Tallinna Ülikool
Matemaatika-loodusteaduskond
Informaatika osakond

Ründetarkvara, tööpõhimõtted ja võimalikud kahjud

Seminaritöö

Hannes Raid

Juhendaja: Kalle Tabur-Jõgi

Tallinn 2007

Sisukord

1.Sissejuhatus....3
Teema valiku põhjendus....4
Töö eesmärgid....4
2.Rünnak....6
Kes on rünnakute taga....6
Turvaauk....7
Rünnakute põhjused....7
3.Ründetarkvara....9
4.Parasiittarkvara....10
Loogikapomm (logical bomb)....10
Trooja hobune (Trojan horse)....11
Uss (worm)....14
Viirus (virus)....17
Arvutiviiruste liigitus....17
Makroviirus (macro virus)....18
Pipett (dropper)....21
5.Kuidas ennetada rünnakuid?....22
6.Kokkuvõte....24
7.Kasutatud kirjandus....25

1. Sissejuhatus

Pidev areng arvutimaailmas ning üha suurem inimkonna arvutikasutus nõuab ka andmeturbe vallas tegutsevate inimeste pidevat teadmiste uuendamist ja eneseharimist. Andmeturbe spetsialistid peavad pidevalt olema virtuaalmaailma kurikaeltest sammu võrra eespool. Uue tarkvara turule jõudmine võib tõenäoliselt endaga kaasa tuua uusi turvaauke, mida on võimelised tundma õppima ja hiljem neid enda huvides ära kasutama kõikvõimalikud tehnokratid. Tänapäeval ei ole ainukeseks ohuks häkkerid, kes eksperimenteerimise korras rünnakuid teevad ja sellega kahju võivad tekitada. Levinud on asutuste vahelised andmete vargused ja konkurentide töö rivist välja löömine, kasutades spetsiaalset ründetarkvara. Neile lisandub veel asutuste sisesed sabotaaž-rünnakud ja kasutaja rumalusega seotud infolekked ning -kaod. Kui mõned aastad tagasi pidi ründetarkvara kasutamiseks päris korralikult vaeva nägema, kas siis ise valmis kirjutades või tellides mõnelt programmeerijalt, siis tänapäeval on see palju lihtsam. Internet kubiseb kõikvõimalikest arvutikuritegudeks mõeldud tarkvaraosadest ja terviklahendustest. Lisaks on veel palju foorumeid ülevaadete ja õpetustega, kuidas saaks tavaline võhik rünnaku sooritamisega üksi hakkama. Tuleb vaid mõnda aega lugemise ja katsetamise kallal vaeva näha ning nõrgemaid lülisid olekski juba võimalik kahjustada. Ükski programm ei saa olla täiesti turvaline. Alati on olemas mingisugune nõrkus. Ründetarkvara on reeglina kirjutatud sellisel viisil, et see oleks võimeline kasutama programmide ja süsteemide turvaauke ehk nende nõrkusi. Süsteemi turvaaukude rohkus määrabki suures osas ära selle süsteemi turvariski suuruse. Turvaaukude lappimiseks tehakse pidevat koostööd häkkeritega, kes üritavad selliseid nõrkusi avastada ja siis vastavalt ise kirjutatud programmidega neid rünnates aukude turvariski suurust hinnata. .

Ajast, kui hakkasid välja kujunema inimesed, kelle huviks olid arvutisüsteemid ning nende ründamine, on nad üritanud välja arendada tehnoloogiaid ja võimalusi, mis aitaks neil tungida süsteemi vältides peasissepääsusid. Selleks loodigi programm, mis tekitaks rünnatavasse süsteemi tagaukse. Tagaukseks nimetatakse ründaja poolt tekitatavat turvaauku, mida mööda on tal alati võimalus süsteemi tungida ilma suuremate raskusteta ja seal vastavalt oma volile käituda. Tagauks peaks võimaldama sissetungijal segamatult tegutseda hoolimata administraatori püüdlustest süsteemi turvalisemaks muuta. Iga kurikaela soov ongi just tegutseda rahulikult, segamata ja jälgi jätmata nõnda. Tänu eelnevalt süsteemi paigaldatud tagauksele ei pea nad aega raiskama süsteemi uurimisele ja selle nõrkuste uuesti välja selgitamisele, vaid saavad rahulikult hakata tegutsema juba olemas olevat ust kasutades.

Ründetarkvara pidev arendamine ja ründemeetodite uuenemine võimaldab häkkeritel iga

aastaga tekitada järjest suuremaid infovaralisi kahjusid, kui ei teadvustata endile sellise tarkvara tööpõhimõtteid ja sellega seonduvaid ohte. Infosüsteemide edukaks kaitseks tuleb kõigepealt selgesti mõista turvalisuse olemust, ründetarkvara suutlikkust ja toimemehhanisme. Vaid seda mõistes on meil võimalik jõuda sammuke lähemale turvalisuse tagamisele, sest oleme enesele selgeks teinud võimalikud ohuallikad.

