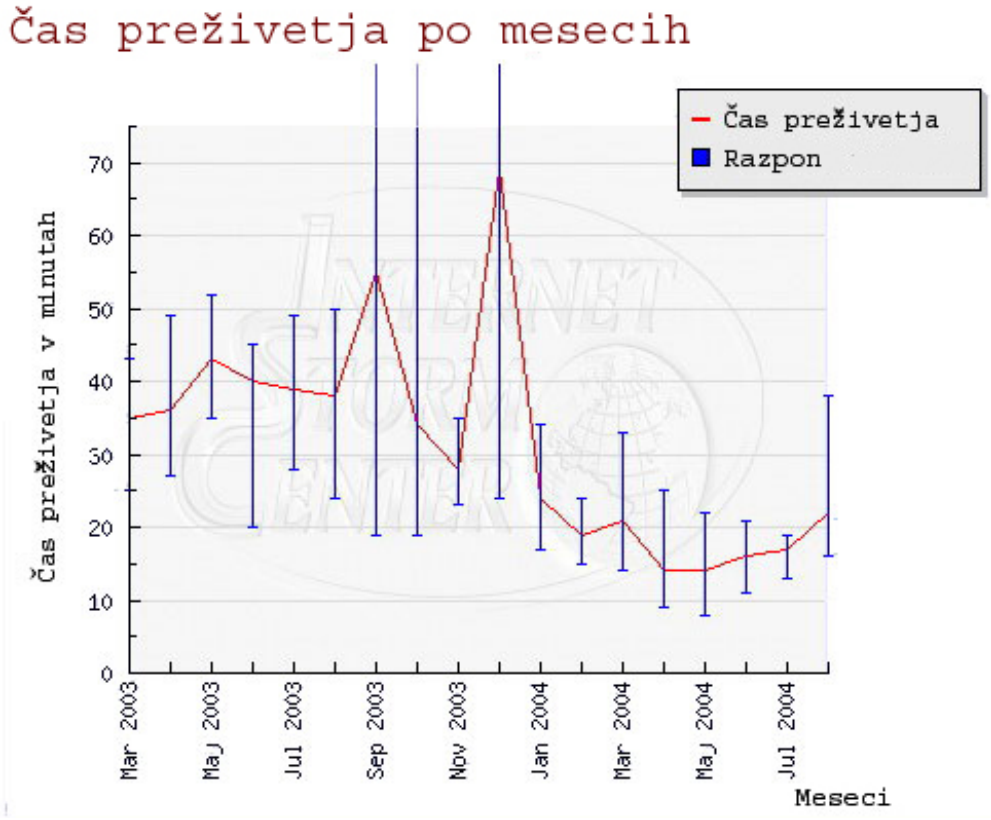
Računalniški črvi vse pogosteje izkoriščajo ranljivosti operacijskih sistemov, ki niso pravilno »zakrpane«. Proizvajalci programske opreme se zato trudijo in pripravljajo razne popravke, ki varnostne luknje zakrpajo, težava pa nastane v distribuciji do končnih uporabnikov. Microsoft za svoje operacijske sisteme, torej Okna, nudi kopico posodobitev na svojem spletnem portalu Windows Update, le namestiti jih je potrebno. Tega opravila se sicer dobro zavedajo sistemski administratorji, tako da je večina podjetij ustrezno zaščitenih, vse premajhna pa je zavednost med končnimi uporabniki, katerih računalniki so vse pogosteje gnezda vseh mogočih »digitalnih škodljivcev«. Je pa sistem posodabljanja in vzdrževanja sedaj enostavnejši in omogoča tudi večjo avtomatizacijo samega posodabljanja.

Varnost operacijskih sistemov vedno bolj pridobiva na pomenu, Microsoft, kot vodilni ponudnik tovrstne programske opreme na svetu, pa v svoje izdelke vpeljuje čedalje več varnostnih elementov. Med izboljšavami, ki jih je deležen operacijski sistem Microsoft Windows XP s paketom popravkov Service pack 2, najdemo nov in izboljšan programski požarni zid, omogočena je strojna zaščita NX na strojnih platformah, ki to omogočajo … Izdatno so izboljšani varnostni mehanizmi vgrajenega spletnega brskalnika Internet Explorer in odjemalca elektronske pošte Outlook Express, ki sta bila do sedaj glavna krivca za številne okužbe z računalniškimi virusi in črvi. V bodočih različicah bo Microsoft omenjena programa tudi ločil od ostalega sistema, kar naj bi preprečilo izbruh virusa na celotnem sistemu. Nič manj nedolžen ni komunikacijski program Windows Messenger, ki ga bo doletela podobna usoda. Dodan je tudi osrednji skrbnik za varnost celotnega sistema, ki sliši na ime Security Center. Ta ustvari centralno lokacijo za informacije o dejanskem stanju računalnika; predvsem o nameščenih varnostnih popravkih in programski opremi, kar pomeni večji nadzor in varnost pri namestitvah programske opreme. Omenjene varnostne novosti bodo vgrajene tudi v vseh prihajajočih Microsoftovih operacijskih sistemih.

