UNIVERZA V NOVI GORICI
POSLOVNO-TEHNIŠKA FAKULTETA

PREPREČEVANJE IN ODPRAVLJANJE ŠKODE ZARADI RAČUNALNIŠKIH VIRUSOV V PODJETJIH

DIPLOMSKO DELO

Stojan Humar

Mentor: doc. dr. Bogdan Filipič

Nova Gorica, 2008

ZAHVALA

Najlepše se zahvaljujem mentorju doc. dr. Bogdanu Filipiču za nasvete in pomoč pri izdelavi diplomske naloge ter veliko mero potrpežljivosti, Univerzi v Novi Gorici za pridobljeno znanje ter podjetju HiSoftPLUS d.o.o., ki mi je omogočilo opravljanje praktičnega usposabljanja. Posebej se zahvaljujem tudi domačim za razumevanje in vso podporo ter slavistki Majdi Malik za lektoriranje besedila.

IZVLEČEK

Danes si računalnika brez stalne modemske povezave v internet ne moremo predstavljati. In če smo lahko pred nekaj leti z navadno modemsko povezavo varno, a počasi brskali po spletnih straneh, lahko danes s stalno ADSL povezavo v internet okužimo računalnik v nekaj minutah. Diplomsko delo obravnava problematiko okužb z računalniškimi virusi in ostalo škodljivo kodo, saj lahko tak napad na računalniški sistem delno ohromi ali celo onemogoči poslovanje podjetja. Predstavljene so vrste škodljivih kod in tehnike zaščite operacijskih sistemov s požarnimi zidovi in ustrezno protivirusno zaščito. Na praktičnih primerih iz podjetij nato prikažemo postopke odpravljanja škode zaradi računalniških virusov in ovrednotimo s tem povezane stroške.

ABSTRACT

Nowadays we can not imagine computers without an ADSL internet connection. If we were a few years ago using the analog modem connection as slow but secure, there are now chances to infect our computer in just a few minutes. This diploma thesis deals with the issue of computer viruses and other harmful code. Such kind of attacks on a computer system of a company may partialy or entirely disrupt the bussiness processes. We present the types of harmful code and techniques of protection with firewalls and antivirus programs. With practical examples from companies we then show the procedures of recovery from computer viruses and evaluate the related costs.

KLJUČNE BESEDE

informacijska tehnologija, računalniško omrežje, internet, poslovni informacijski sistemi, operacijski sistem Windows, računalniški virusi, protivirusna zaščita

KEY WORDS

information techonology, computer network, internet, bussiness information systems, Windows operating system, computer viruses, antivirus protection

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

Stalna povezava računalnika v internet povečuje možnost napada na računalnik in okužbe z računalniškimi virusi. Modemski uporabniki so pred leti s pametnim ravnanjem lahko »preživeli« tudi brez protivirusne zaščite, medtem ko je danes ob priključitvi na širokopasovno omrežje uporaba protivirusne zaščite obvezna. Dejansko lahko ostane nezaščiten računalnik z ADSL povezavo neokužen le kratek čas. Njegova izpostavljenost okužbam je predvsem odvisna od spletnih strani, do katerih z njim dostopamo, varnostnih popravkov programske opreme ter spletnega brskalnika, ki ga uporabljamo.

Upravljalci računalniških sistemov v večjih podjetjih se zadnja leta strinjajo, da brezhibno delovanje računalnikov skorajda ni več možno brez ustrezne protivirusne zaščite. Žal pa popolne zaščite ni, pa naj se zanjo še tako trudimo. V ekonomskem svetu ima pretok informacij velik pomen, saj brez tega podjetja ne bi mogla poslovati. Zadnje čase pa tako poslovanje močno ogrožajo zlonamerni programi, ki so namenjeni povzročanju škode ali kraji podatkov, zato so lahko posledice oškodovanja podjetij velike.

Da bi zagotovili čimboljšo zaščito pred računalniškimi virusi in ostalo škodljivo programsko kodo, izbiro protivirusne opreme ponavadi prepuščamo računalniškim strokovnjakom. Seveda pa tudi če je oprema še tako dobra, brez pravilnih nastavitev ne dosežemo njene funkcionalnosti in učinkovitosti.

1.1 Cilji diplomskega dela

Glavni cilj diplomskega dela je predstaviti problematiko računalniških okužb, ki lahko povzročijo veliko gospodarsko škodo v podjetjih. Kljub sodobnim tehnologijam, namenjenim varovanju podatkov, je še vedno veliko podjetij, ki so bila izpostavljena napadom računalniških virusov ali drugih škodljivih kod. Temu pogosto sledi razočaranje. Kljub vsej zaščiti je podjetje lahko oškodovano zaradi izgube podatkov, nedelovanja računalniških sistemov in stroškov odpravljanja posledic. Obstajajo namreč določene tehnike reševanja podatkov, vendar njihova uporaba zahteva čas in prinaša stroške.

Popolne zaščite računalniških sistemov in informacij ni in je ne bo, pa naj si še tako prizadevamo ohraniti sistem neokužen in stabilen. Velikokrat je za računalniške okužbe kriv tudi človeški dejavnik. Predvsem gre za slabo usposobljenost, včasih pa tudi radovednost zaposlenih. Stroški vzdrževanja računalniškega omrežja na najvišji ravni zaščite so lahko zelo visoki, vendar zanemarljivo majhni v primerjavi z možno nastalo poslovno škodo.

Sistemski administratorji v večjih podjetjih računalniške sisteme zaščitijo že ob vstopni točki, ki predstavlja povezavo v omrežje. Takšne sistemske rešitve so lahko zelo drage, zato o njihovi izvedbi odloča vodstvo podjetja, a žal velikokrat prepozno.

Za obravnavo tematike o preprečevanju in odpravljanju škode zaradi okužb z računalniškimi virusi v podjetjih smo se odločili v sodelovanju z računalniškim podjetjem HiSoftPLUS d.o.o., ki poleg trženja poslovnih programov tudi vzdržuje vse računalniške sisteme svojih strank.

1.2 Pregled vsebine

V drugem poglavju diplomske naloge predstavljamo računalniško podjetje, v katerem je bilo opravljeno praktično delo na nalogi. Opisana je glavna dejavnost podjetja in način poslovanja s strankami v oddelkih strojne in programske opreme. Opredeljeni so tudi načini zaščite v podjetjih, ki jih je potrebno vzpostaviti glede na velikost in obseg poslovanja posameznega podjetja.

V tretjem poglavju opredelimo škodljive programske kode in na kratko opišemo posamezne skupine. Ta del zajema tudi delitev in opis virusov, črvov, trojanskih konjev, vohunskih programov in ostale škodljive kode. Za lažje razumevanje obravnavane problematike je opisanih tudi nekaj konkretnih primerov škodljivih kod.

Temeljni postopki varovanja podatkov v podjetjih, požarni zidovi, izboljšave programske opreme z novostmi operacijskega sistema Windows Vista ter splošne lastnosti protivirusnih zaščit z napredno tehnologijo zaznavanja in odstranjevaja škodljive kode so predstavljeni v četrtem poglavju.

V petem poglavju so opisani štirje primeri podjetij, ki so bila žrtve virusnih okužb ali groženj zaradi drugih škodljivih programov. Primeri se med seboj razlikujejo po velikosti podjetja, vrsti okužbe in načinu odpravljanja težav. Vsak izmed opisanih primerov je stroškovno ovrednoten.

V zadnjem, šestem poglavju sledijo še zaključne ugotovitve in priporočila o ustrezni izbiri protivirusne zaščite, ki so koristna za vsako podjetje.

2 PREDSTAVITEV RAČUNALNIŠKEGA PODJETJA

2.1 Splošno o podjetju

Podjetje, v katerem je bilo opravljeno v tej nalogi opisano delo, se imenuje HiSoftPLUS d.o.o. Sedež podjetja je v Ozeljanu. V tehničnem oddelku je zaposlenih pet programerjev in šest serviserjev. Osnovna dejavnost podjetja je razvoj in trženje poslovnih informacijskih sistemov za potrebe gostinstev, prodajaln na debelo in drobno, proizvodnih podjetij, pa tudi knjigovodskih in računovodskih servisov. Pokritost tržišča zajema celotno Slovenijo, poudarek pa je na primorski regiji. Naloga serviserjev je vzdrževanje računalnikov, tako strojne kot programske opreme, skrb za zaščito in optimalno delovanje računalniških omrežij, vključno z nameščenimi uporabniškimi programi.

Delo je obsegalo predvsem postavitve in vzdrževanje računalniških omrežij, strežnikov in širokopasovnih ADSL povezav ter nameščanje ostale programske opreme v podjetjih. Z nekaterimi večjimi podjetji smo imeli sklenjene vzdrževalne pogodbe. Ta so bila glede vzdrževanja na prednostni listi, kar je pomenilo tudi stalno pripravljenost za pomoč v njihovem delovnem času. Vzdrževalne pogodbe so se obračunavale mesečno, znesek pogodb pa je bil odvisen od velikosti podjetja oziroma števila računalnikov z nameščenimi programi podjetja HiSoftPLUS.

Največ časa smo posvetili problematiki virusnih okužb računalniških sistemov in varovanju podatkov, zato se v diplomskem delu posvečamo pogledu škodljivih kod ter ukrepom za preprečevanje okužb in odpravljanje škode, s poudarkom na praktičnih primerih iz več podjetij.

2.2 Zaščita računalniških omrežij

Podjetje HiSoftPLUS daje največji poudarek zaščiti računalniških omrežij in sistemov v podjetjih, ki poslujejo z veliko količino občutljivih podatkov. Takšni podatki so predvsem računovodski izkazi, podatkovne baze poslovnih informacijskih sistemov, elektronski plačilni promet ter ostali dokumenti, ki so temelj uspešnega poslovanja vsakega podjetja, zato jih moramo čimbolje zaščititi.

Osnova zaščite v takšnih podjetjih se pričenja na strojnem nivoju. Novejši usmerjevalniki imajo že vgrajene mnoge funkcije za postavitev brezžičnih omrežij, filtriranje podatkov, omogočajo pa tudi nadgradnjo programske opreme naprave. S pravilno nastavitvijo usmerjevalnika smo onemogočili dostope do določenih spletnih strani ali do določenih računalnikov v omrežju. V takem omrežju smo na vse računalnike v kombinaciji s programskim požarnim zidom Zone Alarm Pro namestili boljše protivirusne zaščite. Najpogosteje izbrana je bila protivirusna zaščita Panda Titanium, ki pa žal zahteva visoko zmogljivost računalnika.

Zaščita računalnikov, ki so se povezovali le v lokalno omrežje, je bila na bistveno nižjem nivoju. Operacijskemu sistemu Windows XP je bil dodan le paket najnovejših varnostnih popravkov. Funkciji samodejnih posodobitev sistema in dostopa do oddaljenega računalnika sta bili izključeni. Omogočen je bil le požarni zid.

Poleg zaščite na strojnem nivoju lahko računalniško omrežje in posamezne delovne postaje v omrežju zaščitimo s pravilno nastavitvijo vgrajenih funkcij, ki jih ponuja Windows XP SP2. To je nadgradnja osnovne različice operacijskega sistema Windows XP z večjim poudarkom na varnosti. Vsebuje najnovejše popravke operacijskega sistema, dodano pa je še varnostno središče (angl. security center), ki preverja prisotnost protivirusne zaščite, samodejnih posodobitev sistema in funkcije integriranega požarnega zidu.

3 RAČUNALNIŠKI VIRUSI IN DRUGA ŠKODLJIVA KODA

3.1 Definicija računalniškega virusa

Splošno gledano spadajo vsi škodljivi računalniški programi v širšo skupino zlonamernih kod. Glede na tehnike širjenja in škodo, ki jo lahko povzročijo, pa škodljive računalniške programe delimo v štiri skupine:

- 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 ali zagonski sektor na disketi, trdem disku ali drugem pomnilniškem mediju. Značilno za računalniške viruse in črve je tudi, da se razmnožujejo sami. Trojanski konji in programske bombe se navadno sami ne razmnožujejo, čeprav obstajajo tudi virusni hibridi, ki se znajo samodejno širiti.

3.2 Računalniški virusi

Računalniške viruse uvrščamo med zlonamerno programsko kodo, ki se pripne na program ali datoteko z namenom, da bi se razširila iz enega računalnika v druge in jih na ta način okužila. Zanje velja, da povzročajo najrazličnejšo škodo, ki se kaže v upočasnjenem delovanju računalnika, nestabilnosti operacijskega sistema, izjemoma tudi delni ali popolni izgubi podatkov. V hujših primerih lahko celo uničijo strojno opremo. Primer take zlonamerne kode je bil virus WIN95.CIH, ki je uničil osnovne sistemske nastavitve, potrebne za zagon računalnika in njegovo delovanje. Virusi za svoje širjenje potrebujejo gostitelja (programska ali podatkovna datoteka, zagonski sektor na disku, disketi itd.) in se sami razmnožujejo.

Virusi so pri širjenju odvisni od človeškega dejanja, kot je dodeljevanje datotek v skupno rabo ali pošiljanje elektronske pošte. Glede na cilj in način delovanja jih delimo v več kategorij (Rubikon, Več o virusih, 2007):

- zagonski virusi,
- parazitni virusi,
- spremljevalni virusi,
- povezovalni virusi,
- makro virusi,
- večpartitni virusi.

Zagonski virusi okužijo ali poškodujejo zagonsko datoteko operacijskega sistema. Širijo se lahko le iz okuženih zagonskih sektorjev na trdih diskih, disketnih enotah ali drugih pomnilniških medijih. Sistem se okuži šele takrat, ko z zagonskega sektorja poženemo okuženo datoteko. Takšni virusi so sicer danes vse redkejši, lahko pa jih najdemo pri prenosih datotek na internetu oziroma izmenjavi podatkov preko programov tipa P2P (angl. peer to peer), kot so npr. Kazaa, Emule in DC++. Ko enkrat virus okuži sistem, onemogoči zagonsko datoteko NTLoader, tako da ne moremo več zagnati operacijskega sistema. V takem primeru je potrebna njegova ponovna namestitev. Določene medije, kot npr. diskete, lahko zavarujemo pred okužbami tako, da jih zaklenemo in s tem dopustimo le branje podatkov.