Teema valiku põhjendus

Olles töötanud juba mõned aastad IT-spetsialistina ja kokku puutunud paljude infoturbe alaste probleemidega, märkasin, et ei ole loodud eesti keelset, lihtsat ja kõigile kättesaadavat materjali meie varjatud igapäevaohust - ründetarkvarast. Tundes ise antud valdkonna kohta suuremat huvi, arenes välja soov koostada ründetarkvara tutvustav materjal IT valdkonnas töötavatele inimestele, kelle igapäevatööks on tavakasutajate poolt tekitatud probleemide operatiivne lahendamine ja arvutivõrgu administreerimine(nt. IT-tugiisikud ja algajad süsteemi administraatorid). Materjal sobib ka lugemiseks kõikidele teemast huvitatuile, sest on kirjutatud kõigi jaoks võimalikult arusaadavana.

Lõppkasutaja turvateadlikkus on kriitilise tähtsusega, sest just tema on lihtsamini haavatavamaid lülisid.

Töö eesmärgid

Selle töö kirjutamise käigus plaanin uurida, kuidas on arenenud välja selline tarkvara liik nagu ründetarkvara:

- kes on selle tarkvara loomise taga
- miks ja kuidas tekkis idee hakata programmeerima sellist „pahavara“
- millele hakati tähelepanu pöörama esimesi programme kirjutades
- kuidas on arenenud tänapäevaks ründetarkvara toimemehhanismid

Uurin kuidas rünnakuid tehakse:

- milliseid programme kasutatakse
- mis nendega teha saab
- millised on nende võimalikud tekitatud kahjud

Selle töö üldine eesmärk on uurida ja anda ülevaade arvutirünnakuteks kasutatavast tarkvarast, kui laiad on nende võimalused ja mida tuleks silmas pidada kui soovitakse end nende rünnakute eest kaitsta. Autor võtab aluseks tavalise arvutikasutaja vaatenurga ja üritab seda edasi anda viisil, kuidas tema sellest aru on saanud ja püüab anda soovitusi nõrkade kohtade leidmiseks arvutisüsteemis. Samuti püüab autor testida ka mõningaid programme, et veenduda ründetarkvara kasutamisest reaalsuses. Töö käigus ei ohustata ühtegi avalikku ega privaatset arvutisüsteemi. Kõik uuringud sooritatakse enda loodud sisevõrgus.

2. Rünnak

Rünnakuks (infotehnoloogia valdkonnas) võime pidada ükskõik mistahes ettekavatsetud, sihipärast tungimist arvutisüsteemi, mingi kuritahtliku toimingu teostamiseks, kasutades selleks kõiki kättesaadavaid vahendeid.

Ründeid võime jaotada järgnevalt:

- füüsilised ründed
- ressursside väärkasutus
- ressursside blokeerimine
- infopüük
- võltsing
- süsteemi manipuleerimine
- ründed turvamehhanismidele
- ründetarkvara

Kes on rünnakute taga

Me kõik oleme kuulnud häkkeritest (*hacker*) ja paljud meist arvame, et oleme pidanud kannatama just nende rünnakute tagajärgede all.. Aga kes need häkkerid sellised on ja miks on oluline, et me neist ja nende tegutsemisest teadlikud peame olema?

Traditsiooniliselt on häkker keegi, kellele meeldib tegeleda tarkvaraliste või elektrooniliste süsteemidega. Häkkerid naudivad arvutisüsteemide funktsioneerimise ja olemuse uurimist ning selle tundma õppimist. Aja jooksul on aga termin häkker omistanud tava kodaniku jaoks uue tähenduse – keegi, kes pahatahtlikult murrab süsteemidesse sisse isikliku kasu saavutamiseks. Teisiti nimetades on need kriminaalid kräkkerid (*crackers – criminal hackers*) või ka *blackhat hackers*. Kräkkerid murravad süsteemidesse sisse halbade kavatsustega. Reeglina teevad nad seda kasusaamise eesmärgil, kuulsuse saavutamiseks või lihtsalt kellelegi kättemaksuks. Sellise käitumisega võivad nad korraldada tohutuid kaoseid varastades, muutes või kustutades andmeid, mille hind ei pruugi enam rahas mõõdetav olla.

Selliseid rünnakuid valmistatakse vahele jäämise riski vähendamiseks ette mõnikord lausa kuid. Alustatakse täiesti tavalise ja pealtnäha lihtsa info hankimisega nagu nimed, aadressid, telefoninumbrid, internetiteenuse pakkujad, kuni tavaliste töötajate isikuandmeteni välja ning seda tehakse tavaliselt läbi ohvri asutusesiseseid infoallikaid kasutades. Rünnaku ettevalmistamise lõpp-

faasis kogutakse kokku vajalik ründetarkvara, seda vastavalt vajadustele ümber programmeerides ja kohandades. Räägitakse, et ründe efektiivsus sõltub peamiselt ründetarkvara erinevatest võimalustest ja selles sisalduvatest komponentidest. Tänapäeval on internetis kättesaadaval ohtralt erinevaid ründetarkvara komplekte ja ka lihtsalt uuendustena mõeldud programmilõike, mida kõike saab ära kasutada piisavalt suure hävingu tekitamiseks.