Zanimiv je podatek o ranljivosti programske opreme. Rezultati raziskovalnega inštituta SANS[21] so pokazali, da sveže naložen sistem Microsoft Windows na spletu lahko preživi borih 20 minut, preden se okuži s kakšnim izmed črvov ali drugim pesticidom. Še leta 2003 so rezultati enake raziskave, izvedene s strani istega inštituta, ocenjevale nezaščiteno »preživetje« na 40 minut, kar jasno kaže, kako močno se je v enem letu povečala grožnja pesticidov, ki izkoriščajo sistemske luknje. Tako močan padec tega časa pa je sicer zelo zaskrbljujoč, saj uporabnikom niti ne dovoli, da na novo naložen okenski sistem z Microsoftove strani potegnejo vse potrebne popravke, ki bi jih lahko pred tovrstnimi okužbami zaščitili, kaj šele, da si namestijo kvalitetno protivirusno zaščito in požarni zid (Granneman, 2004).

[21] Inštitut SANS (SysAdmin, Audit, Network, Security) je bil ustanovljen leta 1989 kot organizacija za raziskovanje varnosti informacijskih sistemov. Danes pod njegovim okriljem rešitve na varnostne težave sodobnega digitalnega sveta prispeva kar 165.000 različnih strokovnjakov.

Slika 27: Čas preživetja operacijskega sistema Microsoft Windows



Vir: SANS Institute Internet Storm Center: Survival Time History, 2004.

Kot je razvidno iz slike 27, ugotovitve raziskovalnega inštituta SANS sovpadajo z rezultati letne študije laboratorijev ICSA Labs. Medtem ko so pri ICSA Labs ugotovili, da se je število virusnih okužb močno povečalo v mesecu novembru leta 2003, se je slednje jasno odrazilo tudi na sposobnosti preživetja nezaščitenega operacijskega sistema Microsoft Windows »v divjini«. Večje število škodljivih kod v omenjenem obdobju je pomenilo, da navedeni operacijski sistem brez zaščite preživi na spletu manj kot 30 minut, preden se okuži. Da je leto 2004 še bolj neprizanesljivo z digitalno nesnago, priča vsega 15 minut avtonomije Microsoftovih Oken brez škodljivca v aprilu letos. Edini letošnji oddih so si avtorji zlonamernih programskih kot privoščili le v novoletnem obdobju.

Za varnost operacijskih sistemov pa ne skrbi le njihov proizvajalec. Kot gobe po dežju so se v zadnjem desetletju pojavila številna specializirana podjetja, ki se ukvarjajo z varnostno problematiko in rešitvami. Konkurenca na trgu protivirusnih programov je danes tako ostra, da povprečnih izdelkov praktično ni več najti, vsi se trudijo kar najbolj zaščititi svoje uporabnike. Obenem je programska oprema postala vse bolj enostavna za uporabo in namestitev ter tudi vzdrževanje, kar je v boju proti virusnim nevarnostim velik plus. Vsi izdelovalci protivirusne programske opreme imajo tudi svoje laboratorije za analizo škodljivih kod in objavljajo ustrezne popravke ter pripomočke za odstranitev virusov v primeru okužbe. Večina ponudnikov tovrstnih storitev svoje uporabnike redno obvešča o aktualnih nevarnostih, na katere naj bodo še posebej pozorni.

Ponudba protivirusne programske opreme je danes resnično pestra in za ceno dveh do petih odstotkov cene povprečnega osebnega računalnika si lahko uporabniki kupijo protivirusni program, ki bo njihov računalnik pred nevarnostmi ščitil celo leto. Seveda so cene licenc tovrstne programske opreme za podjetja z veliko računalniki še bistveno nižje. Protivirusni programi pa že dolgo ne ščitijo le pred računalniškimi virusi, vedno več programskih rešitev omogoča tudi varovanje pred neželeno pošto (ang. spam), blokiranje t. i. nadležnih reklamnih sporočil v obliki izskočnih oken (ang. pop-up window) ter tudi funkcije požarnega zidu. V bodoče je pričakovati tudi implementacije iskalcev vohunske programske opreme (ang. spyware), ki je vse bolj razširjena oblika računalniških nevšečnosti.