Parazitni virusi okužijo sistem tako, da se pripnejo k izvršilnim datotekam, gonilnikom ali komprimiranim datotekam, pri tem pa spremenijo njihovo izvršilno kodo. Takšne viruse, ki okužijo datoteke, imenujemo tudi datotečni virusi. Aktivirajo se, ko sistem požene okuženo datoteko, pri tem pa okužijo še ostale datoteke. Za širjenje se lahko pripnejo na začetek, na konec ali v sredino datoteke.

Obstajajo tudi virusi, ki ustvarijo izvršilno datoteko z istim imenom, le z drugo končnico. Virus npr. program s končnico exe spremeni v program s končico com. Operacijski sistem daje namreč vedno prednost končnici com in tako se izvede

virusni program. V kolikor se število takih datotek hitro povečuje, gre zelo verjetno za okužbo z virusom tega tipa. Takšne viruse imenujemo spremljevalni virusi.

Izjemno nevarni virusi so povezovalni virusi, ker uporabljajo drugačno metodo okuževanja. Ne spremenijo vsebine izvršilne datoteke, ampak strukturo imenika in preusmerijo vnos imenika okužene datoteke na področje, ki vsebuje virusno kodo. Ko se izvede virusni program, lahko naloži izvršilno datoteko, poznavajoč pravilen datotečni vnos izvršilnega programa. Odstranjevanje takih virusov iz sistema je težko in tvegano, se pa k sreči redko pojavljajo.

Makro virusi se za razliko od vseh ostalih vrst virusov nahajajo v programskih orodjih, ki omogočajo generiranje programske kode. Koda je največkrat napisana v programskem orodju Visual Basic, ki spada v sklop programov Microsoft Office, kot so npr. Word, Excel, predvsem pa Access, ki je namenjen delu z relacijskimi podatkovnimi bazami. Makro virusi delujejo tako, da spremenijo ali zbrišejo obstoječe makro ukaze v programu in s tem povzročijo nepravilno delovanje programa. Zaradi varnosti so v novejših orodjih iz zbirke Microsoft Office makri, ki nimajo digitalnega potrdila, onemogočeni, tako da jih ni mogoče aktivirati.

Večpartitni virusi kombinirajo dva ali več osnovnih tipov virusov, ki smo jih opisali doslej. Poznamo na primer viruse, ki so zmožni okužiti izvršilne datoteke in Wordove datoteke, ter viruse, ki so zmožni okužiti izvršilne datoteke in zagonske sektorje. Nekateri starejši virusi pa ne spremenijo vsebine zagonskega sektorja, ampak delno spremenijo datotečno porazdelitev sistemske datoteke io.sys z namenom, da bi vključili zaporedje virusne kode na začetek te datoteke. Ko operacijski sistem bere datoteko io.sys, se naloži virusna koda prej kot koda datoteke io.sys. Virusna koda se izvede in tako okuži računalnik.

3.3 Črvi

Črvi (angl. worms) so skupina škodljivih računalniških programov. Črv se od virusa razlikuje po tem, da se lahko sam kopira. Za širjenje ne potrebuje gostitelja. Ko se naseli v operacijskem sistemu, se lahko širi sam. Nevaren je prav zaradi izjemne sposobnosti hitrega širjenja. Svoje kopije lahko pošlje na vse naslove iz poštnega imenika, računalniki naslovnikov pa naredijo isto, kar povzroči učinek domin. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, zato je potrebno včasih dosti dlje čakati na ogled posameznih spletnih strani. Ker se črvom ni treba širiti prek gostiteljskega programa ali datoteke, se lahko zajedo v sistem in omogočijo drugim osebam, da prevzamejo nadzor nad računalnikom. Glede na način, kako dosežejo uporabnika, jih razdelimo v naslednje skupine:

- črvi z vgrajenimi funkcijami za protokol pošiljanja elektronske pošte preko poštnega odjemalca (angl. SMTP): zlonamerne kode se iz prizadetega računalnika razpošljejo same, ne da bi uporabnik sploh vedel za to. Za razmnoževanje uporabljejo imenik poštnega odjemalca, programe MSN Messenger, NET Messenger ter Yahoo Pager in vse tiste, ki jih najdejo v HTM datotekah na računalniku;

- črvi, ki se širijo preko interneta in P2P programov: pri tem lahko izvedejo vrsto akcij, vključno s samodejnim zagonom. V tej skupini sta najbolj znana črva Nimda in Klez.I, ki izkoriščata ranljivost brskalnika Internet Explorer. Lahko se samodejno zaženeta, ko se sporočilo, ki prenaša črva, prikaže v predoglednem oknu;

- črvi, ki se širijo preko programov za klepetanje na internetu (angl. internet relay chat, IRC): mIRC_Worm, pIRC_Worm, vIRC_Worm.

3.4 Trojanski konji

Trojanski konji ali trojanci (angl. trojans) so programi, ki pridobijo dostop do računalnika na račun lažne identifikacije in povzročijo nezaželene stranske učinke. To skupino škodljivih programov lahko razdelimo v naslednje podskupine (Tittel, 2003):

- preprosti trojanski konji (angl. simple trojans): povzročajo škodo okuženemu sistemu ob zagonu programa ali kadar je izpolnjen določen pogoj. Zato temu tipu rečejo tudi logična bomba;

- trojanski konji z uporabo stranskih vrat (angl. backdoors): so trojanski konji, ki za napade na oddaljene računalnike uporabljajo t.i. stranska vrata. To so zaporedja ukazov, ki omogočijo uporabniku, da preskoči običajni varnostni sistem računalnika;

- trojanski konji za lovljenje pritiska tipk na tipkovnico (angl. keyloggers): pridobijo zaupne podatke, kot so gesla in številke kreditnih kartic. Informacije hranijo v posebnem dnevniku, do katerega lahko dostopa napadalec;

- trojanski konji s funkcijo zavračanja storitev (angl. denial-of-service, DoS): gre za novejšo podskupino trojancev, ki poskušajo blokirati delovanje spletne strani tako, da pošiljajo velike količine paketov ali pa nepravilne zahteve. Zelo poznan primer takšnega trojanskega konja je Trojan/D_O_S.Tfn2k, ki je poskušal blokirati nekatere obsežne spletne strani;

- trojanski konji, imenovani tatovi gesel (angl. password stealers): kradejo gesla, ki omogočajo nadzor nad računalnikom. Poleg tega poiščejo na računalniku še datoteke, ki bi vsebovale gesla ali druge zaupne informacije. Zbrane podatke pošljejo v kodirani obliki njihovemu avtorju;

- klikajoči trojanski konji (angl. trojan clickers): uporabljajo se za preusmeritev uporabnika na določeno spletno stran. To storijo tako, da pošljejo brskalniku

ukaz za odprtje določene strani ali pa zamenjajo sistemsko datoteko, v kateri so shranjeni internetni naslovi;

- presnemovalni trojanski konji (angl. trojan downloaders): so trojanci, ki prenesejo in zaženejo vrsto škodljivih programov iz interneta;

- posredovalni trojanski konji (angl. trojan proxies): delujejo kot posredovalni strežniki in omogočajo anonimni dostop do interneta preko okuženega računalnika. Zelo priljubljeni so med pošiljatelji elektronske pošte.

Vse tri doslej predstavljene kategorije škodljivih računalniških programov, t.j. virusi, črvi in trojanski konji, so lahko združene v en sam program. Primer take zlonamerne kode je Win32/Moridin, ki je hkrati (Rubikon, Več o virusih, 2007):

- virus, ki okuži izvršilne datoteke operacijskega sistema Windows in datoteke, pripravljene s programom Microsoft Word,

- črv, ki se širi s pomočjo programov za klepetanje na internetu IRC programov in poštnih odjemalcev, ki za pošiljanje pošte uporabljajo vmesnik MAPI (angl. messaging application programming interface), in

- trojanski konj z uporabo stranskih vrat, ki sprejema ukaze z oddaljenega računalnika.

3.5 Programske bombe

Programske bombe so ravno tako kot virusi škodljiva koda, vendar se od njih razlikujejo po tem, da se sprožijo na določen datum ali ko je izpolnjen določen pogoj. Takim vrstam programskih bomb pravimo časovne bombe oziroma logične bombe. Lahko povzročijo odpiranje oken, upočasnjeno delovanje računalnika ali pa tudi vnovičen zagon računalnika.

3.6 Vohunski programi

Vohunski programi (angl. spyware) zbirajo in pošiljajo informacije o spletnih straneh, ki jih uporabniki najpogosteje obiskujejo, čas povezav, celo spreminjajo nastavitve operacijskega sistema. Zbirajo tudi uporabnikove osebne ali zaupne informacije, kar bistveno prizadene zaupnost na računalniku shranjenih podatkov.

Obstajajo tudi programi za vohunjenje, ki lahko odkrijejo in poročajo, ali je nameščena programska oprema na računalniku legalna ali ne. Primer take vohunske programske opreme je Windows Genuine Advantage (So nelegalnim Windowsom šteti dnevi?, 2007), ki sporoči uporabnikom operacijskih sistemov Windows, če so njihovi programi legalni.

Med prave vohunske rekorderje spada program Cool Web Search (CoolWeebSearch, 2008), ki dobesedno prevzame celoten računalniški sistem, še posebej pa vpliva na delovanje brskalnika Internet Explorer. Njegova odstranitev je zelo težavna, včasih je potrebno celo ponovno namestiti operacijski sistem.

Pri večini okužb z vohunskimi programi so vidni znaki predvsem upočasnjen zagon brskalnika Internet Explorer ter odpiranje kopice novih oken v brskalniku. Takratna obremenjenost procesorja se lahko giblje tudi med 90% in 100%. Težavo z dostopom do interneta lahko začasno odpravimo z namestitvijo brskalnika Mozilla Firefox (Mozilla Firefox – bodi med rekorderji!, 2008), vendar je tak način reševanja problema le začasen.

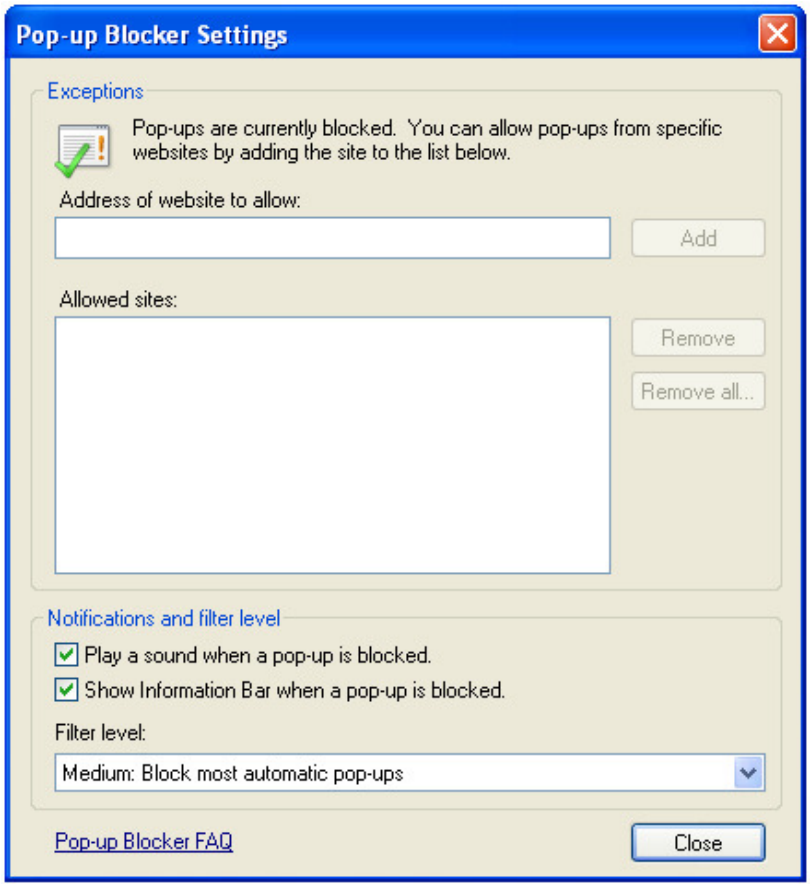
Najbolj razširjen vohunski in reklamni program na svetu se imenuje Gator ali po novem Claria. Simptomi okuženega računalnika se kažejo kot upočasnjeno delovanje računalnika, napačno delovanje spletnega brskalnika Internet Explorer, včasih pa tudi kot nestabilnost celotnega operacijskega sistema.

Namen vohunskih programov je, da prevzamejo identiteto uporabnika na več načinov (Spyware – vohunska programska oprema, 2007):

- berejo njegovo e-pošto,
- beležijo pogovore oziroma vse, kar uporabnik tipka,
- odtujijo bančne podatke (beležijo komunikacijo z banko, kar je lahko povezano s krajo gesla),
- onesposobijo delovanje interneta,
- upočasnijo delovanje računalnika z izvajanjem skritih nalog,
- spremenijo privzeto spletno stran,
- odpirajo oglase (angl. adware), lahko tudi dodajo orodne vrstice.

Vohunski programi največkrat okužijo sistem preko oglasnih pasic, če oglaševalci škodljivih programov prepričajo obiskovalce, da jih namestijo. Drugi način prenosa vohunskih programov je tudi uporaba P2P programov za imenjavo datotek, sistemov za komuniciranje tipa Messenger, spletnih iger, predvsem pa spletnih strani s pornografsko vsebino.

Večina škodljivih kod usmerja napade na različice brskalnikov Internet Explorer 6 ali starejše, ki imajo še vedno kopico nezakrpanih varnostnih lukenj. Novejši brskalniki, kot so Internet Explorer 7, Mozilla Firefox in Opera, pa se lahko že pohvalijo z višjo stopnjo varnosti, saj imajo že vgrajene komponente, kot so Pop-Up Blocker, Phishing Filter ter upravljalnik krmilnikov ActiveX. Slika 1 prikazuje nastavitev programa Pop-Up Blocker, ki preprečuje odpiranje pojavnih oken.