Turvaauk

Rääkides infoturbest ja ründetarkvarast ei saa me mööda minna sõnast turvaauk ehk nõrkus (*vulnerability*). Kui nõuda lühivastust küsimusele, mis on turvaauk, siis oleks õige vastus: „Turvaauk võib olla mis iganes.“ Peamiselt kõike, mida saab kasutada masina ohustamiseks, võib käsitleda kui turvaauku. Ohustamine võib endaga kaasa tuua järgmist:

- Juurdepääsu saavutamine
- Lihtsustatud juurdepääsu saavutmine
- Arvutisüsteemi kokkukukutamine
- Väärtusliku informatsiooni väärtusetuks muutmine

Näiteks firma prügi läbi otsimine väärtusliku info leidmise eesmärgil. Ka täiesti tavalist prügikasti võime võtta arvesse kui suurt ohuallikat ja turvaauku. Kui ründaja otsib läbi asutuse prügikasti ja avastab sealt kellegi poolt välja prinditud salajased dokumendid firma uute toodete kohta, mis lohakuse tõttu on sattunud prügikasti, siis võib ta sellega ohtu seada firma tegevuse ilma, et ta oleks üldse midagi seadusevastast teinud.

On esinenud juhtumeid, kui asutuse infosüsteeme on mingit turvaauku kasutades rünnatud, siis suunatakse millegi pärast liiga suurel määral energiat ja raha just selle augu lappimiseks. Teised turvaaugud jäävad aga lahti ja nende kõrvaldamiseks ei pruugi enam vahendeid leiduda. Rünnak ühele turvaaugule võib olla pelgalt suitsukate palju hullema rünnaku sooritamiseks. Üks sellistest võimalustest juhtida suurematest aukudest tähelepanu kõrvale on lihtlabane võrgu skanneerimine, mis koondab piisaval määral IT-spetsialistide tähelepanu tegelikust ründest eemale.

Rünnakute põhjused

Teadagi varitseb meid kõikjal oht sattuda erinevate rünnakute alla. Lähtudes põhjuslikkuse teooriast võime väita seda, et kui on toimunud rünnak, siis peab olema ka selle põhjus.

Vaadeldes arvutiründeid pinnapealselt võidakse esmapilgul arvata, et tegemist on

mingisuguste pahade häkkerite kavatsusega lihtsalt kellelegi halba teha. Selline väide on aga liialt üldistav ja kitsarinnaline. Laias laastus võib öelda, et rünnakute põhjusteks võib olla uudishimu, kuritahtlikkus, isiklik kasu või teaduslik uurimine. Eelneva loetelu põhjal võib öelda, et rünnakutel on nii head kui halvad kavatsused.

Nõndanimetatud "heatahtliku rünnaku" ajendiks on tavaliselt püüe panna proovile mingisuguse arvutisüsteemi või programmi turbeomadused ning avastada selle nõrku külgi ennetamaks võimalikke kahjusid. Selliste rünnete taga on kõrgelt haritud arvutiturbe valdkonnas tegutsevad eksperdid. Need ründed on ette planeeritud ja hoolikalt läbi mõeldud, arvestades kõiki eetilise häkkimise kriteeriumeid. Vajadus eelnimetatud rünnakute jaoks on eelkõige tarkvaraarendus firmadel, kes soovivad pidada oma tooteid ajakohaste ja turvalistena, et hoida ära võimalikke rikkeid programmide töös ja ennetada ilmnevate nõrkuste ärakasutamisi. Mitte ainult spetsialistid ja palgalised turbeeksperdid ei teosta sellist laadi rünnakuid vaid ka tavalised, arvutivõrkude turbest huvitatud olevad kasutajad, kes panevad proovile oma oskusi rünnates süsteeme, kuid neid mitte kahjustades. Seda võib nimetada pigem süsteemi testimiseks või auditeerimiseks kui sooviks süsteemi kahjustada.

Halvaloomuliste rünnete tagamaid võib otsida juba ründaja kuritahtlikkusest, majanduslikust kasust või siis püüdlustest saavutada autoriteetsust. Siia alla käivad sabotaaž, luure, informatsiooni vargused konkureerivast asutusest ja huligaansus.

3. Ründetarkvara

Tarkvara kõikvõimalike rünnete sooritamiseks jaguneb laias laastus kolmeks:

- legaalsed tüüptooted oma dokumenteeritud omadustega: nende hulka kuuluvad eeskätt operatsioonisüsteemide faili- ja kettafunktsioonid ning paljud faili-, ketta-, diagnostika-, häälestus- jm. utiliidid, mis volitamatul kasutamisel on äärmiselt ohtlikud, kuna võimaldavad läbi murda mitmetest lihtsamatest turvamehhanismidest.
- parasiittarkvara (seal hulgas viirused)
- turvamehhanismide ründeprogrammid: Sellesse rühma kuuluvad programmid, mis on spetsiaalselt määratud paroolide püüdeks, šifreeritud andmete dekrüpteerimiseks jne. Juba ainuüksi häkkeritoodetena on neid ühel paljudest "põrandaalustest" teatetahvlitest loendatud üle saja. Sageli on nad varustatud iseloomulike nimedega - *Thief* ("varas"), *Cracker* ("lahtimurdja") jms.

Neist enamlevinud parasiittarkvara jaguneb veel omakorda alaliikideks:

- loogikapomm (*logical bomb*)
- trooja hobune (*trojan horse*)
- uss (*worm*)
- viirus (*virus*)
- makroviirus (*macro virus*)
- hüpermeediumi aktiivsisu
- pipett (*dropper*): programm, mis installeerib viiruse või trooja hobuse.

Arvestades, et siiski kasutatakse rünnete sooritamiseks peamiselt parasiittarkvara, siis tookski täiendava ülevaate tänapäeval arvutisüsteeme ohustavatest programmiliikidest.