Najnovejši protivirusni programi pa se poslužujejo tudi novih tehnologij za odkrivanje še neznanih računalniških virusov. Angleški izraz za omenjeno tehnologijo oziroma pristop je »sandboxing«, ustreznega slovenskega prevoda pa v tem trenutku domači jezik še ne premore. Gre za t. i. sočasno kreiranje virtualnega računalniškega sistema, v katerem se izvajajo isti procesi kot na samem sistemu. Vsi novi procesi se najprej naložijo v vitrualni sistem, kjer protivirusni program opazuje njihovo sumljivo obnašanje. V primeru, da ti procesi ne kažejo znakov škodljivega delovanja, jim protivirusni program dovoli, da se poženejo tudi v samem sistemu. Seveda ta tehnologija zahteva večji del sistemskih sredstev kot običajni protivirusni program, a glede na povprečne računske in pomnilniške zmogljivosti sodobnih računalnikov tudi to ni prevelik zalogaj. Omenjene tehnologije predstavljajo radikalno spremembo v pristopu k učinkovitemu ravnanju z grožnjami z interneta, saj pomenijo premik od tradicionalnega koncepta reagiranja na pojav virusa na inteligenten, preventiven pristop, ki anticipira pojav novih groženj in vnaprej prepoznava potencialne težave. Primera takšnih novih tehnologij sta Norman Sandbox ter Pandin TruPrevent.

Osnovni pristopi »sandboxinga« (Murčehajič, 2004, str. 1–2) so:

- odkrivanje virusov na osnovi obnašanja,
- odkrivanje zlonamernih omrežnih paketov,
- zaščita pred prekoračitvami medpomnilnikov,
- definicija varnostnih politik.

Tudi strokovnjaki in analitiki so mnenja, da bodo podjetja z varnostnimi rešitvami na področju informacijske tehnologije v prihodnosti rasla. Tako pri IDC-ju[22] za prihodnja leta napovedujejo (Burke, 2004) večje spremembe na trgu programske opreme. Protivirusni programi bodo v bližnji prihodnosti v sebi združevali ne le pogon za hevristično iskanje virusov, temveč tudi orodja za nadzor in preprečevanje neželene elektronske pošte ter orodja za odkrivanje programske opreme za vohunjenje. Opisani večnivojski način zaščite je praktično nujen za zajezitev kuge 21. stoletja. IDC-jevi strokovnjaki v svojih napovedih predvidevajo, da naj bi trg programske opreme, namenjene računalniški varnosti v podjetjih, leta 2008 dosegel vrednost 7,5 milijarde ameriških dolarjev. Med vso varnostno programsko opremo naj bi imeli protivirusni programi do leta 2008 kar 64-odstotni tržni delež. Vsi navedeni podatki veljajo za ZDA[23].

[22] IDC velja za eno največjih ameriških analitičnih organizacij, ki preučuje predvsem globalne dejavnike v informacijski in telekomunikacijski industriji ter z njima povezane finančne tokove.
[23] Združene države Amerike.

5.3 BOLJŠA ODZIVNOST PROTIVIRUSNIH EKIP

Sam protivirusni program kot tak že dolgo ni več pravo merilo varnosti. Z izjemnim porastom števila škodljivih kod, se je poudarek na kvaliteti zaščite preselil drugam – na odzivnost protivirusnih ekip posameznih podjetij, proizvajalcev protivirusne programske opreme. Dejstvo je, da računalniške viruse lahko zaustavi ter odstrani le ustrezno posodobljen protivirusni program, ki premore aktualno protivirusno bazo, torej pozna način, kako zaznati in odstraniti posamezni virus. V zadnjih dveh letih računalniški virusi in črvi sprožajo številne okužbe na tedenski, celo dnevni osnovi. Zato je ključnega pomena, da protivirusna podjetja čimprej odkrijejo računalniški virus in pripravijo »zdravilo« zanj. Pri tem so izjemno pomembne posamezne ekipe protivirusnih strokovnjakov, ki analizirajo skupke škodljivih kod in pripravljajo ustrezne rešitve. Večji in uspešnejši proizvajalci protivirusne programske opreme premorejo večje število takih protivirusnih ekip, ki so locirane po centrih na posameznih celinah – večina ima tako svoje protivirusne ekipe strokovnjakov v centrih, ki se nahajajo v Aziji, Evropi in Severni Ameriki. Hitrost odkritja računalniškega virusa, priprava ustrezne rešitve za odpravo le-tega ter distribucija posodobitve do končnih uporabnikov je tisto, kar dejansko šteje. Podjetja, ki uspejo omenjene korake izvesti v najkrajšem času, pridobivajo nove stranke in tržne deleže.