Slika 1: Nastavite programa Pop-Up Blocker v okolju Windows XP

4 UKREPI ZA PREPREČEVANJE ŠKODE V PODJETJIH

Škoda, ki jo povzročijo napadi računalniških virusov, je zelo različna, vsekakor pa je na prvem mestu padec produktivnosti. Večina okužb z virusi povzroči nestabilnost računalniških sistemov, nepravilno delovanje programov ali pa močno upočasni njihovo delovanje. V redkih primerih jih lahko okvari tako, da je potrebna ponovna namestitev. Vse to pa zahteva svoj čas in povzroča stroške vzpostavitve sistema v prvotno stanje. Večina podjetij, ki so utrpela škodo zaradi virusnih napadov, ne zaupa več v računalniške sisteme, saj so mnenja, da so ti preveč ranljivi.

Najpogostejši pokazatelji virusnih napadov v podjetjih, v katerih smo izvajali ukrepe za odpravo škode, so bili:

- nestabilnost operacijskega sistema,
- upočasnjeno delovanje sistema in programov,
- razmetani, preimenovani ali zbrisani podatki,
- nezanesljivost delovanja programov.

4.1 Izvori in širjenje okužb

Zadnja leta med izvori okužb prevladujeta elektronska pošta in okužene spletne strani. Virusi se širijo z različnimi mediji in so zadnje čase vse redkejši. Čeprav se podjetja vse bolj zavedajo te problematike, saj so osveščena, se še vedno večina okužb prenaša z elektronsko vsebino. Značilen primer virusne okužbe je bil črv MyDoom, ki se je širil v elektronski priponki. Črv se je na okuženem računalniku samodejno razposlal na vse naslove, shranjene v adresarju.

Obstajajo pa tudi trdoživi omrežni črvi, ki lahko ohromijo poslovanje podjetja celo za več dni. Zloglasen primer je bil črv Sasser (Sasser okužil milijone računalnikov, 2008), ki je okužil milijone računalnikov. Okrnil je delovanje nekaterih železnic, bank in celo uradov Evropske komisije.

4.2 Zaščita pred napadi v podjetjih

Računalniki se v podjetju med seboj povezujejo v lokalno omrežje. Lokalno omrežje pa je lahko v eni ali več točkah povezano v internet. Če želimo podjetje čimbolje zaščititi pred vdori, virusi in drugo škodljivo kodo, moramo zavarovati ravno vstopne točke. Načini zaščite so odvisni od velikosti podjetja ter količine in občutljivosti podatkov, s katerimi podjetje posluje. Pri varovanju informacijskega premoženja so ključni naslednji pristopi, ki morajo biti izpolnjeni za dobro zaščito informacij v podjetju (Bratuša, 2006):

- z varovanjem pred osebjem se določi možnost dostopa posameznika do terminala ali glavnega računalnika. Pomembna je tudi stopnja znanja, saj lahko neizobražen delavec nevede škoduje podjetju;

- z zaščito komunikacije preprečimo neavtorizirane dostope v omrežje ali računalniške sisteme. Nadzor dostopa z gesli omeji pretok komunikacij med računalniki v omrežju in prepreči zlorabe in nezakonita dejanja;

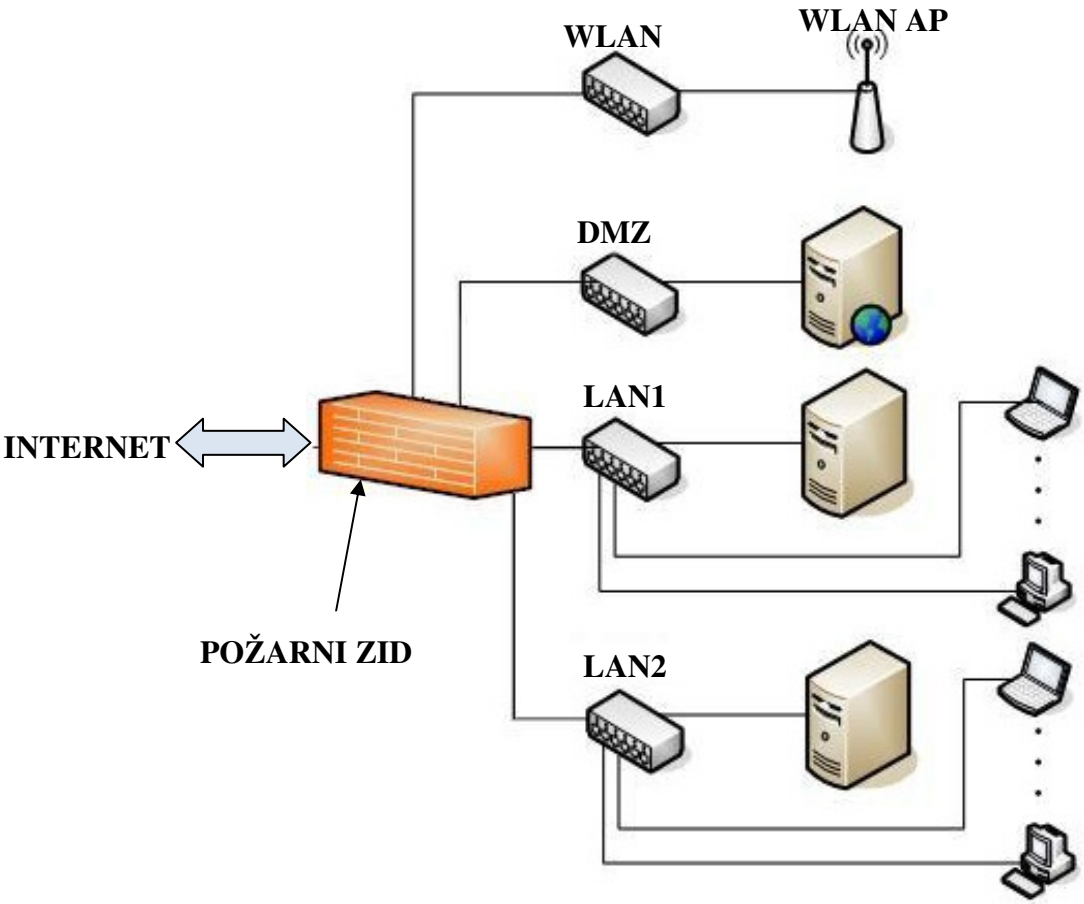
- z metodami šifriranja zaščitimo podatke v e-bančništvu, pri izmenjavi sporočil z agencijami za plačilni promet ter ostalimi agencijami za zbiranje in obdelavo podatkov o uspešnosti poslovanja podjetja. Varnostni ukrepi morajo zagotoviti zaupnost, celovitost, overjanje, preprečevanje tajenja in nadzor dostopa;

- z uporabo požarnih zidov, ki so učinkovita metoda, s katero napadalcem omejimo možnosti za vdor v sistem, hkrati pa nam omogoča varno uporabo interneta. Ustrezno zaščito omrežja dosežemo tudi s pravilno nastavitvijo požarnega zidu;

- z uporabo protivirusnih zaščit in protivohunskih programov lahko dobro zaščitimo računalnike v računalniškem omrežju. Izbiro ustrezne protivirusne zaščite pa prepušča vodstvo svojim administratorjem.

4.2.1 Požarni zidovi

Osnovne zaščite omrežja se začno pri postavitvi požarnega zidu, s katerim omrežje zaščitimo pred zunanjimi vdori. Požarni zid je strojna ali programska oprema, ki ščiti računalniški sistem pred vdori ali okužbami s škodljivimi programi. To naredi tako, da preverja podatke iz interneta ali omrežja in jim dovoli ali pa prepreči vstop v računalnik. Slika 2 prikazuje lokalno računalniško omrežje, povezano v internet preko požarnega zidu. V internet se preko lokalnih omrežij LAN1 in LAN2 povezujejo delovne postaje in osebni računalniki. Spletni strežnik dostopa do interneta preko omrežja DMZ (angl. demilitarized zone), ki je ločeno od našega krajevnega omrežja. Kratica WLAN AP (angl. wireless access point) pa pomeni brezžično dostopno točko, ki se največkrat uporablja pri vzpostavljanju brezžične povezave na razdalje do nekaj sto metrov.



Slika 2: Lokalna omrežja, povezana v internet preko požarnega zidu

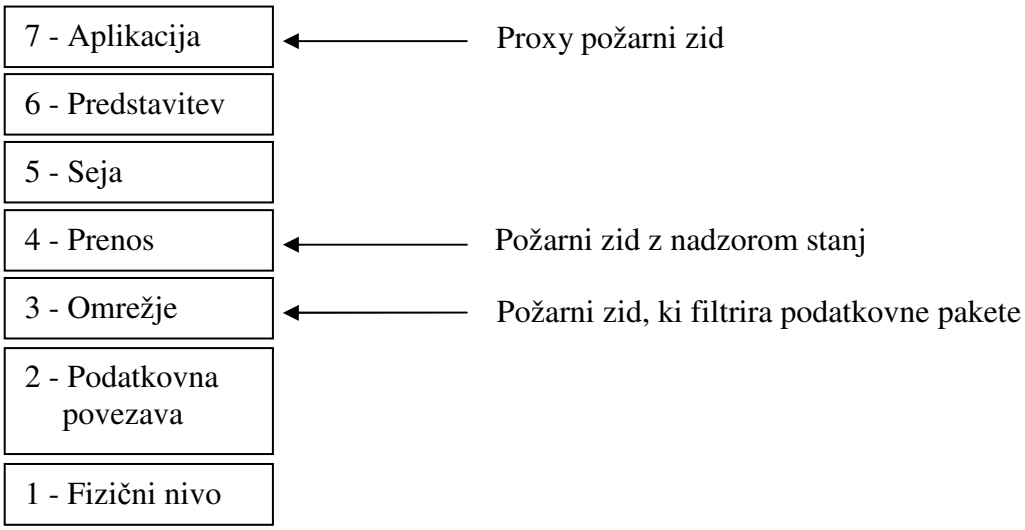
Za varovanje omrežja lahko uporabimo dvoje požarnih zidov:

- proxy požarne zidove,
- programske požarne zidove.

Proxy požarne zidove lahko opišemo z referenčnim OSI modelom (ISO/OSI referenčni model, 2008) (slika 3) povezanih odprtih sistemov za določanje okvira pri uvedbi komunikacijskih protokolov na sedmih nivojih. Podatki se v proxy strežnikih prenašajo iz enega nivoja na drugega. Začnejo se na nivoju aplikacij in napredujejo proti fizičnemu nivoju, nato se po hierarhiji spet vrnejo do svojega cilja.

Najpomembnejši nivo je aplikacijski, ki predstavlja vmesnik med ISO modelom in uporabnikom. Tu so definirani protokoli za prenos pošte, dostop do interneta, prenašanje datotek, ipd. Ostali nivoji skrbijo za komunikacijo med računalniki, ustrezno kodiranje za aplikacijski nivo, odpravljanje napak pri prenosu sporočil, upravljanje s povezavo med računalniki in določanje načina ugotavljanja napak.

Za pretok podatkov med temi nivoji pa skrbi fizični nivo, ki predstavlja električne in mehanske lastnosti vodnikov, po katerih potujejo podatki.



Slika 3: Referenčni model OSI in požarni zidovi

Više po modelu OSI so požarni zidovi strožji, delovanje pa se upočasni, ker ga spremenijo iz filtriranja paketov v požarne zidove proxy. Požarni zidovi, ki filtrirajo pakete in nadzorujejo stanja, so precej hitri v smislu pretoka, ki ga lahko obdelajo. Slabost proxy požarnih zidov je, da so počasnejši, ker imajo več dela. Za skoraj vse je tudi značilna zmožnost nadzora stanj na določenih povezavah. Pri proxy požarnih zidovih lahko izbiramo med načinom proxy ali filtriranjem paketov. Vkolikor imamo spletno mesto z manj prometa ali občutljivimi podatki, je primernejši požarni zid proxy.

Ponudba takšnih požarnih zidov je danes zelo pestra. Proizvajalci protivirusne opreme Panda Sofware (Panda GateDefender Performa, 2008) trenutno nudijo na tržišču tri različne modele proxy požarnega zidu GateDefender Performa. Sestavljata ga kakovostna in zmogljiva strojna in programska oprema za zagotavljanje maksimalne zaščite pred računalniškimi virusi, neželeno pošto ter poskusi vdorov v računalniško omrežje.

Najprestižnejši model GateDefender Performa serije 8000 premore kar 2 GB fizičnega spomina s procesorjem Xeon 3,2 GHz Duo. Največja zmogljivost filtiranja spletne vsebine je do 170 Mb/s ter 350 sporočil na sekundo. Primerna je za velika podjetja, saj zadošča za do 500 uporabnikov.

Poleg proxy požarnih zidov poznamo tudi programske požarne zidove. Takšen je npr. požarni zid, ki je vključen v operacijski sistem Windows XP SP2.

Znan programski požarni zid in hkrati tudi eno od najučinkovitejših orodij proti vdorom v operacijske sisteme je ZoneAlarm, ki omogoča veliko nastavitev. Zaščito je mogoče nastaviti za vsak program posebej in predpisati, pri kakšni povezavi (lokalna, internet) naj se ta zaščita izvaja. Ob vdoru v sistem nas program opozori in prikaže napako oziroma problem. Združljiv je z vsemi operacijskimi sistemi Windows. Žal pa je njegova slabost, da upočasni delovanje računalnika kot tudi pretok podatkov v omrežju zaradi nadzora programov, ki se izvajajo. Požarni zid nas obvešča o vsakem progamu, ki se želi povezati v internet zato je pred uporabo

programskega paketa priporočljiva predhodna nastavitev pravic posameznim aplikacijam, kot je prikazano na sliki 4.

Slika 4: Nastavitev pravic programom v požarnem zidu ZoneAlarm

4.2.2 Protivirusna zaščita

Razvijalci protivirusnih zaščit in varnostni strokovnjaki so enotnega mnenja, da so računalniški virusi in ostala škodljiva programska koda vse večja problematika 21. stoletja. Škoda, ki jo škodljiva programska koda vsakodnevno povzroča, je težko izmerljiva. Sklepamo pa lahko, da se zneski škode vrtijo v milijardah evrov.

Danes protivirusni programi že dolgo ne ščitijo le pred računalniškimi virusi, temveč imajo vgrajene še ostale module kot so:

- požarni zid,
- začita pred neželeno e-pošto (angl. antispam),
- samodejne posodobitve.