4. Parasiittarkvara

Koos Interneti kasutusala laienemisega on suurenenud oluliselt pahavara levik. Kuid pahavara arendajatel on probleem - pidevalt hingavad kuklasse mitmesuguste tõrjesüsteemide arendajad. Seetõttu toimub intensiivne uute võimaluste ja tehnoloogiate otsimine ja areng. Tõusvaks trendiks on saanud tehnoloogiad, mis võimaldavad pahalasel jääda märkamatuks nii tõrjeprogrammidele kui ka operatsioonisüsteemile. Üldiseks nimetuseks kõigile sellisele on saanud juurkomplekt (*rootkit*), mille all mõeldakse nii nähtamatuks jäävat pahalast ennast, kui ka meetodeid ja valmis koodilõike, mis annavad mõnele pahaprogrammile peitumisvõime.

Loogikapomm (logical bomb)

Loogikapommiks nimetatakse pahatahtlikku koodilõiku kusagil programmis, mis on just nimelt istutatud sinna ohtralt kurja tegema, alates siis failide rikkumise või kustutamisega ning lõpetades hajutatud teenusetõkestamise ründe (DDOS - Distributed Denial of Service) käivitamisega. DDOS on üks karmimaid viise süsteemide halvamiseks ja maha võtmiseks. Nimelt on võimalik sellega hukutada sadu süsteeme üheaegselt. Loogikapomm on tavaliselt osa viirusest, milliseid saadetakse maili teel, või poogitakse mõne pealtnäha ohutu programmi/faili külge. Samas on olnud ka juhtumeid, kus legaalse tarkvara osaks on juba alguses kirjutatud selline koodilõik, saamaks kasutaja arvuti kohta infot. Tavaliselt on sellest hoiatatud toote litsentsis, aga enamus kasutajaid ei ole huvitatud litsentsi läbi lugemisest. Klikkides *accept licence* ollakse automaatselt nõus, et programm hakkab tootjale saatma infot nii, et lõppkasutaja sellest aru ei saa.

Näiteks on võimalik ka selline variant, et programmeerija peidab selle „kurja“ koodilõik programmi sisse. Selle koodilõik ülesandeks on hakata kustutama andmebaasi faile, juhul kui see töötaja on sunnitud firmast lahkuma.

Tarkvara, mis on sünnipäraselt õelaks loodud nagu viirused ja ussid, sisaldavad väga tihti loogilisi pomme, mis on mõeldud käivituma ja tegutsema kindlate sündmuste tagajärjel. Selline tehnika võimaldab käivitada viiruses oleva loogilise pommi näiteks hetkel, kui ohver siseneb teatud leheküljele, mis töötab koos selle kindla viirusega. Teine võimalus on panna pomm nii öelda plahvatama mingil konkreetsel kuupäeval - näiteks 13. reedel või 1. aprillil.

Loogiliseks pommiks ei saa aga nimetada programmide prooviversioone, mille koodi on kirjutatud lõik, mis peatab programmi töö või siis halvab osa selle tööst peale kindla päevade arvu möödumist.

Veidi tõesti sündinud juhtumitest:

Juunis 1992 aastal arreteeriti firma General Dynamics töötaja Michael Lauffenburger, kes pookis firma tarkvarasse loogilise pommi, mis oleks võinud hävitada raketi arendusprojekti eluliselt tähtsad andmed. Väideti, et tema plaan oli tulla firmasse tagasi kui kõrgepalgaline konsultant, kes suudab selle vea parandada peale pommi käivitumist. Kuid üks teine töötaja avastas tema kirjutatudkoodilõigu. Lauffenburgerile määrati süüdistus arvutisüsteemide töö segamises ja pettuses ning karistuseks taheti määrata 500000 $ ning vanglakaristust, kuid seda vähendati 5000 $ peale.

2000. aasta veebruaris otsustas üks saksa programmeerija istutada loogilise pommi firma süsteemifailidesse, mis ennast automaatselt levitama hakkaks. Pommi käivituse kuupäevaks oli määratud 2000 aasta juuli. Kui teised programmeerijad selle avastasid, oli programm juba laialdaselt levinud. Selle kustutamine kogu firma arvutisüsteemist võttis aega mitmeid kuid.

Trooja hobune (Trojan horse)

Nii nagu müütiline Trooja hobune nägi välja nagu kingitus sisaldades Kreeka sõdureid, kes Trooja linna vallutasid, on tänapäeva Trooja hobused arvutiprogrammid, mis näivad kasulikud, kuid tegelikult ohustavad teie turvalisust ja võivad teha palju hävitustööd. Hiljuti levis üks Trooja hobune meilisõnumis manusfailina, näiliselt sisaldades Microsofti turvavärskendusi; tegelikkuses osutusid need viiruseks, mis üritasid välja lülitada viirusetõrje- ja tulemüüritarkvara.