Takšne meritve odzivnosti protivirusnih podjetij periodično opravljajo nemški neodvisni preizkuševalci protivirusne opreme, AV-test.org, ki so se leta 2003 odločili za temeljitejše preizkuse sodobnih protivirusnih programov. Priprave na prvi obsežni preizkus programske opreme za odkrivanje virusov so se tako začele že v maju leta 2003. Preizkus je za razliko od običajnih hitrostnih testov (koliko virusnih teles lahko posamezni program odkrije v določenem času) temeljil predvsem na drugi sposobnosti protivirusne zaščite – samodejnem posodabljanju. Tu so merili predvsem odzivnost posameznega programa in podjetij – kako hitro se le-ta odzovejo z ustreznimi popravki ob novih izbruhih zlobnih kod. Pri AV-test.org so merili število dnevnih in tedenskih posodobitev protivirusnih baz in orodij za odstranjevanje virusov. Za osnovo so vzeli poštnega črva Win32/Sober.C[24], ki je izbruhnil tik pred lanskimi novoletnimi prazniki, odkrit je bil 20. 12. 2003 ob 3:00. Za omenjenega črva je prvo rešitev našel program BitDefender, ekipa njegovih inženirjev je zanjo potrebovala dobrih deset ur. Drugo mesto na preizkusu so zasedli programi, temelječi na Kaspersky pogonu (takšni programi so eScan 2003, Kaspersky AV in drugi). V razmaku manj kot treh ur sta ustrezne popravke objavila še protivirusna programa F-prot (Risk) ter F-Secure. Ostali ponudniki so potrebovali bistveno daljši čas za odziv, nekateri tudi po več dni, kar je za ustrezen nivo zaščite vsekakor preveč.

[24] Članek se nahaja na naslovu: [URL: http://www.av-test.org/down/papers/2004-02_vb_outbreak.pdf], 21. 6. 2004.

Tabela 23: Odzivni čas protivirusnih podjetij ob izbruhu črva Win32/Sober.C

Table 1. Response times of AV companies (CET) to the outbreak of W32/Sober.C (worm discovered 2003-12-20 at 03:00 h).

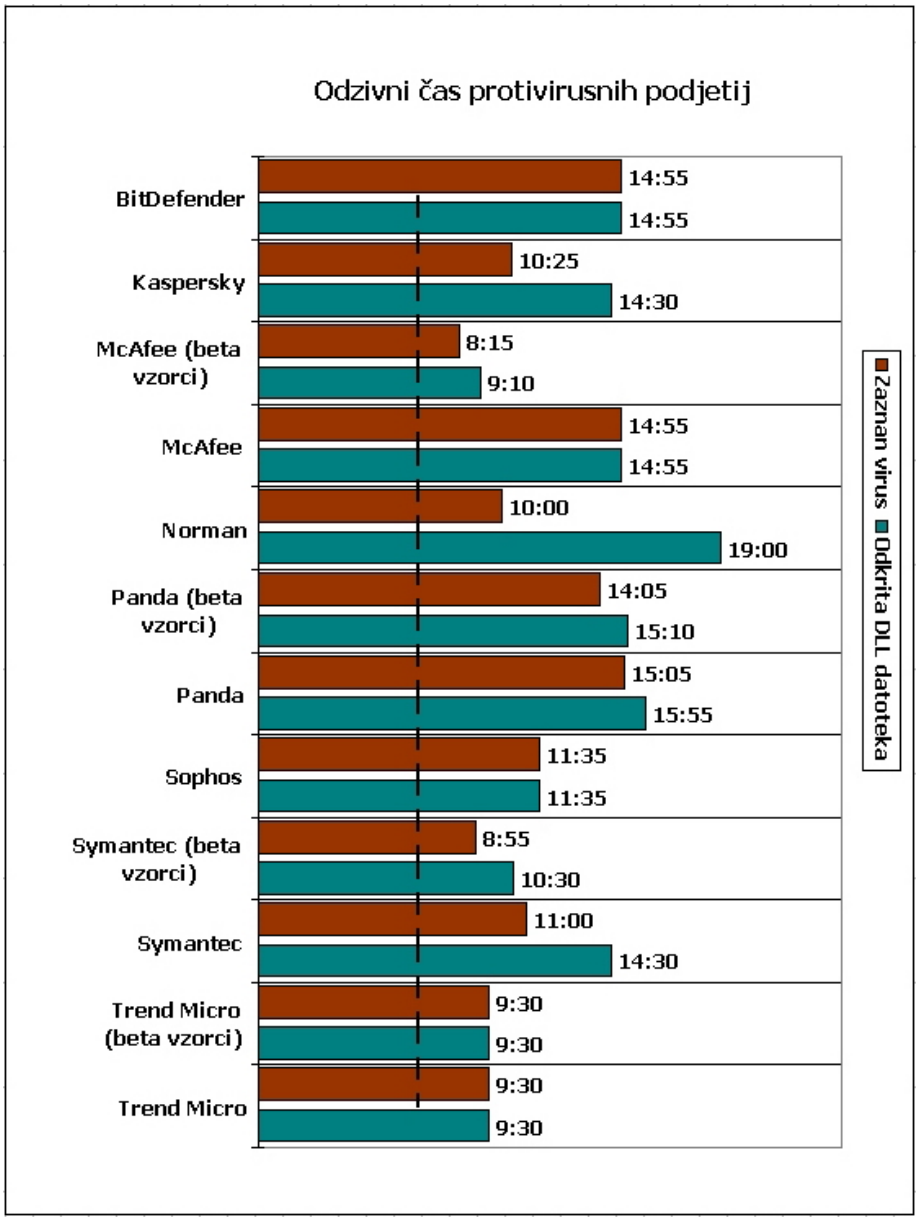
BitDefender	2003-12-20 at 13:20 h
Kaspersky	2003-12-20 at 14:45 h
F-Prot (Frisk)	2003-12-20 at 15:25 h
F-Secure	2003-12-20 at 15:45 h
Norman	2003-12-20 at 18:25 h
eSafe (Aladdin)	2003-12-20 at 18:35 h
Trend Micro	2003-12-20 at 19:50 h
AVG (Grisoft)	2003-12-20 at 20:15 h
AntiVir (H+BEDV)	2003-12-20 at 22:20 h
Symantec	2003-12-21 at 04:05 h
Avast! (Alwil)	2003-12-21 at 09:55 h
Sophos	2003-12-21 at 14:35 h
Panda AV	2003-12-21 at 17:05 h
McAfee/NAI	2003-12-22 at 04:10 h
Ikarus	2003-12-22 at 10:35 h
eTrust (CA)	2003-12-22 at 17:50 h
AVK (G Data)	2003-12-23 at 23:50 h