Najnovejši protivirusni programi pa se poslužujejo tudi novih tehnologij, imenovanih SandBox (Patentirana tehnologija Norman Sandbox, 2008), za odkrivanje še neznanih računalniških virusov. Primer takšne nove tehnologije je tudi Pandin

TruPrevent. Gre za tako imenovano sočasno kreiranje virtualnega računalniškega sistema, v katerem se izvajajo isti procesi kot na dejanskem sistemu. Vsi novi procesi se najprej naložijo v virtualni 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 na dejanskem sistemu. Seveda ta tehnologija zahteva več sistemskih virov kot običajni protivirusni program, a glede na povprečne računske in pomnilniške zmogljivosti sodobnih računalnikov ne predstavlja prevelikih obremenitev delovanja sistema.

Nekateri boljši protivirusni programi v sebi poleg pogona za hevristično iskanje virusov združujejo tudi orodja za odkrivanje vohunske programske opreme, filtriranje spletne vsebine (angl. anti-phishing), nadzor telefonske povezave, zaščito brezžičnih omrežij itd.

4.2.3 Nadzor dostopa uporabnikov

Z nadzorom dostopa zaščitimo komunikacijske točke in preprečimo nepooblaščene dostope v računalniške sisteme ali omrežje.

V velike omrežne sisteme lahko uvrstimo podjetja, ki imajo poleg osrednje lokacije več oddaljenih enot. Vsaka enota ima svoje lokalno omrežje, ki se povezuje v internet in tvori celoto računalniškega omrežja v podjetju ali organizaciji. Pri tako velikem številu računalnikov in razpršenosti omrežja je priporočljiva vzpostavitev navideznega zasebnega računalniškega omrežja (angl. virtual private network, VPN), ki je temelj varne medsebojne omrežne komunikacije z možnostjo nadgraditve velikega števila IP naslovov.

Z navideznim zasebnim omrežjem se lahko prek javnega omrežja varno povezujemo v poslovno računalniško omrežje kadarkoli in kjerkoli. Navidezno zasebno omrežje se danes v podjetjih uporablja za podporo intraneta in ekstraneta s šifriranjem podatkov pred njihovim pošiljanjem skozi javno omrežje. Prednost zasebnega omrežja je tudi nastavitev pravic dostopa v omrežje za uporabnike iz oddaljenih računalnikov.

Pri postavitvi velikih omrežij, ki so skoncentrirana na eni lokaciji, je priporočljiva nastavitev ene ali več domenskih skupin. Nastavitev domenskih skupin omogoča povezljivost več sto ali tisoč računalnikov v sklop računalniškega omrežja. Administratorske pravice v domenskih skupinah upravljajo administratorji na strežnikih. Upravljanje celotnega omrežja je hitro in enostavno, saj se nastavitve uveljavijo na vseh računalnikih, povezanih v isto domeno.

4.2.4 Izboljšave programske opreme

Škodljiva programska koda vse pogosteje napada ranljive računalniške sisteme, ki še nimajo zakrpanih varnostnih lukenj. Varnostne pomankljivosti pa se najpogosteje nahajajo v spletnem brskalniku Internet Explorer ter poštnem odjemalcu Outlook Express.

Za odpravljanje teh pomankljivosti izdaja Microsoft za svoje operacijske sisteme redne posodobitve, ki so na voljo uporabnikom na spletnem portalu http://www.microsoft.com/downloads. Potrebno je le, da jih prenesemo na svoj računalnik in namestimo.

Novejši operacijski sistemi, vključno z Windows XP SP2, imajo možnost samodejnega posodabljanja že vključeno, tako da administratorjem v podjetjih za takšne zadeve skorajda ni več potrebno skrbeti. Vse, kar je potrebno storiti, je le računalnik ponovno zagnati, da se posodobitve uveljavijo.

Med izboljšavami, ki jih je deležen operacijski sistem Microsoft Windows XP s paketom varnostnih popravkov SP2, najdemo tudi nov in izboljšan programski požarni zid. Novost sta tudi programska zaščita Windows Defender in prenovljena različica spletnega brskalnika Internet Explorer 7, ki ju lahko namestimo le na računalnike s pristnim (angl. genuine) operacijskim sistemom.

Na voljo pa je že nova generacija operacijskega sistema, Windows Vista, ki vključuje tehnološke izboljšave, ki so zlasti ključne za Microsoftovo prizadevanje na področju varnosti in zanesljivosti od leta 2007 naprej. Uporabniki sistema Windows

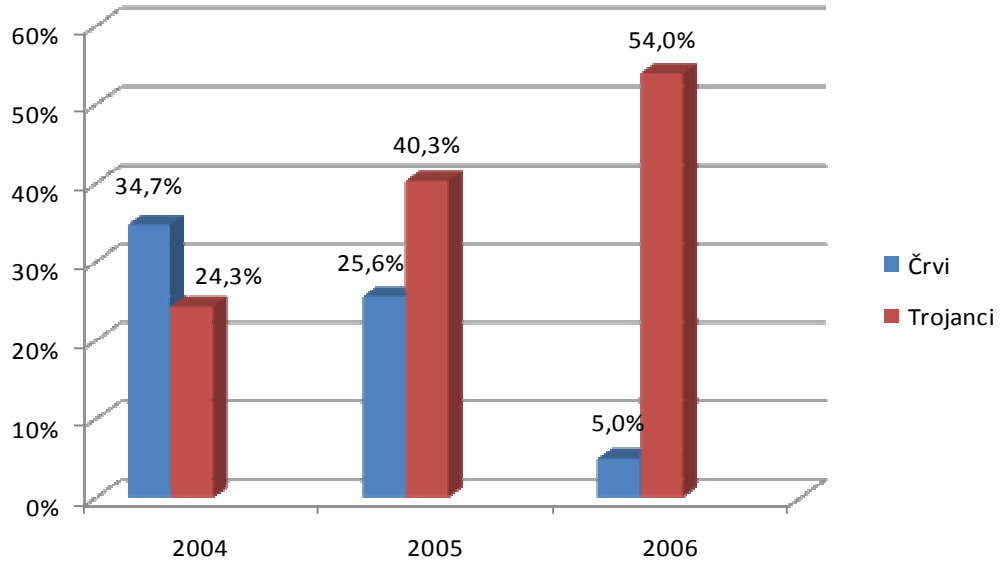
Vista lahko pričakujejo varnostne izboljšave na vseh področjih, od nadzora uporabniškega računa (angl. user account control, UAC), boljše podpore pametnim karticam in izboljšane zaščite s požarnim zidom do izboljšanih zmožnosti za varnost in zasebnost v brskalniku Internet Explorer 7.0 in odjemalcu elektronske pošte Outlook Express. Uporabniki bodo deležni prednosti funkcionalnosti za večjo zaščito informacij, kot sta BitLocker Drive Encryption in Backup and Restore Center. To sta rešitvi, ki odpravljata skrb zaradi izgube podatkov pri poškodovanih ali ukradenih računalnikih (Zaupanja vredno računalništvo v letu 2005, 2007).

Za razliko od prejšnjih različic operacijskih sistemov Windows Vista omogoča tudi nastavitve obnašanja požarnega zidu za vse vrste omrežij. Požarni zid lahko nastavimo po privzetih nastavitvah in na tak način tudi optimalno zaščitimo računalnik pred vdori. Za odhodne podatke nam priporoča dovoljenje razen izjem, ki jih sami določimo. Za dohodne podatke, ki nimajo dovoljenja, nam program priporoča blokado.

Žal še vedno ni operacijskega sistema, ki bi lahko ubranil računalniške sisteme in omrežja pred črvi, trojanci in ostalimi škodljivi programski kodami. Proizvajalec vodilnega operacijskega sistema Windows si z raznimi popravki in posodobitvami prizadeva omiliti nastalo škodo v podjetjih zaradi tovrstnih napadov na računalniška omrežja. Nedvomno pa so različice Linuxa še vedno najvarnejše med odprtokodnimi brezplačnimi sistemi, zato so tudi primerne za večje strežniške sisteme.

4.2.5 Uporaba protivohunskih orodij

Prestrezanje vnosov preko tipkovnice, sledenje in beleženje njihove aktivnosti so v večini primerov povezani z bančnimi prevarami. Finančne koristi prinašajo tudi geselni in vohunski trojanski konji za kraje zaupnih podatkov in njihovo prodajo. Po podatkih, ki jih je zbralo protivirusno podjetje Panda Software, so leta 2004 črvi predstavljali 34,7% škodljive kode (slika 5). Do druge polovice leta 2006 je njihov delež padel na 5%. V primerjavi s črvi se je število trojanskih konjev v istem obdobju več kot podvojilo.



Slika 5: Delež črvov in trojancev v škodljivi kodi v letih 2004 do 2006 (Varnostne rešitve Panda Software, Sporočila za javnost, 2007)

Razlog takšnega porasta trojancev je preprost. Pisci črvov in ostale škodljive kode so poleg dokazovanja znanja in tekmovanja med seboj našli nov motiv finančnega okoriščanja. To so dosegli z ustvarjanjem trojanskih konjev.

Primer, ki ga recimo navaja Microsoft Slovenije, je finančno okoriščanje z izrabo trojanskih konjev. Neko podjetje namreč ocenjuje, da je bila samo leta 2004 zaradi »ribarjenja« gesel (angl. phishing) povzročena neposredna škoda v višini 137 milijonov ameriških dolarjev (Ne ujemite se v mreže ribičev za gesli, 2007).

Večina trojanskih konjev se prenaša s spletno vsebino in shranjuje v začasno mapo brskalnika Internet Explorer. Ker se v sistemu obnašajo kot popolnoma neškodljiva koda, jih protivirusni programi poredko in težko zaznajo, zato je v kombinaciji s protivirusno zaščito že skorajda obvezna uporaba protivohunskih orodij. Kot tako orodje lahko uporabimo Spy Sweeper ali Lavasoft Ad-Aware (Lavasoft, 2007).

Ad-Aware SE Personal je trenutno brezplačni program, ki zazna in uspešno odstrani večino škodljivih datotek in vrednosti iz registrov. Je enostaven, pregleden, predvsem pa učinkovit, zato je tudi primeren za uporabo v manjših podjetjih, še posebej v tistih, ki imajo velik pretok podatkov preko interneta.

4.2.6 Odzivnost protivirusnih ekip

Protivirusni programi danes niso več glavno merilo za uspešno zaznavanje in odstranjevanje škodljive programske kode. Ali bo program škodljivo kodo zaznal ali ne, je odvisno od definicij, ki jih izdaja protivirusna ekipa. Nekateri protivirusni programi se lahko le enkrat do nekajkrat tedensko posodabljajo, medtem ko je odzivnost protivirusnih ekip priznanih blagovnih znamk protivirusnih programov bistveno večja. BitDefender ali ESET NOD32 izdajata definicije vsaj enkrat dnevno, zato je ob njuni uporabi verjetnost okužbe zelo majhna.

Testi, ki jih je opravljala svetovno znana in najprestižnejša organizacija za testiranje protivirusnih programov Virus Bulletin, so pokazali, da je do konca decembra leta 2005, program NOD32 zaznal približno 88% virusov s hevristiko TreatSense (NOD32 in TreatSense tehnologija, 2008). Hevristično preiskovanje je uporaba pametnejših postopkov ali algoritmov pri iskanju škodljive kode. Za primer, vse verzije črvov MyDoom, Netsky, Bagle in Mytob so bile zaznane hevristično, še preden so konkurenčni proizvodi sploh imeli virusno definicijo.

Poleg tega je NOD32 tudi brez virusnih definicij proaktivno zaznal 90% najnovejših (angl. in-the-wild, ITW) virusov in 62% vzorcev vseh škodljivih kod in s tem v povprečju za 95% premagal vso konkurenco. Proaktivna zaznava pomeni odkrivanje in odstranjevanje škodljive kode tudi takrat, ko se ob čakanju na nove posodobitve virusnih definicij ustvari časovna luknja. Tehnologija NOD32 TreatSense pa za razliko od drugih protivirusnih zaščit to luknjo zapre.

Iz tabele 1 lahko razberemo, da je protivirusna zaščita NOD32 še vedno najučinkovitejše sredstvo proti različnim virusnim okužbam, čeprav nima integriranega požarnega zidu, kot ga imajo nekateri drugi zaščitni programi. Po učinkovitosti odkrivanja in odstranjevanja virusne nesnage mu sledita še Symantec Norton in Norman.

Četrti na lestvici je Kaspersky, ki zaostaja z učikovitostjo dobrih 22%. Najmanj učinkovit je protivirusni program AVG, ki bi ga priporočali le za preprosto zaščito domačih računalnikov. Zanimiv podatek je tudi ta, da NOD32 kljub svoji učinkovitosti zahteva le 15 do 22 MB RAM-a, kar je zelo malo v primerjavi z ostalimi protivirusnimi programi. Zato je njegova uporaba možna tudi na spominsko šibkejših računalnikih.

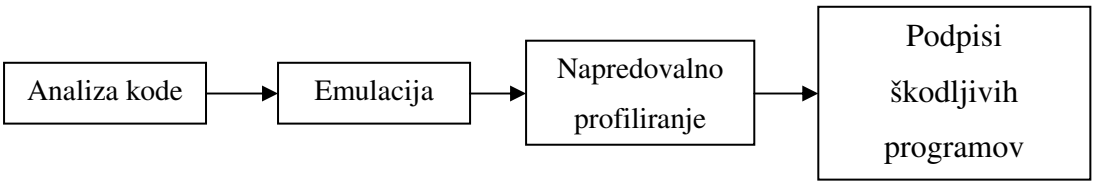
Tabela 1: Primerjava učinkovitosti različnih protivirusnih zaščit (Si lahko privoščite manj kot najboljšo zaščito za svoj računalnik?, 2007)

PROTIVIRUSNI SISTEM	**UČINKOVITOST (%)**
NOD32	92,1%
Symantec Norton	83,3%
Norman	73,8%
Kaspersky	69,7%
eTrust	67,4%
F-Secure	62,5%
McAfee	56,0%
Avast32	45,4%
AVG	32,3%

Hevristika TreatSense, ki jo uporablja ESET NOD32, je nova tehnologija preiskovanja škodljive kode, ki daje protivirusnemu programu vrhunsko zmogljivost zaznavanja virusov, trojanskih konjev, vohunskih programov in raznih tehnik zavajanja uporabnikov ob minimalni porabi sistemskih virov.