Trooja või kaugjuhtimis-, kaughaldamistarkvara on ühelt poolt süsteemihaldajale väga vajalik töövahend, aga see, et seda nii peidetult ja lihtsalt saab sokutada kellegi masinasse, teeb sellest potentsiaalse ohuallika, mis on küllalt tõsine. Enamjaolt nimetatakse Trooja hobuseks ikkagi pahaloomulist programmiversiooni. Trooja hobused jagunevad veel omakorda 7 klassiks vastavalt meetodile, mille järgi nad hakkavad klientsüsteemi kasutama:

- Kaugpöördus Trooja (*Remote Access Trojan*)
- Andmeedastus Trooja (*Data Sending Trojan*)
- Hävituslik Trooja (*Destructive Trojan*)
- Proksi Trooja (*Proxy Trojan*)
- FTP Trooja
- Turbetarkvara sulgemise Trooja (*Security Software Disabler Trojan*)
- Teenusetõkestamise Rünnaku Trooja (*Denial of Service Attack Trojan*)

Trooja hobused levivad tavaliselt ohvri arvutisse elektronpostiga kaasapandud failina,

peibutades inimesi käivitama programme, mis näivad pärinevat ohutust allikast. Kui saaja selle avab, installeerib Trooja end lahti ja muudab ohvri arvuti nn kliendiks. Seejärel pääseb igaüks, kel on tarkvara teine pool ehk serveri pool, interneti kaudu ohvri arvutisse ning saab seal teha kõike seda, mida ohvergi. Trooja hobuse kasutamisulatus sõltub ka rünnatava arvuti kasutaja õigustest konkreetse süsteemi üle. Kui ohver on näiteks *root* õigustes (Linux OS) või *administrator* (Windows keskkond), siis on sissetungijal võimalus kasutada kõiki nende õigusi:

- kustutada faile
- endale ohvri arvutist alla laadida faile ja neid lugeda
- muuta faile
- installeerida teisi programme administraatori õigustes, näiteks programme, mis võimaldavad võrgule juurdepääsu nagu *keylogger*id
- saab muuta kasutajaõigusi sellisel viisil, et peaõigused (*full control*) jäävad ainult Trooja istutajale ehk ründajale ja tegelikul kasutajal võetakse ära enamus õigusi, kasvõi käivitada anti-viirus programme kahtlaste failide avastamiseks.
- saab installeerida ohvri arvutisse teisi rünnakutarvarasid ja neid enda äranägemise järgi peita operatsioonisüsteemi failidesse
- installeerida teisi Trooja hobuseid.

Äärmiselt ohustatud on arvutisüsteemid, mis jagavad võrku ja mis ei ole kaitstud riistvaraliste ega tarkvaraliste krüpteerimisvahenditega (VPN, HTTPS, SFTP, SSH, Netscreen). Sellises sisevõrgus levivad pahatihti paroolid, kasutajanimed ja salajane info avatud teksti kujul. Trooja kaudu on võimalik paigaldada nuuskvara (*sniffer*), mis hakkab kogu seda infot salvestama ja ründajale edastama.

Eesti suurettevõtted, sealhulgas pangad on spetsialistide sõnul uue rünnaku eest piisavalt kaitstud. Vähemkaitstud on pahatahtlike eest keskmise suurusega ja väikesed firmad. Kasutajate parema kaitse huvides saadab Microsoft turvabülletääne sageli meiliga, kuid mitte kunagi pole nendega kaasas manuseid. Trooja hobuseid saab kaasa panna ka tarkvarale, mida te tasuta alla laadite.

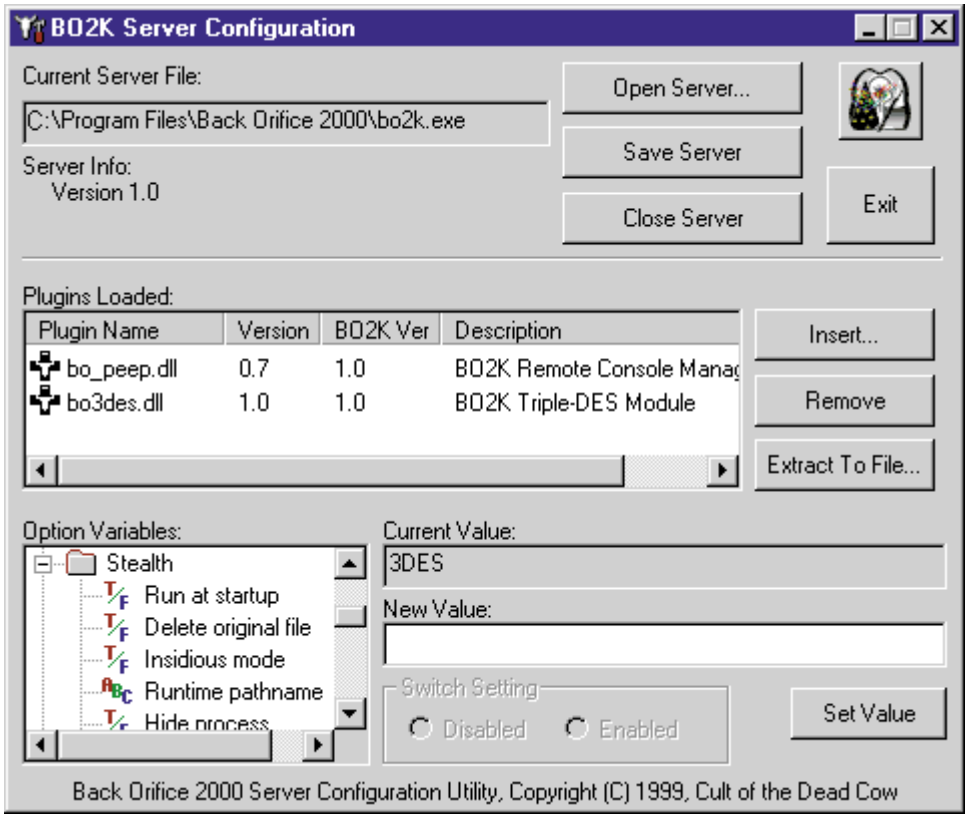
Järgnevalt veidi praktilisi nõuandeid, et vältida nakatumist:

- Kunagi ei tasu pimesi alla laadida faile/tarkvara inimestelt või saitidelt, mille turvalisuses ei ole sa 100% kindel. Teisiti öeldes: ei maksa kunagi võõrastelt kommi vastu võtta. Kui arvutikasutaja on selline, kes armastab ohtralt alla laadida erinevaid programme ja faile,

sellel on ainult aja küsimus, millal ta langeb Trooja ohvriks.