Vir: AV-Test.org: Outbreak response times - putting AV to the test, 2004.

Zgoraj predstavljeni preizkus je povzročil velik odziv pri vseh protivirusnih podjetjih in varnostnih strokovnjakih. Dejstvo, da so tudi najboljša podjetja potrebovala 10 ur za pripravo ustrezne rešitve ob napadu črva Win32/Sober.C, je grozeče. Številna podjetja, ki so »zaspala« in ustrezne popravke objavila šele čez dan ali dva, so bila deležna številnih kritik.

Podoben periodični preizkus je sledil tudi ob izbruhu črva Win32/MyDoom.A, prvega februarja 2004. Rezultati odzivov protivirusnih podjetij se nahajajo v tabeli 25. Računalniški virus MyDoom.A, ki se širi preko elektronske pošte ter omrežja za izmenjavo datotek Kazaa, premore dve komponenti, po katerih ga je moč odkriti – samo škodljivo kodo virusa ter DLL datoteko, ki jo pusti za seboj. V tabeli 25 so označeni časi, potrebni za odziv posameznih protivirusnih podjetij. Prve zaznave novega virusa so se pojavile dobrih šest ur in pol pred njegovim masovnim izbruhom, ki je v sliki 29 označen s črtkano črto. Tokrat so najboljše ekipe posameznih podjetij potrebovale nekaj manj kot devet ur za pripravo ustreznih posodobitev za odpravo virusa, najslabše pa celih 19 ur.

Slika 28: Odzivni čas protivirusnih podjetij ob izbruhu črva Win32/MyDoom.A



Vir: PC Magazine: Why your antivirus program won't catch the next attack, 2004.

Kot vidimo, se je odzivni čas protivirusnih podjetij ob izbruhu virusa Win32/MyDoom.A glede na izbruh črva Win32/Sober.C nekoliko zmanjšal, še vedno pa velja, da podjetja potrebujejo več ur, preden izdelajo in distribuirajo varnostno rešitev. Med tem časom pa so računalniški sistemi bolj ali manj prepuščeni sami sebi. Seveda je ob pravilno implementiranih varnostnih mehanizmih in upoštevanju varnostne politike podjetja možnost za okužbo majhna, a obstaja.

Protivirusni ponudniki tako vseskozi bijejo bitko s časom, saj morajo v najkrajšem možnem času pripraviti rešitev za odstranitev posledic virusne okužbe. Problematično je tudi zavedanje nove nevarnosti, saj veliko računalniških virusov in črvov ob svojih začetkih okužb ni hitro vidnih, dokler dosežejo kritične mase – okužijo večje število računalnikov in strežnikov, nakar se začne število okuženih računalnikov eksponencialno večati.