Napredno preiskovanje škodljive kode ali TreatSense (slika 6) poganja in analizira kodo programov v varnem okolju, ki se izvajajo znotraj operacijskega sistema brez kakršnekoli potrebe po posodobitvah virusnih definicij. Protivirusna zaščita je lahko aktivna v trenutku napada le, če se izvede analiza programske kode, ki se izvaja v realnem času. Podpisi škodljivih programov, imenovani tudi virusne definicije, pa so tisti, ki zaznajo, ali je program, ki se emulira, škodljiv ali ne.

Takšna tehnologija zaznavanja potencialne škodljive kode prepreči nadaljnjo okužbo sistema tako, da zazna okuženo datoteko in jo dezinficira ali pa zbriše, še preden se dejansko zažene.



Slika 6: Tehnologija naprednega iskanja potencialne škodljive kode

4.2.7 Izobraževanje zaposlenih

Glede na tehnologijo, ki napreduje iz leta v leto, bi morali zaposleni v podjetju imeti ustrezno znanje in izobrazbo. Veliko okužb žal še vedno nastane zaradi pomanjkljivega znanja zaposlenih, brskanja po spletnih straneh s škodljivo vsebino, odpiranjem neznanih priponk v elektronski pošti itd.

Cilji podjetij so med drugim tudi oblikovanje varnostne politike, ki temelji tudi na varnosti računalniških sistemov in omrežij. Pomembno je, da vodstvo podjetja ali administratorji poskrbijo za ustrezno izobraževanje zaposlenih. Razložiti jim morajo uporabo različnih programov, ki jih bodo uporabljali, preventivne ukrepe pred možnimi okužbami, pa tudi ravnanje v situacijah, ko je sistem okužen.

Zadnja leta se vse bolj uveljavlja izobraževanje zaposlenih, ki ga organizirajo in izvajajo nekatera računalniška podjetja. Tečaji, ki jih izvajajo, zajemajo poznavanje in obvladovanje pisarniških orodij, interneta in elektronske pošte. Stopnje zahtevnosti tečajev se razlikujejo po znanju posameznika. Na Primorskem večino takšnih tečajev organizirata podjetji SAOP d.o.o. in SPIN d.o.o. iz Šempetra pri Gorici.

5 PRAKTIČNI PRIMERI ODPRAVLJANJA ŠKODE

V tem poglavju predstavljamo nekaj primerov odstranjevanja škodljive računalniške kode v podjetjih. Opisani so problematika posameznega podjetja, postopki odstranjevanja škodljive kode, reševanje podatkov in ustrezna izbira protivirusne zaščite z oceno stroškov ponovne vzpostavitve delovanja računalniških sistemov. V navajanju primerov bodo imena podjetij ostala anonimna.

5.1 Primer podjetja A

Podjetje A šteje 18 zaposlenih in ima tri proizvodne linije, na katerih izdelujejo polnila za pohištveno industrijo (vzmetnice, blazine, sedežne garniture, ipd.), konfekcijo (odeje, vzglavnike, okrasne blazine, igrače, itd), čevljarsko industrijo, filtracijske materiale in različne izolacije za gradbeno stroko.

5.1.1 Znaki okužbe

Kot večina podjetij, ki so se odločila za najem povezave ADSL brez dodatne protivirusne zaščite, so se kasneje soočili z znanim črvom, imenovanim W32.Opaserv, ki je okužil dva računalnika z operacijskim sistemom Windows 98. Črv ustvari datoteki scrsvr.exe in alevir.pif, ki se pojavita na namizju, shranjeni pa sta v mapi operacijskega sistema Windows. O okužbi s škodljivo kodo smo bili obveščeni kmalu po vzpostavitvi povezave ADSL. Okužbo smo prepoznali po tem, da se je črv poskušal povezati na trenutno nedosegljivo spletno stran (angl. blank page). Ker je imelo podjetje vzdrževalno pogodbo, smo takoj ukrepali in okužbo v kratkem času uspešno odpravili.

5.1.2 Opis črva

Črv W32.Opaserv se zelo hitro širi po računalniškem omrežju, kjer so trdi diski računalnikov dodeljeni v skupno rabo. Ko se na lokalnem računalniku začne razmnoževati, ustvari datoteki scrsvr.exe ter alevir.exe v mapi Windows.

Prav tako ustvari tudi dva zapisa v registru, da ju lahko požene ob vsakem zagonu operacijskega sistema:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ScrSvr
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Alevir

Širi se tako, da išče IP naslove ostalih računalnikov, povezanih v LAN omrežje. Kodo črva prekopira v mapo na ostalih računalnikih in preoblikuje datoteko win.ini tako, da se lahko tudi sam zažene ob vsakem zagonu operacijskega sistema Windows. Ko je enkrat računalniško omrežje okuženo, črv začne enako preiskovati internet tako, da uporabi naključne IP naslove. Njegovo širjenje po računalniškem omrežju lahko preprečimo z nastavitvijo pravic skupne rabe trdih diskov.

Skupna raba particij v operacijskih sistemih namreč omogoča več načinov dodeljevanja podatkov ostalim uporabnikom:

- branje podatkov (angl. read),
- polni dostop (angl. full control).

Pogoj za širjenje črva po lokalnem računalniškem omrežju je polni dostop. Ta administratorska pravica dovoljuje branje in spreminjanje podatkov iz oddaljenih računalniških postaj, ki se povezujejo v lokalno omrežje z isto omrežno skupino.

5.1.3 Postopek odpravljanja škode

Tehnik odstranjevanja takih črvov je več. Ena izmed možnosti, ki smo jo v praksi tudi uporabljali, je opisana na spletni strani protivirusnega programa Symantec. Na tej strani so na voljo razna orodja za njihovo odstranjevanje, ki se imenujejo Removal Tools. Ker se simptomi okužb s škodljivimi kodami med seboj razlikujejo, je potrebno najprej ugotoviti, kateri program je napadel računalniški sistem.

Na podlagi ugotovitev o vrsti zlonamerne kode smo na okužena računalnika namestili diagnostično orodje FixOpaserv. Program je pregledal particije trdih diskov, vključno z zapisi vrednosti v registru, in odstranil najdene okužene datoteke. Prav tako je zbrisal vrednosti zapisov črva iz registrov.

Črv se širi z izkoriščanjem varnostnih lukenj v spletnem brskalniku Internet Explorer 5 ali 5.5, zato smo namestili njegovo novejšo različico, ki je na voljo na Microsoftovi spletni strani.

Naročnikove želje o uporabnosti računalnika in njegovi zmogljivosti so ključni elementi, pomembni za ustrezno izbiro protivirusne zaščite. Na zalogi smo imeli predvsem programsko zaščito podjetja Panda Software, možna pa je bila tudi dobava drugih protivirusnih programov, kot so ESET NOD32, BitDefender in Norton Antivirus.

Na popravljena računalnika smo namestili protivirusni program Panda Titanium. Ta velja za zelo učinkovitega, saj ima vgrajeno tehnologijo TruPrevent, kar pomeni dodatno zaščito pred novimi virusnimi okužbami. Vkolikor zazna okuženo datoteko, jo skuša po privzetih nastavitvah »ozdraviti«, če pa to ne uspe, jo osami v »karanteno«.

Tako preprečimo dodatno širjenje okužb z raznimi črvi in virusi. Poleg tega nam programska zaščita dopušča še veliko možnosti, kot so na primer avtomatsko posodabljanje virusnih definicij, hitro in temeljito preiskovanje operacijskega sistema, požarni zid itd. Vse te funkcije lahko tudi prilagajamo glede na naše potrebe in zmogljivost računalnika.

Ko so bili računalniki popravljeni, smo še preverili delovanje uporabniških poslovnih programov. Ker črv usmerja napade samo na sistemske datoteke, so uporabniški programi ostali neokuženi. Ker operacijski sistem ni bil ponovno nameščen, tudi ni bilo potrebno ponovno vzpostavljati omrežja.

5.1.4 Stroški popravila v podjetju A

Stroške, ki so nastali v podjetju zaradi okužbe, delimo na stroške popravila sistema in padec prihodka od prodaje v času okvare sistema. Stroški popravila računalniškega sistema so prikazani v tabeli 2.

Padec prihodka od prodaje izračunamo po enačbi za izračun prihodka kot produkt med prodajno ceno izdelka in njegovo proizvedeno količino. Ker prikazujemo padec prihodka, moramo upoštevati razliko med proizvedeno količino izdelkov v polnem delovanju sistema in zmanjšano količino izdelkov v času okvare sistema:

$$\Delta Cp = pc * (n_1 - n_2) \qquad (1)$$

kjer so:

- ΔCp padec prihodka od prodaje,
- pc prodajna cena izdelka,
- n_1 proizvedena količina izdelkov v polnem delovanju sistema in
- n_2 proizvedena količina izdelkov v času okvare sistema.

Padec prihodka je bil v tem primeru zanemarljivo majhen, saj sta bila podjetju po vzdrževalni pogodbi dodeljena nadomesta računalnika.

Tabela 2: Stroški popravila v podjetju A

Opis dela	Cena v €	Količina	Enota	Znesek v €
Priključitev nadomestnih računalnikov	12,25	2	kom	25,04
Protivirusni program Panda Titanium	50,07	2	kom	100,14
Popravilo 2 računalnikov	25.03	4	ure	100.12
			Skupaj:	270,36

5.2 Primer podjetja B

Podjetje B je eno večjih podjetij v Sloveniji. Obsega več kot 70 poslovalnic, njihova vizija pa je tudi širitev na Hrvaško. Glede na njihovo velikost smo z njimi mesečno ustvarili največ prometa. V vzdrževalni pogodbi je bila vključena 24-urna asistenca v primeru tehničnih težav z računalniki ali programsko opremo ne glede na to, koliko posegov mesečno je bilo potrebnih.

5.2.1 Znaki okužbe

Prve večje težave s programsko opremo so nastale po povezavi računalnikov s širokopasovnim omrežjem ADSL. Dostopi do spletnih strani s škodljivo vsebino, slaba protivirusna zaščita in neredne posodobitve operacijskega sistema so prispevali k okužbi računalnikov s trdoživima črvoma Sasser in Blaster. Črva sta bila prepoznavna po naključnem ponovnem zagonu sistemov po eni minuti in napaki pri izvajanju programa lsass.exe. Črva, ki sta okužila sistem, sta za nekaj časa popolnoma ohromila delo. Glede na število okuženih računalnikov in obseg poslovanja smo takoj ukrepali.

5.2.2 Opis črvov

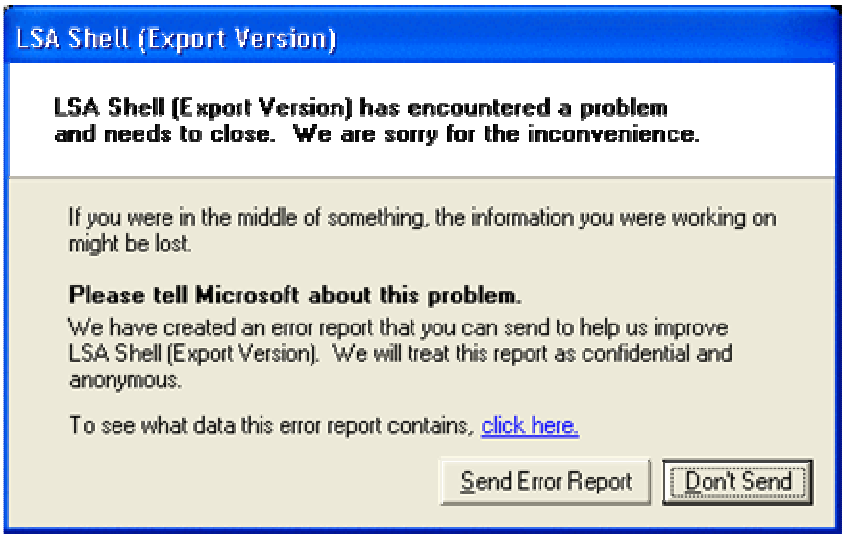
Za različice črva W32.Sasser je značilno, da se pojavljajo v operacijskih sistemih Windows 95, Windows 98 ter Windows ME, vendar jih ne okužijo. Čeprav sistemi niso okuženi, so lahko prenašalci te skupine črvov na računalnike z operacijskim sistemom Windows XP v primerih, ko se ti povezujejo v omrežje.

Črv pregleduje naključne IP naslove, dokler ne najde ranljivih sistemov. Ko jih najde, se prekopira v mapo Windows pod imenom avserve.exe in ustvari zapis v registru, ki mu omogoča samodejen zagon ob zagonu operacijskega sistema:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avserve.exe

Širi se preko TCP vhoda 445, ob okužbi pa namesti FTP strežnik na TCP vhodu 5554 in dostop do ukazne vrstice na TCP vhodu 9996. Ranljivost, ki jo izrablja,

lahko povzroči napako v izvajanju programa lsass.exe (slika 7), zato se pojavi okno z besedilom *LSA Shell (Export Version) has encountered a problem and needs to close* in nato še okno z naslovom *System Shutdown*, ki uporabnika opozarja, da se bo računalnik samodejno ponovno zagnal v roku ene minute.



Slika 7: Napaka pri izvajanju programa LSA Shell (F-Secure Virus Information Descriptions: Sasser, 2007)

Na spletni strani protivirusnega podjetja Symantec je na voljo orodje za odstranjevanje črva FixSasser. Računalnik najprej izključimo iz omrežja. Ravno tako izključimo funkcijo Obnovitev sistema (angl. system restore). Najbolje je, da računalnik poženemo v varnem zagonu in s tem preprečimo ponovni zagon sistema med izvajanjem programa FixSasser. Z urejevalnikom registrov preverimo, ali se zapis črva še vedno nahaja v registru, in ga po potrebni ročno zbrišemo. Ponovno okužbo s tem črvom preprečimo z namestivijo varnostnega popravka KB835732.