- Isegi siis, kui fail tuleb sõbra käest (maili teel, IRC kanalite vms. kaudu), tasub enne faili avamist uurida selle tausta ja mida see sisaldab. Pahatihti ei pruugi see sõber aimatagi, et saadab edasi faili, mis on juba eelnevalt tema arvutis nakatatud Trooja hobusega. Vähimagi kahtluse korral tasub fail läbi kontrollida kõige uuema viirusetõrje programmiga.
- Peab olema ettevaatlik peidetud faili laiendite suhtes. Vaikimisi peidab Windows ära viimase faili laiendi nii, et süütu väljanägemisega „kutsu.jpg“ võib tegelikult osutuda hoopis „kutsu.jpg.exe“-ks, mis on tõenäoliselt käivitatav Trooja. Et selliseid situatsioone vältida, tuleb Windowsi seadistusi muuta nii, et kogu faili nimi ja laiend(id) oleksid näha.
- Kunagi ei tasu kasutada programmides lisavõimalust, mis pakub faili enne avamist automaatselt seda vaadata. Näiteks pildiprogrammid ja ka Outlook võimaldavad faile (maile) eelvaadelda. See võib küll tunduda mugavana, kuid tegelikult see programmi lisaomadus käivitab selle faili automaatselt ja võib nakatada süsteemi.
- Kunagi ei tasu pimesi kirjutada käske, mida keegi, keda sa ei tunne, palub kuhugi sisestada. Samuti ei tasu külastada võõraste poolt välja reklaamitud veebilehekülgi ja klikkida tundmatutel või kahtlastel saidi linkidel. Ka lingid võivad sisaldada koodijuppi, mis võib teie arvutis käivitada viiruse või tekitada muid kahjustusi, mis ei pruugi väljagi paista.
- Ei tasu usaldada turbeprogramme, mis on kaasa antud mõne teise tarkvaraga (tavaliselt pakutakse selliseid programme kaasa just vabavaraga). Need programmid ei ole reeglina tunnustatud ekspertide poolt ja ei tee oma tööd nii nagu peavad. Turvalisuse tagamise asemel võivad nad tekitada lihtsalt süsteemi lisa turvaaugu.
- Lõpetuseks, ei tasu alla laadida suvalisi programme „lihtsalt selleks, et seda korraks vaadata kuna keegi soovitas“. Kui selline programm peaks juhuslikult sisaldama Trooja viirust oled sa automaatselt peale käivitamist nakatunud.

Tuntumaid trooja hobuseid ja rünnakuid Windowsi operatsioonisüsteemi ebaturvalisuse demonstreerimiseks on Cult of the Dead Cow (Surnud Lehma Sekt) häkkerite poolt internetti riputatud tarkvara, mille kasutamine võimaldab kerge vaevaga tungida internetiga ühendatud ja Windowsil põhinevatesse personaalarvutitesse ja seal omatahtsi tegutseda. Näiteks saab selle abil minna teise inimese arvutisse ja vaadata, mis tal parasjagu ekraanil ja failides on. Kui host kirjutab maili saab seda avada, pärast ise muuta või kustutada. Selle kaughaldamistarkvara nimi on Back Orifice 2.0 (vt joonis 1), mille lehmasekti liikmed on tuletanud Microsofti Back Office programmi nimest ning selle esimene variant on ringelnud maailmas juba aastapäevad.



Joonis 1. Back Orifice serveraken (allikas: www.sourceforge.net)

Uss (worm)

Uss on iseennast kopeeriv programm, täpselt nagu viiruski, kuid mida päris viiruseks nimetada ei saa ja kvalifitseerub pigem ründetarkvara alla. Kui viirus vajab levimiseks mingit teist programmi, mille külge klammerdudes levida, siis uss on iseseisev ja teeb selle töö autonoomselt ära. Ta ei vaja levimiseks nö emaorganismi. Uss võib oma paljunemise käigus olla programmeeritud tegema kõiksugu pahandusi: nt kustutama faile või saatma dokumente sinu arvutist kuskile mujale. Sellise ülikiirelt leviva pahaloomulise kasvaja vohamine arvutivõrgus kulutab kõvasti masina ressurssi ning aeglustab ka võrguühendust. Ussi tüüpiline levimisskeem joonisel 2. Kui viirusetõrje suudab küll ussi nime kindlaks teha, kuid ei suuda seda kuidagi ära hävitada, tuleks Internetist tõmmata konkreetselt selle ussi eemaldamist mõeldud programm. Üks laialdasema levikuga usse oli „Love Letter“, mis tungis miljonitesse arvutitesse.