5.4 PONUDNIKI INTERNET DOSTOPA

Tudi ponudniki internet dostopa (ang. ISP – internet service providers) lahko marsikaj naredijo za manjše širjenje računalniške nesnage in posledično zmanjšanje poslovne škode. Večja podjetja imajo običajno lastne strežnike za elektronsko pošto, za manjša podjetja v Sloveniji pa takšna investicija pogosto ni racionalna, zato le-ta raje zakupijo več e-poštnih predalov pri svojem ponudniku dostopa do interneta. Kot je pokazala raziskava ICSA Labs, se večina računalniških virusov in črvov širi ravno preko elektronske pošte, kjer naletijo na svoje cilje – žrtve – nezavedne uporabnike.

V ta namen sem pridobil tudi podatke o domačem prometu z elektronsko pošto. Podatke za mesec avgust 2004 sta posredovala dva največja domača ponudnika internet storitev, podjetji SiOL, d. o. o., ter Medinet, d. o. o.[25], podatkov akademsko-raziskovalnega omrežja ARNES[26] pa žal nisem uspel pridobiti.

Obravnavana domača ponudnika internet storitev preko svojih strežnikov za elektronsko pošto vsak delavnik prejmeta ter odpošljeta okoli milijon in pol elektronskih sporočil. Seveda je vsa pošta pregledana s protivirusnimi programi za škodljivimi vsebinami. SiOL-ovi strežniki na delovni dan v povprečju obdelajo 1,2 milijona, AMIS-ovi pa 0,3 milijona sporočil. Ob vikendih količina elektronske pošte nekoliko upade, a še vedno znaša skupni seštevek okoli 0,85 milijona sporočil (SiOL 0,7 ter AMIS 0,15 milijona sporočil) na dan. V mesecu avgustu sta tako oba ponudnika internet storitev na svojih strežnikih pregledala kar dobrih 41 milijonov elektronskih sporočil. Takšna količina seveda zahteva tudi izjemno zmogljivo strojno opremo (računalnike), zato je SiOL-ov poštni strežnik ob posameznih izbruhih računalniških poštnih črvov imel tudi krajše zamike pri dostavi elektronske pošte. Količina elektronske pošte se namreč ob izbruhih škodljivih kod, predvsem računalniških virusov in črvov, ki se razpošiljajo preko elektronske pošte, v določenem časovnem intervalu drastično poveča – tudi za večji mnogokratnik.

Med vsemi sporočili, ki jih pregledajo SiOL-ovi poštni strežniki, jih je okuženih približno 15 odstotkov, neželene pošte pa kar 70 odstotkov. Podjetje Medinet, d. o. o., poroča o 60 odstotkih odvečne elektronske pošte. Zanimiva je tudi vsebina zavrnjene/blokirane elektronske pošte – približno polovica elektronskih sporočil, ki jih protivirusni program zavrne, vsebuje virus, druga polovica pa predstavlja neželeno pošto, t. i. spam. Poštni strežniki obeh podjetij vsa sporočila, ki vsebujejo računalniški virus ali drugo škodljivo kodo, blokirajo in s tem preprečijo, da bi virus dosegel naslovnika. Oba ponudnika internet storitev pričakujeta, da se bo s koncem poletnih mesecev ter jesenjo in povečano delovno aktivnostjo v podjetjih ter izobraževalnih ustanovah število okuženih sporočil še povečalo.

Seveda obstaja pri pregledu vse elektronske pošte tudi možnost, da protivirusni program zaradi različnih razlogov zavrne dobro (neokuženo) elektronsko sporočilo. Pri SiOL-u so potrdili, da so takšne težave v preteklosti imeli, a so le-te sedaj popolnoma odpravljene. Zaradi nedostavljenih ali napačno dostavljenih sporočil, za katere bi bil lahko kriv protivirusni program, namreč v mesecu avgustu 2004 niso prejeli nobenih pritožb uporabnikov. Tudi AMIS-ovi poštni strežniki in njihova protivirusna zaščita so skorajda

[25] Podjetje Medinet, d. o. o., je upravitelj omrežja Amis.