Namen črva W32.Blaster je enak kot pri Sasserju. Črv povzroči ponoven zagon računalnika po eni minuti, tako da popolnoma onemogoči delo z računalnikom. Širi se v datoteki dolžine 6176 znakov, imenovani msblast.exe, na računalnike z operacijskim sistemom Windows 2000 ali Windows XP, če nimajo nameščenih najnovejših varnostnih popravkov.

Koda črva vsebuje besedilo: *I just want to say LOVE YOU SAN!! billy gates why do you make this possible? Stop making money and fix your software!!* Črv lahko hitro prepoznamo, saj se nam na zaslonu (slika 8) pojavi okence z vsebino: *Windows must restart because the Remote Procedure Call (RPC) Service terminated unexpectedly*. Po preteku ene minute se računalnik samodejno zažene.

Slika 8: Proces ponovnega zagona zaradi napake prekoračitve pomnilnika (F-Secure Virus Descriptions: Lovsan, 2007)

Zanimiv je tudi način širjenja črva W32.Blaster. Črv 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. Črv najprej prebere IP naslov okuženega računalnika. Zatem se z izbiro naključnega števila med 1 in 20 odloči, ali bo okuževal lokalne ali naključno izbrane računalnike. Če je naključno izbrana številka večja od 11, uporabi lokalno številko. Če je C večji od 20, od številke odšteje 20. D je vedno 0. Če črv izbere naključno številko, se A, B in C tvorijo naključno v območjih:

- A od 1 do 254,
- B od 0 do 253,
- C od 0 do 253,
- D je vedno 0.

Z uporabo teh naslovov črv W32.Blaster prične pregledovati računalnike, zaporedoma v skupinah po 20 računalnikov. Črv se poizkusi povezati na vhod 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 (angl. trivial file transfer protocol) skopira svojo kodo. Zatem se na napadenem računalniku požene.

Računalniki, okuženi s tem črvom, začnejo z izvajanjem DoS (angl. denial of service) napadov na spletno stran s popravki www.windowsupdate.com z namenom, da bi jo začasno onemogočili. Da se črv lahko zažene vsakič ob zagonu računalnika, ustvari naslednji zapis v registru:

HKLM\Software\ Microsoft\ Windows\ CurrentVersion\Run\windows auto update

Postopek odstranjevanja Blasterja je podoben kot pri odstranjevanju Sasserja. Zanj je potrebno uporabiti drugo programsko orodje, to je FixBlast. Pri odstranjevanju tega črva je priporočljivo pognati računalnik v varnem načinu (angl. safe mode). Naloge, ki jih opravi orodje za odstranjevanje črva, so:

- ustavi delovanje procesov, ki jih izvaja črv,
- zbriše okužene datoteke,
- odstrani zapise črva iz registra, ki mu omogočajo ponoven zagon ob zagonu Windows XP.

Ko je črv odstranjen iz registrov in mape Windows, samo namestimo še popravek KB823980.

5.2.3 Postopek odpravljanja škode

Ker sta W32.Sasser in W32.Blaster omrežna črva, je bilo prizadeto celotno računalniško omrežje v podjetju. V tem sklopu je bilo deset delovnih postaj in strežnik, na katerem sta bili shranjeni vsa dokumentacija in podatkovna baza o poslovanju podjetja. Za to podjetje smo imeli posebej pripravljene tri nadomestne računalnike z operacijskim sistemom Windows 98, vendar nam ni uspelo popolnoma

omogočiti nadaljnjega dela, saj je bilo število okuženih računalnikov preveliko. Glede na posledice, ki sta jih povzročila črva, smo se odločili za ponovno namestitev operacijskega sistema na vse računalnike.

Na prenosni trdi disk smo prekopirali vse pomembne podatke iz okuženih računalnikov (elektronsko pošto, mapo HiSoft, ikone na namizju, programe za izdelavo nalepk, deklaracij ipd.). Da je bilo delo čimbolj natančno opravljeno, smo na prenosnem disku za vsak računalnik ustvarili svojo mapo, v katero smo shranili podatke posameznih računalnikov. Pri petih računalnikih z operacijskim sistemom Windows XP smo varnostno kopiranje lahko izvedli le iz varnega zagona, saj smo samo na tak način preprečili ponoven zagon računalnika. Strežnika z operacijskim sistemom Windows 2000 ni bilo potrebno arhivirati, saj so bili vsi podatki shranjeni na drugi particiji trdega diska.

Za vsak računalnik posebej smo morali prepisati še naslednje nastavitve:

- delovna skupina (angl. workgroup): je skupina računalnikov, ki se med seboj povezujejo z namenom, da bi si izmenjevali datoteke, tiskalnike, fakse;

- sistem domenskih imen (angl. domain name system, DNS): je tehnologija, ki spremeni domenski naslov v IP naslov, tako da lahko dostopamo do spletne strani. Če na primer vpišemo v IE brskalnik www.microsoft.com, bo ime prevedeno v IP naslov, ki se ga uporablja za dostop do njihove spletne strani;

- IP naslov (angl. IP address): je okrajšano ime za internet protokol address. Določa posamezen računalnik, ki se povezuje v mrežo ali internet. Lahko je samodejno dodeljen ali pa ga določimo sami;

- omrežni pogon (angl. network drive): je navidezni pogon, do katerega lahko dostopajo ostali uporabniki v lokalnem (angl. LAN) omrežju. Omogoča izmenjevanje podatkov. Pogoj vzpostavitev navideznega pogona je skupna raba particije.

Vse te nastavitve omrežja so določene za skupni dostop do svetovnega spleta prek ADSL modema in usmerjevalnika (angl. router) ter komunikacijo med ostalimi računalniki.

Pri ponovnih namestitvah operacijskih sistemov smo celotni trdi disk razdelili na dve particiji, C in D. Delitev particij prinaša določene prednosti:

- na particiji D so lahko shranjeni dokumenti, instalacijske datoteke in podobno;
- v kolikor je potrebno ponovno namestiti operacijski sistem, ne prenašamo podatkov, saj ostanejo ti ohranjeni na particiji D;
- tudi v primeru ko pride do fizične okvare površine diska (angl. bad sector), lahko podatki ostanejo nekaj časa ohranjeni.

Na vse računalnike smo namestili operacijski sistem Windows XP, orodja skupine Microsoft Office, razne brezplačne programe za pregledovanje pdf dokumentov, Mozillo Firefox, programe prejšnjih namestitev ter vso potrebno protivirusno zaščito vključno s paketoma varnostnih popravkov SP1 in SP2.

Za delovanje programov smo še dodelili skupno rabo particijam delovnih postaj s polnim dostopom, nastavili omrežno skupino, preslikavo omrežnega pogona, IP in DNS naslove ter vzpostaviti prvotno stanje začasno shranjenih podatkov.

Za protivirusni program smo izbrali BitDefender Professional 8, ki ponuja vrhunsko zaščito proti virusom, trojanskim konjem in črvom. Hitra zaznava in odstranjevanje virusov, dnevno osveževanje programa, varovanje zasebnosti in nadzor internetnega prometa postavljajo BitDefender v svetovni vrh protivirusne zaščite.

5.2.4 Stroški popravila v podjetju B

Med neposredne stroške štejemo tudi izpad prihodka v podjetju, ki ga lahko ovrednotimo po enačbi (1) za izračun padca prihodka.

Ob predpostavkah, da je prodajna cena *pc* čevlja v proizvodni liniji moških čevljev 41,7 €, razlika v dnevni proizvedeni količini *Δn* tega izdelka v času okvare sistema pa 7 kosov, znaša padec dnevnega prihodka od prodaje *ΔCp* 291,90 €.

V tabeli 3 je prikazan znesek popravila računalnikov v računalniškem omrežju.

Tabela 3: Stroški popravila v podjetju B

Opis dela	Cena v €	Količina	Enota	Znesek v €
Priključitev nadomestnih računalnikov	12,25	3	kom	37,56
Protivirusni program BitDefender	41,42	11	kom	455,62
Windows XP Pro	208,64	5	kom	1.043,20
Popravilo 11 računalnikov	25,03	22	ur	550,66
			Skupaj:	2.504,45

Ker je bilo delo zaradi vzpostavljanja sistema v prvotno stanje moteno dva delovna dneva, smo stroške izgube ocenili na vrednost 583,80 €. Do tega izračuna smo prišli tako, da smo pomnožili padec dnevnega prihodka s številom neefektivnih delovnih dni v času okvare sistema.

Če osnovnim stroškom popravila računalnikov prištejemo še stroške izgube, znašajo skupni stroški podjetja 3.088,25 €.

5.3 Primer podjetja C

Podjetje C z dejavnostjo proizvodnje industrijskih delovnih stolov in različnih poliuretanskih izdelkov, je bilo ustanovljeno leta 1993. S petnajstimi zaposlenimi spada med manjša podjetja.

5.3.1 Znaki okužbe

Črv, znan kot MyDoom.A, ki je napadel omrežno infrastukturo v podjetju, je le začasno ohromil omrežje, ni pa povzročil večjih težav. Njegov namen je namreč zlomiti računalniško omrežje z izredno hitrim širjenjem po elektronski pošti in izvanjem DoS napadov na spletno stran. Omogoča tudi vdore hekerjev v računalniške sisteme in nepooblaščeno upravljanje računalnikov.

5.3.2 Opis črva

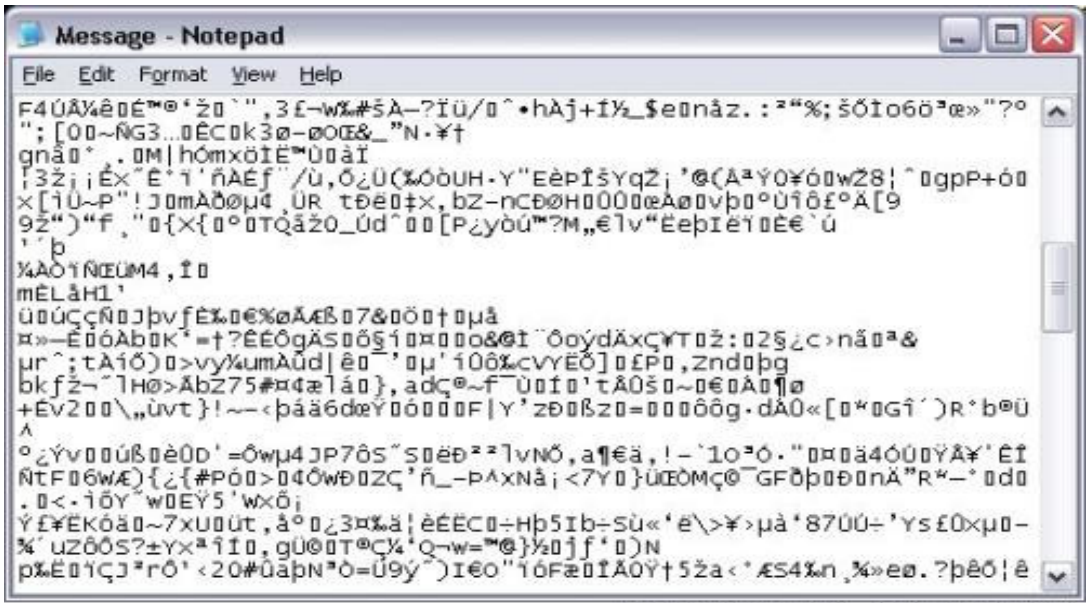
Črv MyDoom.A se širi preko elektronske pošte s sporočilom, ki ima spremenljive značilnosti, opisane v tabeli 4. Prav tako se lahko širi preko P2P programov, kot so KaZaa, eMule, BitTorent itd. Če je sistemski čas 1. februar 2004 ali več, zažene DoS napad na stran www.sco.com. Prav tako presname datoteko shimgapi.dll, ki odpre prva TCP vrata med 3127 in 3198, ki so dostopna. S tem omogoči napadalcu oddaljen dostop do okuženega računalnika. Prepoznamo ga lahko po tem, da ob okužbi odpre beležnico (angl. notepad) in prikaže razmetane podatke (slika 9). Da se kopiji črva Mydoom.A ne zaženeta istočasno, ustvari objekt »mutex« websipcsmtxso. V registre zapiše naslednje vrednosti:

- HKCU\Software\Microsft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

ki omogoča kopiji črva v datoteki taskomon.exe, da se zažene ob vsakem zagonu operacijskega sistema Windows.

Tabela 4: Značilnosti črva MyDoom.A v elektronskem sporočilu (F-Secure, 2007)

MyDoom.A	**Opis**
Zadeva	• Test, Hello, Server Report, Status, Error, Mail Delivery System
Sporočilo	• Mail Transaction Failed. Partial message is available. • The message contains Unicode characters and has been sent as a binary attachment. • The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
Priponka	Končnice priponk so : pif, scr, exe, cmd, bat, zip



Slika 9: Razmetani podatki črva MyDoom.A, izpisani v Beležnici (F-Secure Virus Descriptions: MyDoom, 2007)

Naslednji zapis v registru omogoča brskalniku Internet Explorer, da zažene datoteko shimgapi.dll za odpiranje stranskih vrat 3127 skozi vrata 3198:

HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

Računalnik se okuži ob zagonu datoteke. V kolikor opazimo znake, opisane v tabeli 4, gre po vsej verjetnosti za okužbo s tem črvom. Takrat je najbolje, da zbrišemo vse kontaktne naslove, vključno s prejeto in poslano elektronsko pošto. S posodobljeno protivirusno zaščito pregledamo particije računalnika. Najdene okužene dateteke program samodejno odstrani. Lahko pa tudi uporabimo orodje za odstranjevanju vseh različic tega črva PQREMOVE.

5.3.3 Postopek odpravljanja škode

Največ škode je povzročil črv na računalnikih, ki niso imeli nameščene protivirusne zaščite. Pri ostalih računalnikih z operacijskim sistemom Windows XP in rednimi posodobitvami, ki so že imeli nameščen protivirusni program, je bil uspešno odstranjen. Protivirusni program Sophos ga je prepoznal kot W32/Mydoom-A.

Računalnike je bilo treba najprej izključiti iz omrežja. Okužen računalnik z nameščenim operacijskim sistemom Windows 98 smo zamenjali z Windows XP. Podatke smo arhivirali na zunanji prenosni disk. To so bile ikone na namizju, elektronska pošta, dokumenti, mapa HiSoft z nameščenim trgovinskim programom TDEWIN, podatkovna baza Bank@Net, program eMLK za izvajanje kompenzacij med podjetji, program za pripravo nalepk in etiket NiceLabel. Ker črv lahko okuži le operacijske sisteme, nam arhiviranih podatkov ni bilo potrebno preveriti s protivirusno zaščito.