Nimi „uss“ võeti 1970-ndatel aastatel ilmunud John Brunneri ulmenovellist „The Shockwave Rider“.

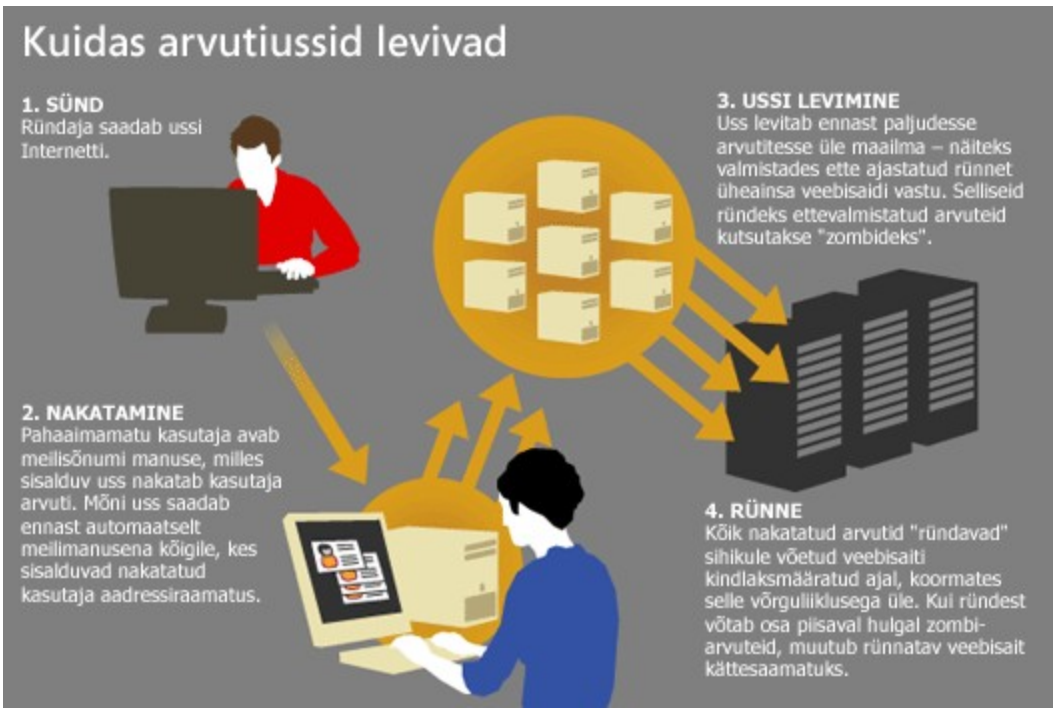
Esimene ussi loomine teostati kahe teadlase poolt Xerox PARC-is aastal 1978. Selle autorid John Shoch ja Jon Hupp disainisid selle ussi algselt selleks, et avastada võrgus mittetöötavaid protsessoreid ja neile ülesandeid määrata, jaotades protsessid laiali ning sellega täiustada kogu arvutivõrgu efektiivsust.

Esimene teadaolev interneti ussi rünnak toimus aastal 1988 USA-s. Autoriks osutus Cornelli Ülikooli üliõpilane Robert Morris. See „uss“ nakatas lühikese ajaga 6200 VAX- ja Sun-arvutit, mis töötasid operatsioonisüsteemi Unix teatud versioonidega. Paljud organisatsioonid, sealhulgas suured teaduskeskused olid sunnitud ennast mõneks ajaks internetist lahti ühendama. Kogu kahju oli ligikaudu 98 miljonit USD.

2004 aasta veebruaris hakkas ennast kiirelt levitama Novarg/MyDoom nimeline uss. Uss levis KaZaA võrgus või läbi e-maili. KaZaA olemasolul levitati viirust jagatud failide kataloogis kõiksugu .exe/.bat/.pif/.scr failidena, e-maili korral, nagu ikka, oli tegu manusega, mille kasutaja peab käima panema. Selleks oli ussi loojal mõeldud välja väga muljet avaldav trikk. Ta meisterdas hoolikalt mitu tõelisena tunduvat meilisüsteemi veasõnumit, kasutades erinevaid pealkirju nagu "Mail Delivery System," "Test," ja "Mail Transaction Failed". Arvatavasti on sellist tüüpi meilisõnumite saamine kõigile täiesti tavaline. Niisugused on ka tõelised sõnumid, mis annavad teile teada, et mõni teie saadetud meilisõnum ei jõudnud soovitud adressaadini. Sageli sisaldavad need tehnilisi väljendeid, mida paljud inimesed ei mõista. MyDoomi looja jäljendas neid väljendeid sellisel viisil, et suutis petta miljoneid inimesi ja meelitada neid manust avama.

Hilisemates MyDoomi versioonides on kasutatud hirmutamistaktikat, saates muuhulgas võltssõnumeid, mis näivad pärinevat kasutaja internetiteenuse pakkujalt, hoiatusega, nagu oleks kasutaja arvutis uss ning ainuke viis selle eemaldamiseks oleks kasutada meilile lisatud manust. Nagu võib aimata, sisaldas manus tegelikult ussi.

Lisaks levimisele on ussi programmeeritud 1. ja 12. veebruari vahel GET päringutega pommitama SCO (www.sco.com) veebisaiti.



Joonis 2. Näide usside levimismeetodist ja rünnakust (allikas: www.microsoft.com).