[26] Kratica ARNES označuje akademsko in raziskovalno mrežo Slovenije. Javni zavod ARNES je bil ustanovljen z namenom, da skrbi za načrtovanje, organiziranje in upravljanje računalniških povezav med organizacijami s področja raziskovanja, razvoja, izobraževanja in kulture, za povezovanje v izobraževalna in raziskovalna omrežja v drugih državah in s tem posredno tudi v svetovno internet omrežje.

nezmotljivi. Ocene tehničnega osebja o nepravilno zavrnjenih e-poštnih sporočilih v mesecu avgustu 2004 se ustavijo pri številki 10, kar je tudi odličen rezultat glede na milijonski promet, ki mesečno poteka čez te strežnike. Tovrstne napake naj bi v večini primerov zakrivili le drugi poštni strežniki (predvsem tuji), ki se ne držijo predpisanih standardov za pošiljanje elektronske pošte. Oba ponudnika internet dostopa se v svojih omrežjih srečujeta tudi z različnimi računalniškimi virusi in črvi, ki se razmnožujejo s pomočjo varnostnih lukenj v sistemih. Kadar strokovnjaki v podjetju zaznajo tovrstno dejavnost, začasno blokirajo promet preko vrat, ki povzročajo širjenje okužbe, v celotnem omrežju. Tako preprečijo širši razmah okužb, dokler podjetja in domači uporabniki ne zakrpajo varnostnih lukenj v svojih računalniških sistemih.

Domača ponudnika internet storitev imata izdelano strategijo, kako ravnati v primeru večjih okužb računalniških sistemov v omrežju. Na podlagi prispelih obvestil tehnična služba fizičnega uporabnika takoj izklopi, da prepreči nadaljnje širjenje okužbe, nato ga nemudoma obvesti, da ima okužen računalnik in da ga mora očistiti. Po izkušnjah obeh ponudnikov namreč velika večina uporabnikov ne ukrepa, če jim pustijo povezavo v internet omogočeno. Podjetja o okužbi najprej obvestijo in jih nato v primeru neupoštevanja opozoril po določenem času tudi izključijo.

Tuji strokovnjaki ocenjujejo, da naj bi evropski internet ponudniki v letih 2004 in 2005 za preprečevanje okužb z računalniškimi črvi in odpravo posledic teh okužb porabili okoli 282 milijonov evrov (Jaques, 2004).

5.5 IZOBRAŽEVANJE ZAPOSLENIH

Vsej tehnologiji navkljub ima človek še vedno zadnjo besedo. Pri računalniških virusih ni nič drugače. Največji problem okužb z računalniškimi virusi je namreč nevednost, neznanje uporabnikov. Ti pri svojem delu lahko kaj hitro okužijo računalnik z računalniškim virusom, če ne upoštevajo varnostnih pravil. Odpiranje neznanih poštnih priponk, obisk spletnih strani s sumljivo vsebino so le delci človeške radovednosti, ki večkrat povsem nezavedno pripelje do okužbe z računalniškim virusom. Glede na hitrost širjenje sodobnih računalniških črvov se lahko okužba iz enega računalnika v podjetju v vsega nekaj minutah preseli še na vse ostale delovne postaje in strežnike, še posebej v t. i. kritičnem obdobju[27] ob izbruhih novih virusov.

To so relativno hitro ugotovila tudi podjetja, saj se deleži okužb pri podjetjih v primerjavi z domačimi uporabniki močno manjšajo. Zasluge pri tem gredo predvsem izdelani varnostni politiki podjetja, ki jo ima vedno več podjetij, izdatnejši skrbi za ustrezno strojno in programsko opremo ter nenazadnje tudi izobraževanju zaposlenih. Prav pri slednjem je še veliko rezerv; podjetja oziroma strokovnjaki v podjetjih bi morali večkrat podučiti zaposlene o nevarnih posledicah računalniških virusov in ustrezni preventivi. Tudi sankcije, predvsem finančne, so ena izmed metod »izobraževanja« zaposlenih, ki jo včasih uporabijo v podjetjih. Ameriška študija laboratorijev ICSA Labs namreč vsako leto nazorno kaže določen delež zaposlenih, ki med učinke ter posledice računalniških virusov prištevajo tudi nevarnost izgube delovnega mesta.

Cilj podjetij je pri svojih zaposlenih doseči zavedanje nevarnosti in škode, ki jo lahko okužba z računalniškim virusom povzroči v podjetju. Razložiti jim morajo tudi načine, kako se pred virusi obraniti in kaj storiti, če do okužbe z računalniškim virusom dejansko pride.

[27] Kritično obdobje je opredeljeno od trenutka, ko je virus opažen, do trenutka, ko protivirusna podjetja ponudijo ustrezno zaščito.

6. SKLEP

Računalniški virusi in črvi so digitalna kuga 21. stoletja. Predstavljajo veliko nevarnost za podjetja in domače uporabnike, pravzaprav kar za globalno ekonomijo, ki vsako leto zaradi posledic virusnih napadov utrpi milijardno škodo – v poljubni svetovni valuti. Število okužb narašča iz leta v leto in težko je napovedati, kdaj se bo trend rasti ustavil. V bližnji prihodnosti se to najverjetneje ne bo zgodilo. Razlogov za pesimistične napovedi je več. A prevladati mora optimizem, moč in volja po odpravi digitalnih škodljivcev.