Po ponovni namestitvi operacijskega sistema uporabniških programov smo namestili še vse varnostne popravke ter protivirusno zaščito Kaspersky. Na okuženi računalnik z operacijskim sistemom Windows XP smo poleg posodobitve z varnostnimi popravki namestili še protivirusni program, ki je črv samodejno odstranil.

5.3.4 Stroški popravila v podjetju C

Popravilo sistema je trajalo skupno tri ure, zato je bil padec prihodka zanemarljiv. Stroški ponovne vzpostavitve sistema v delujoče stanje so prikazani v tabeli 5.

Tabela 5: Stroški popravila v podjetju C

Opis dela	Cena v €	Količina	Enota	Znesek v €
Popravilo dveh računalnikov	25,03	3	ure	75,09
Protivirusni program Kaspersky	58,42	2	kom	116,84
Windows XP Pro	208,64	1	kom	208,64
			Skupaj:	480,68

Poleg osnovnih stroškov popravila sistema, ki so znašali 480,68 €, je podjetje investiralo tudi v izobraževanje treh zaposlenih. Znesek izobraževanja je bil 990 €. Skupni stroški so tako znašali 1.470,68 €.

5.4 Primer podjetja D

Podjetje D proizvaja cisterne polprikolice, prikolice, avtocisterne ter črpalno merilne agregate. Ustanovljeno je bilo leta 1990. Skozi ta leta se je uspelo uveljaviti ne le na domačem trgu, ampak tudi na evropskem, zadnje čase pa se njihov trg še širi, kar tudi pripomore k stalni rasti podjetja.

5.4.1 Znaki okužbe

Prve težave v podjetju so se začele s počasnim delovanjem računalnikov, saj se je ozadju operacijskega sistema izvajalo veliko programov, ki so bili v sklopu oglaševalskega programa Gator, imenovanega tudi Claria. Pri novejših in zmogljivejših računalnikih, ki premorejo veliko procesorske moči in delovnega pomnilnika, je okužba s takšnim sklopom oglaševalskih programov skorajda neopazna, zato prepoznamo okužbo tudi po odpiranju raznih pojavnih oken in spletnih strani.

5.4.2 Opis škodljive kode

Gator ali Claria, ki se je utrdil v računalniku z operacijskim sistemom Windows XP, spada med oglaševalsko programje s kopico plačljivih internetnih oglasov. Vključuje razne programe kot so DashBar, DateManager, PrecisionTime, WeatherScope, WebSecureAlert in eWALLET. V internet se povezuje preko vrat 80, vendar le na spletne strani, ki vsebujejo frazo »gator.com«.

Razmnoževanje se začne z namestitvijo komponent ActiveX kot povsem neškodljivega programa. Da bi uporabnike dodatno prepričal o varnosti svoje namestitve in potrdil zaupanje v korporacijo Gator, prikaže pogovorno okno z digitalnim potrdilom *VeriSign Class 3 Code, Signing 2001-4 CA*. Slika 10 prikazuje obliko digitalnega potrdila o namestitvi Clarie.

Slika 10: Digitalno potrdilo oglaševalskega programa Gator ali Claria (Panda Security, Encyclopedia, 2008)

Zanimiv je tudi način njegovega širjenja. Da bi ga teže odkrili, ustvari svojo zagonsko kopijo v sistemskem imeniku operacijskega sistema Windows z različnimi imeni:

- fsg.exe,
- fsg_3202.exe,
- fsg_3210.exe,
- gain_trickler_3102.exe,
- gain_trickler_3202.exe, ali
- trickler.exe.

Vsakokraten zagon z operacijskim sistemom mu v sistemskem registru omogoča vrednost HKLM\Software\Gator.com.

Drugi zapis v registru pa kaže na sistemski imenik, v katerem je shranjena namestitvena datoteka:

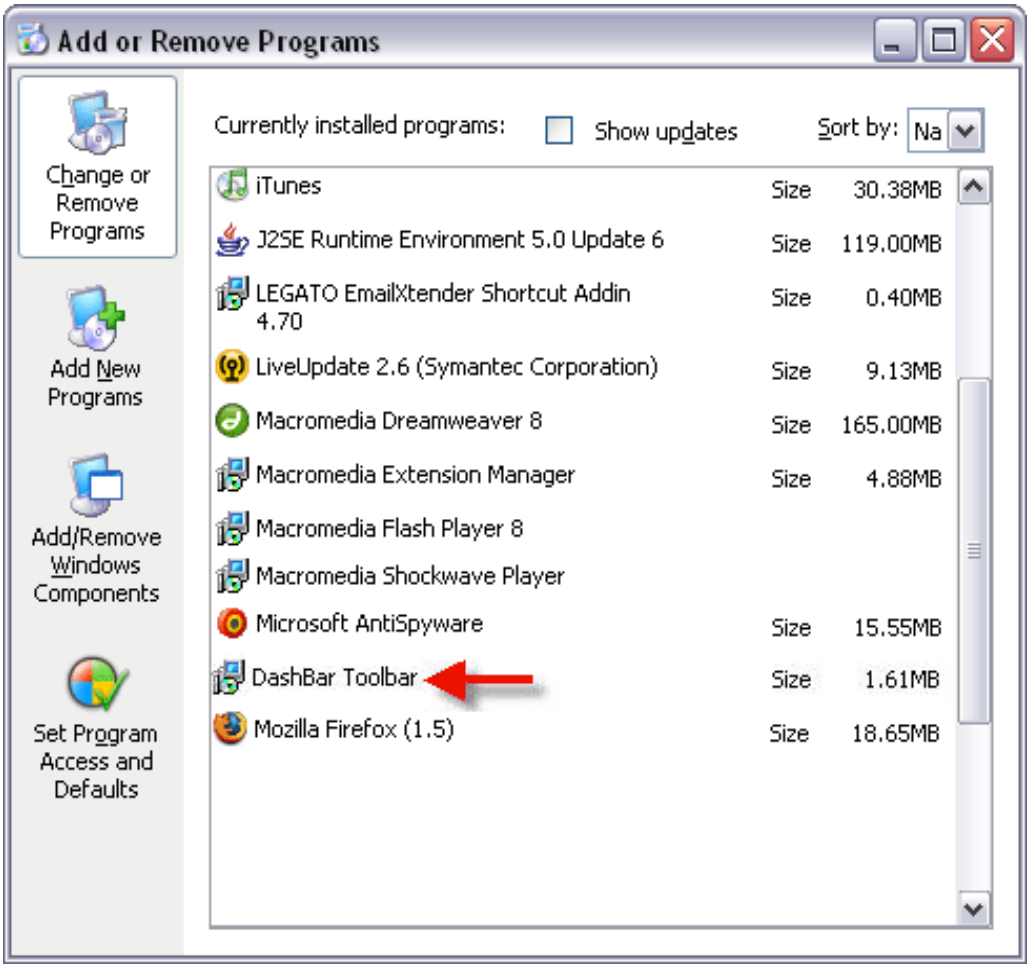
HKLM\Software\Microsoft\Windows\CurrentVersion\Run Trickler= path%\%file%

Ker je Gator ali Claria oglaševalsko programje, obstaja verjetnost, da ga protivirusna zaščita brez modula adware ne bo zaznala. Takrat so potrebne alternativne metode odstranjevanja z uporabo raznih protivohunskih orodij. Oglaševalski program Gator se sicer ne širi preko lokalnega omrežja, lahko pa povzroči uporabnikom s stalnim odpiranjem reklamnih oken kopico nevšečnosti.

5.4.3 Postopek odpravljanja škode

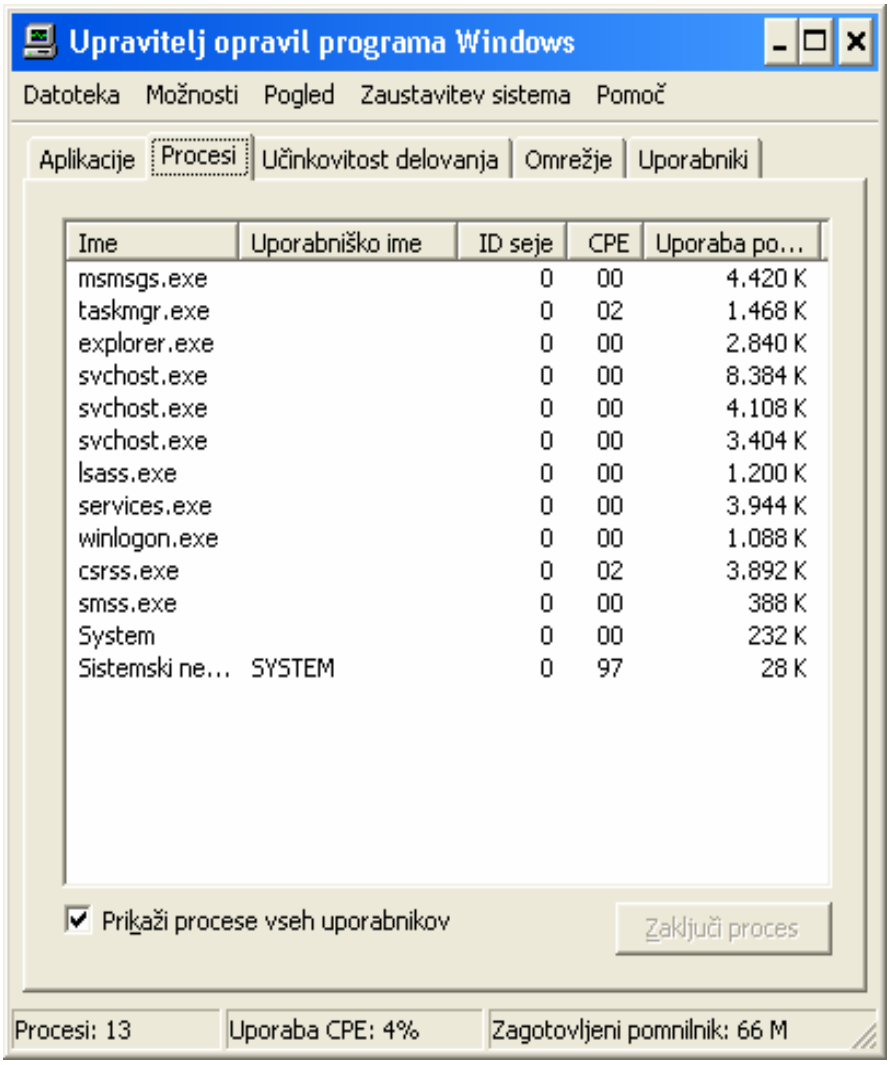
Čeprav podjetje ni utrpelo večje škode, omenjamo primer ravno zaradi raznolikosti zlonamernih kod, s katerimi se vse pogosteje srečujemo, tako poslovni kot domači uporabniki računalnikov.

Aplikacije, ki so delovale v sklopu oglaševalskega programa, smo odstranili s funkcijo za dodajanje in odstranjevanje programov (angl. add or remove programs) v nadzorni plošči (angl. control panel). Postopek odstranjevanja posameznih komponent prikazuje slika 11.



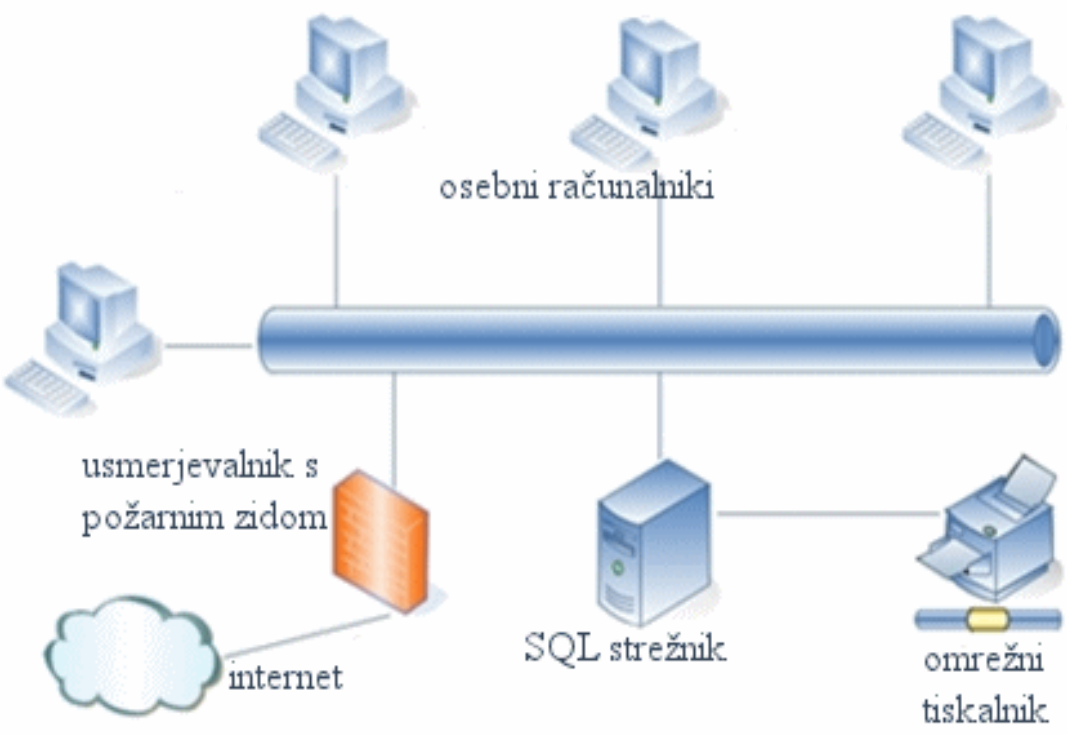
Slika 11: Odstranjevanje aplikacij oglaševalskega programa Gator ali Claria

Izvajanje procesov Gatorja smo onemogočili z zagonom sistema v varnem načinu (slika 12). Tega se v praksi tudi pogosto uporablja za ročno odstranjevanje trdovratnih škodljivih kod, ki si z zapisi v registre omogočajo, da se lahko zaženejo vsakič ob zagonu računalnika.



Slika 12: Procesi v varnem zagonu WindowsXP

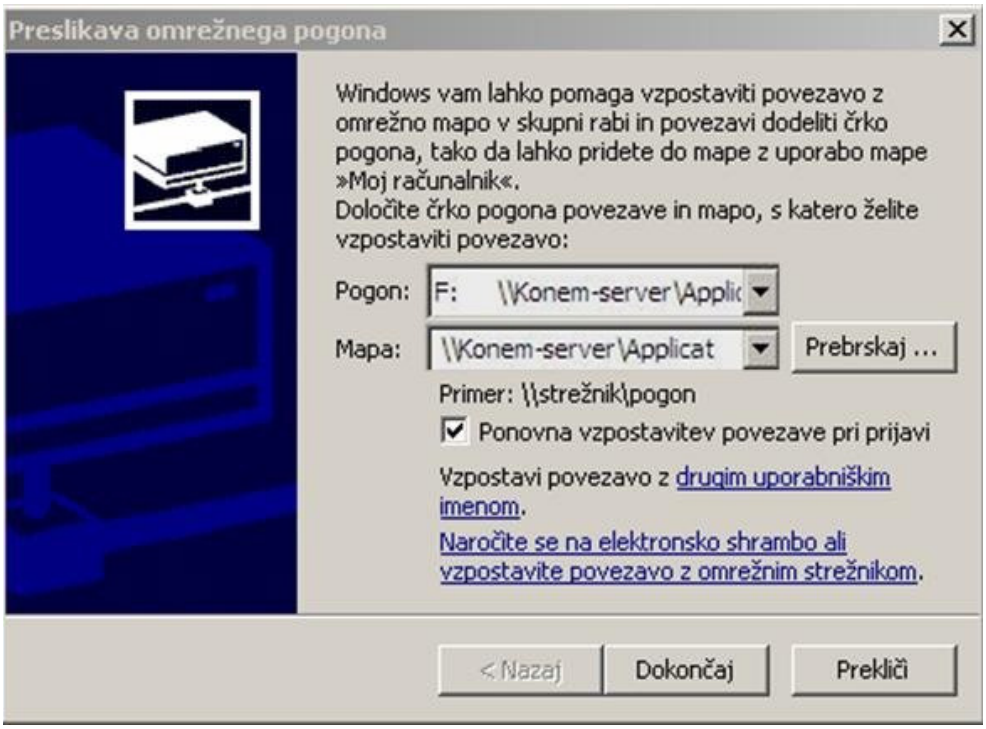
V računalniško omrežje v podjetju so povezane 4 delovne postaje z operacijskim sistemom Windows XP Home Edition ter strežnik SQL Server 2000. Vsak računalnik v omrežju ima dodeljen IP naslov, masko podomrežja ter privzeti prehod, ki je dejansko IP naslov ADSL usmerjevalnika. Dodatno sta vnesena tudi DNS naslova ponudnika internetnih storitev SiOL. Shemo omrežja prikazuje slika 13.



Slika 13: Shema računalniškega omrežja v podjetju D

Ko smo računalnik popravili, smo morali ponovno vzpostaviti programe HiSoft v delujoče stanje. Večina teh programov je prilagojenih na omrežno različico. To pomeni, da se programi izvajajo lokalno na delovnih postajah, podatkovna baza pa je skupna, shranjena na podatkovnem strežniku.

Če želimo ustvariti takšno različico programa, moramo najprej vsem računalnikom v omrežju dodeliti enako delovno skupino ali domeno. Particija na podatkovnem strežniku, kjer bo podatkovna baza shranjena, mora biti v skupni rabi s polnim dostopom za branje in shranjevanje podatkov. V omreženih nastavitvah (angl. my network places) vzpostavimo še povezavo z omrežnim pogonom (angl. map network drive), kjer se podatkovna baza nahaja. Vzpostavitev povezave z omrežnim pogonom prikazuje slika 14.



Slika 14: Preslikava omrežnega pogona za podatkovno bazo HiSoft

5.4.4 Stroški popravila v podjetju D

Claria ali Gator spada med vohunsko programsko opremo, ki za svoje širjenje izkorišča tehnike zavajanja uporabnikov s prepričevanjem o varni vsebini. Na računalniku za uporabnika ne kaže znakov okužb, zato ga je tudi težko prepoznati brez protivirusne zaščite ali protivohunskih orodij.

Delo je bilo zaradi popravil le delno moteno, zato je bil padec prihodka od prodaje po enačbi (1) zanemarljiv. Skupni stroški popravila v podjetju so znašali 365,51 €. Prikazani so v tabeli 6.

Tabela 6: Stroški popravila v podjetju D

Opis dela	Cena v €	Količina	Enota	Znesek v €
Popravilo računalnika	25,03	3	ure	75,09
Protivirusni program Eset NOD32	45,90	5	kom	229,50
			Skupaj:	365,51

6 ZAKLJUČEK

V diplomskem delu smo predstavili pojav zlonamernih računalniških programov in jih poskušali čimbolj pregledno razvrstiti po kategorijah, čeprav to ni enostavno. Težava je že v njihovem poimenovanju, ki je posledica zgodovinskega razvoja. Marsikateri avtor postane nedosleden in viruse, ki so le ena kategorija zlonamernih programov, povzdigne na prvo mesto. Virus postane skupen izraz za vse tipe zlonamernih programov. Poleg tega pa vse več zlonamernih programov vsebuje več značilnosti, zaradi katerih jih lahko uvrščamo v različne kategorije.

V veliki meri smo se posvetili celoviti zaščiti računalniških omrežij pred zlonamernimi kodami. Sledenje zaposlenih navodilom, ustrezna izbira protivirusne programske opreme ter redne posodobitve operacijskega sistema omogočajo visoko stopnjo zaščite. A kljub temu pogosto sledi razočaranje. Žal popolne zaščite še vedno ni in jo je tudi nemogoče vzpostaviti. Vedno se tudi v najpopolnejši obrambi skrivajo pomankljivosti, ki so lahko posledica različnih dejavnikov. Največkrat je to naivnost ali malomarnost uporabnikov, ki lahko ogrozijo še tako dobro zaščiten sistem.

Operacijski sistem, ki je nedvomno še vedno najmanj ogrožen, je Linux. Razlog za to je preprost. Pisci zlonamernih kod se finančno okoriščajo z napadi na že dolgoobstoječe, a še vedno ranljive operacijske sisteme Microsoft Windows, katerih tržni delež je svetovnem merilu še vedno največji.

Čeprav je Linux odprtokodni brezplačni operacijski sistem, ga zaenkrat še redko zasledimo. Primeren je predvsem za spletne strežnike, lahko pa ga uporabimo tudi kot podatkovni strežnik v podjetju. Vsekakor pa uporabo Linuxa na delovnih postajah v podjetjih zaradi nezdružljivosti s poslovodskimi, bančnimi in drugimi programi zaenkrat še odsvetujemo.

Pri implementaciji zaščite računalniških sistemov smo za poizkus namestili dva različna protivirusna programa, BitDefender Professional in Panda Titanium, vendar so se pojavile težave glede združljivosti programov, zato se ta možnost ni uveljavila. Predvsem so bile težave v združljivosti protivirusnih zaščit v kombinaciji s protivirusno zaščito proizvajalca Panda Labs.

Vsekakor pa je poleg protivirusne zaščite priporočljiva tudi uporaba požarnega zidu, ki je lahko komponenta operacijskega sistema Windows, ali pa protivirusne programske opreme znanih proizvajalcev kot sta ZoneAlarm Pro in Kerio Personal Firewall.

Po opravljenih testih z različnimi protivirusnimi zaščitami ugotavljamo, da je ESET Nod32 zelo učintovit obrambni sistem, ki zazna večino škodljivih kod ob minimalni porabi sistemskih virov. Temu sledijo še BitDefender, Kaspersky, Panda Antivirus in Norman, vendar je njihova obremenitev sistema bistveno večja.

V praktičnem delu diplomske naloge smo predstavili nekaj konkretnih primerov odpravljanja škode zaradi škodljivih programov v podjetjih. Vse primere odpravljanja škode smo tudi stroškovno ovrednotili. Obravnavani primeri se medseboj razlikujejo po velikosti podjetja, vrsti okužbe in stroških vzpostavitve sistema v prvotno stanje, kajti le tako lahko predstavimo raznolikost problema okužb računalnikov v poslovnem svetu, s katerim se lahko sreča vsako podjetje.

Glede na pridobljene izkušnje priporočamo izobraževanje zaposlenih, predvsem pa odgovornost na delovnem mestu. Veliko servisiranih računalnikov je bilo namreč okuženih zgolj iz radovednosti zaposlenih in brskanja po spletnih straneh, ki vsebujejo razne reklamne oglase in škodljivo kodo, skrito v opisih spletnih strani.

Predvidevamo, da se bo delež okužb računalniških sistemov s škodljivo kodo v prihodnosti še povečal, saj je danes v svetu računalništva in informatike, ki se neizmerno hitro razvija, težko slediti razvoju različne škodljive kode. Njeni pisci si namreč prizadevajo čimbolj izpopolniti te programe in to do te mere, da bi navzven delovali kot popolnoma neškodljivi. Vendar je njihov namen čisto drugačen. Programi so namreč razviti za krajo raznih informacij uporabnikov interneta, ki bi ustvarjalcem programa lahko prinašale finančne koristi.

Razvijalci kakovostne protivirusne zaščite se sicer trudijo redno izdajati protivirusne definicije, vendar še vedno obstaja možnost okužbe računalnikov. Še vedno je namreč veliko število trojanskih konjev in črvov, ki jih protivirusna zaščita ne zazna. Odlična kombinacija s protivirusno zaščito je programsko orodje Lavasoft Ad-Aware, ki zazna večino še neodkrite kode (Lavasoft, 2007).

Izboljšave, ki jih prinaša operacijski sistem Windows Vista, temeljijo na večji varnosti podatkov. Popolnoma prenovljen je spletni brskalnik Internet Explorer 7, ki za razliko od prejšnjih različic preverja spletno vsebino in ugotavlja, če vsebuje načine zavajanja, namenjene pridobivanju tuje identitete. Druga izboljšava, ki jo prinaša novi operacijski sistem, je tudi poštni odjemalec Outlook Express. Ta filtrira neželeno elektronsko pošto (angl. spam) in elektronsko pošto, ki vsebuje priponke z neznanimi končnicami.

Z gospodarskega vidika so zlonamerni programi velika digitalna nevarnost, ki lahko ogrozi podjetje, po drugi strani pa spodbujajo pomemben segment računalniškega trga, saj se za obrambo proti njim kupuje strojna in programska oprema, od katere živijo proizvajalci.

7 LITERATURA

Bratuša, T. (2006). Hekerski vdori in zaščita. Ljubljana: Pasadena.

CoolWeebSearch. Pridobljeno 19.09.2008 s svetovnega spleta: http://en.wikipedia.org/wiki/CoolWebSearch

F-Secure. Pridobljeno 20.03.2007 s svetovnega spleta: http://www.f-secure.com

F-Secure Virus Descriptions: Lovsan. Pridobljeno 20.03.2007 s svetovnega spleta: http://www.f-secure.com/v-descs/msblast.shtml

F-Secure Virus Descriptions: Mydoom. Pridobljeno 20.03.2007 s svetovnega spleta: http://www.f-secure.com/v-descs/novarg.shtml

F-Secure Virus Descriptions: Sasser. Pridobljeno 20.03.2007 s svetovnega spleta: http://www.f-secure.com/v-descs/sasser.shtml

ISO/OSI referenčni model. Pridobljeno 19.09.2008 s svetovnega spleta: http://sl.wikipedia.org/wiki/ISO/OSI_referen%C4%8Dni_model

Lavasoft. Pridobljeno 01.01.2007 s svetovnega spleta: http://www.lavasoft.si/

Mozilla Firefox – bodi med rekorderji! Pridobljeno 19.09.2008 s svetovnega spleta: http://zelenik.net/2008/05/mozilla-firefox-bodi-med-rekorderji/

Ne ujemite se v mreže ribičev za gesli. Pridobljeno 01.03.2007 s svetovnega spleta: http://www.microsoft.com/slovenija/malapodjetja/issues/sgcv2/security-guidance-centre/dont-get-hooked-by-phishing.mspx

NOD32 in TreatSense tehnologija. Pridobljeno 19.09.2008 s svetovnega spleta: http://www.g-server.com/?stran=novice&novica=201&headline=NOD32+in+ThreatSense%AE+tehnologija

Panda GateDefender Performa. Pridobljeno 15.03.2008 s svetovnega spleta: http://www.panda.anti-virus.si/index.cgi?k=202

Panda Security, Encyclopedia. Pridobljeno 01.04.2008 s svetovnega spleta: http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?idvirus=40681

Patentirana tehnologija Norman Sandbox. Pridobljeno 19.09.2008 s svetovnega spleta: http://www.antispyware.si/default.asp?mID=sl&pID=SandBox

Rubikon, Več o virusih. Pridobljeno 01.01.2007 s svetovnega spleta: http://www.rubikon.si/virusi.htm

Sasser okužil milijone računalnikov. Pridobljeno 19.09.2008 s svetovnega spleta: http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=9&c_id=33380

Si lahko privoščite manj kot najboljšo zaščito za svoj računalnik? (2007). Ljubljana: SISPLET.

So nelegalnim Windowsom šteti dnevi? Pridobljeno 01.01.2007 s svetovnega spleta: http://www.itnovice.si/programje/So-nelegalnim-Windowsom-teti-dnevi/

Spyware – vohunska programska oprema. Pridobljeno 01.01.2007 s svetovnega spleta: http://e-izdaja.comtron.si/Izdaja3/Spyware.htm

Tittel, E. (2003). PC Magazine Fighting Spyware, Viruses, and Malware. Ljubljana: Pasadena.

Varnostne rešitve Panda Software, Sporočila za javnost. Pridobljeno 15.01.2007 s svetovnega spleta: http://www.ribera.si/Default.asp?Page=42

Zaupanja vredno računalništvo v letu 2005. Pridobljeno 10.03.2007 s svetovnega spleta: http://www.si21.com/news.php?id=48665