Več korakov je že bilo narejenih v pravo smer. Proizvajalci protivirusne opreme, ki bo v prihodnosti postala ključno orožje v tem boju, se trudijo v svoje protivirusne programe vgraditi kar največ funkcij odkrivanja in preprečevanja razvoja škodljivih kod. Prav tako se pričakuje od monopolista na trgu operacijskih sistemov, Microsofta, bistvene izboljšave varnostnih mehanizmov, ki bi pripomogle manjšanju števila škodljivih kod. To se ne bo zgodilo čez noč, vendar lahko pričakujemo, da bo ob ustreznem razvoju strojne in programske opreme operacijski sistem Microsoft Windows postal varna platforma okoli leta 2010.

Podjetja bodo morala poskrbeti za kar najboljšo implementacijo teh varnostnih rešitev in izobraževanje zaposlenih. Prav tu sam vidim ključ do uspeha. Ljudi, uporabnike računalnikov ter zaposlene po podjetjih, je treba seznaniti z nevarnostmi in posledicami škodljivih zlonamernih kod. Danes so ti škodljivci še vedno podcenjeni, čeprav se stalno pojavljajo kot glavni akterji bombastičnih časopisnih naslov ter TV poročil.

Svoj delež bo morala prispevati tudi zakonodaja in organi pregona, ki bodo posamezne oddelke specializirali za lov digitalnih kriminalcev. Kraja ali poškodovanje ključnih informacij v podjetjih namreč vse pogosteje vodita v ekonomski propad.

7. LITERATURA

1. Ahuja Vijay: Secure Commerce on the Internet. London : Academic Press, Inc., 1997. 298 str.
2. Gupta Uma G.: Information systems Success in the 21st Century. New Jersey : Prentice Hall, 2000. 464 str.
3. Hajtnik Tatjana: Priporočila za pripravo informacijske varnostne politike. Ljubljana : Center Vlade RS za informatiko, 2002. 231 str.
4. Murčehajič Hari: Nove grožnje z interneta. Trebnje : Ribera, d. o. o., 2003. 31 str.
5. Oldfield Paul: Computer viruses demystified. Oxford : Sophos Plc., 2001. 72 str.
6. Shimmin Bradley: Effecitive e-mail: File transfer, Security and Interoperability. London : Academic press Limited, 1997. 292 str.

8. VIRI

1. AV-Test.org: Outbreak response times - putting AV to the test. [URL: http://www.av-test.org/down/papers/2004-02_vb_outbreak.pdf], 21. 6. 2004.
2. Bennet, Madeline: Virus costs keep rising. [URL: http://www.vnunet.com/news/1139852], 19. 6. 2004.
3. Burke, Brian E.: Worldwide Secure Content Management 2004–2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security. [URL: http://www.idc.com/getdoc.jsp?containerId=fr2004_08_18_163332], 28. 8. 2004.
4. Computer mail services: Spam cost calculator. [URL: http://www.cmsconnect.com/Marketing/spamcalc.htm], 21. 6. 2004.
5. F-Secure: Opisi virusov. [URL: http://f-secure.kabi.si/], 21. 6. 2004.
6. Firewalls: a technical overview. [URL: http://www.boran.com/security/it12-firewall.html], 21. 6. 2004.
7. Granneman Scott: Infected in twenty minutes. [URL: http://www.securityfocus.com/columnists/262], 21. 8. 2004 .
8. ICSA Labs Computer Virus Prevalence Survey 2003. [URL: http://www.icsalabs.com/2003avpsurvey/index.shtml], 21. 6. 2004.
9. Interni podatki slovenskih protivirusnih podjetij, 2004.
10. Jaques Robert: Worms to cost European ISPs £188m. [URL: http://www.vnunet.com/news/1155469], 28. 6. 2004.
11. Murčehajič, Hari: Panda Software na trg poslala novo tehnologijo TruPrevent. Ribera, d. o. o., sporočilo za javnost, 25. 8. 2004.
12. PC Magazine: Why your antivirus program won't catch the next attack. [URL: http://www.pcmag.com/article2/0,1759,1586106,00.asp], 25. 8. 2004.
13. SANS Institute Internet Storm Center: Survival Time History. [URL: http://isc.sans.org], 18. 6. 2004.
14. Thurrtott Paul: OS Market Share: Microsoft Stomps the Competition. [URL: http://www.winnetmag.com/Article/ArticleID/40481/40481.html], 11. 7. 2004.
15. Varovanje informacijskega premoženja. [URL: http://www.nevarnost.net/index.php], 26. 6. 2004.
16. Wikipedia: Timeline of notable computer viruses and worms. [URL: http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms], 21. 6. 2004.