Viirus (virus)

Arvutiviiruseks nimetatakse programmi, mis on võimeline looma endast koopiaid ning neid ilma kasutaja teadmata salvestama. Piirideks jäävad vaid arvutite võimalused ja viiruse programmeerija fantaasia. Salvestada saab viirusi mitmesugustesse operatsioonisüsteemi- ja võrguobjektidesse, sealjuures ei pea tekkivad koopiad korduma üks-ühele, ainult peavad säilitama oma levikuvõime. Tavalise arvutikasutaja teadmised viirustest on kasinad. Selle näiteks on ühelt poolt ettevaatamatus e-posti kirjade manuste avamisel, teiselt poolt aga arvamus, nagu võiks viirus arvuti protsessori läbi kõrvetada. Tegelikult on viirused siiski sügavalt tarkvaraline nähtus, mis halvemal juhul saavad näiteks rikkuda kogu kõvakettal asuva informatsiooni.

Arvutiviiruste suhtes kõige tundlikumaks on osutunud IBM PC-ühilduvad arvutid. Nendel arvutitel on avastatud praktiliselt kümme korda rohkem viiruseid kui teistel. Seni on viiruste suhtes kõige töökindlamaks osutunud Macintosh tüüpi arvutid. Üldiselt võib IBM tüüpi arvuti viirused jagada kahte suurde gruppi. Esimeseks oleksid viirused, mis kasutavad oma levikuks faile (nakatades neid). Enamasti osutuvad nakatunuteks *.EXE ja *.COM failid, aga on olemas viiruseid, mis suudavad nakatada ka teistsuguste laienditega (*.SYS, *.OVL, *.PRG) faile. Faile nakatavad viirused võib omakorda jaotada kaheks: viirused, mis loevad end residentselt mällu ja viirused, mis ei loe end residentselt mällu. Teiseks viiruste rühmaks oleksid süsteemi või buut-sektori viirused. Siia gruppi kuuluvad viirused, mis kirjutavad oma koodi ketta buut-sektorisse. Seega tehes algkäivituse nakatunud kettalt aktiviseeritakse ka viirus. Sellised viirused on tavaliselt üsna destruktiivsed, sest kirjutades viiruse koodi buut-sektorisse, kirjutatakse üle seal eelnevalt asunud info ketta kohta. Kuid on olemas ka viiruseid, mis suudavad nakatada nii faile, kui ka buut-sektorit. Selliseid viiruseid kutsutakse Multi-Partite viirusteks. On välja mõeldud palju nn. "abi"tehnoloogiaid, mis raskendavad viirustõrje programmidel viirusi leidmast. Need on "mootorid", mida saab viiruse koodi juurde panna, et viirus oleks raskesti avastatav või oleks tema levik kiirem/laialdasem.

Arvutiviiruste liigitus

Viiruseid võib jagada 6 peamisesse kategooriasse:

- Failiviirused ehk parasiitviirused - nakatavad programmifaile - tavaliselt COM-, EXE- või SYS-faile ning saavad aktiveeruda ainult nakatatud faili käivitamisel. Tavaliselt saab juhtimise kõigepealt viirus, seejärel täidetakse algne programm ise.
- Buutsektori viirused - peituvad kõvaketta laadesektoris ning laaditakse mällu enne

süsteemifaile. Maskeerimiseks väljastab viirus alglaadimisel normaalseid teateid. Tavaliselt liigitatakse sellesse viiruserühma ka sektsioonitabeli (*partition table*) viirused, mis nakatavad kõvaketta füüsilise nullsektori. Tuntumaid esindajaid: Brain, Form, Michelangelo, Stoned.

- Skriptiviirused - skriptikeeles kirjutatud viirus. Tavaliselt sisaldub veebilehtedes ja käivitub nende avamisel. Võib peituda ka HTML-formaadis kirjutatud kirjades. Kuulsamaiks skriptiviiruseks sai 2000 aasta 5 mail levima hakanud LoveLetter, mis kindlustas ka koha Guinessi rekordite raamatus.
- Makroviirused - Makroviirused levivad ainult makrokeele kasutamist võimaldavates süsteemides. Seda tüüpi viiruste lemmikobjektideks on MS Wordi ja MS Exceli dokumendid.
- Polümorfsed viirused ehk mutatsioonviirused - peitviiruste uus põlvkond, mis ilmus 1990. aastatel. Nendes on rakendatud vahendeid peitumiseks mitte ainult lihtsa diagnostika, vaid ka viirusetõrjeprogrammide eest. Kuna niisugused tõrjeprogrammid põhinevad teatavate iseloomulike koodilõikude tuvastusel, on kood näiteks permuteeritud, üle külvatud juhusliku jaotusega tühikäskudega (NOP) või krüpteeritud. Kuulsaimaks polümorfseks viiruseks sai OneHalf, mis veel praegugi maailma arvutikasutajale muret valmistab.
- Nähtamatud viirused - haarab enda kätte lisaks failide käivitamise katkestusele ka teisi kettaoperatsioone teostavaid katkestusi: tema tööpõhimõte seisneb BIOS-i rutiinide saboteerimises nii, et nad annaks ketta kohta valeinformatsiooni. Lihtsamad stealth viirused näitavad nakatunud faili suuruse asemel algse faili suurust, põhjalikumad aga võltsivad lausa failide sisu, näidates viiruse asemel algset sisu.

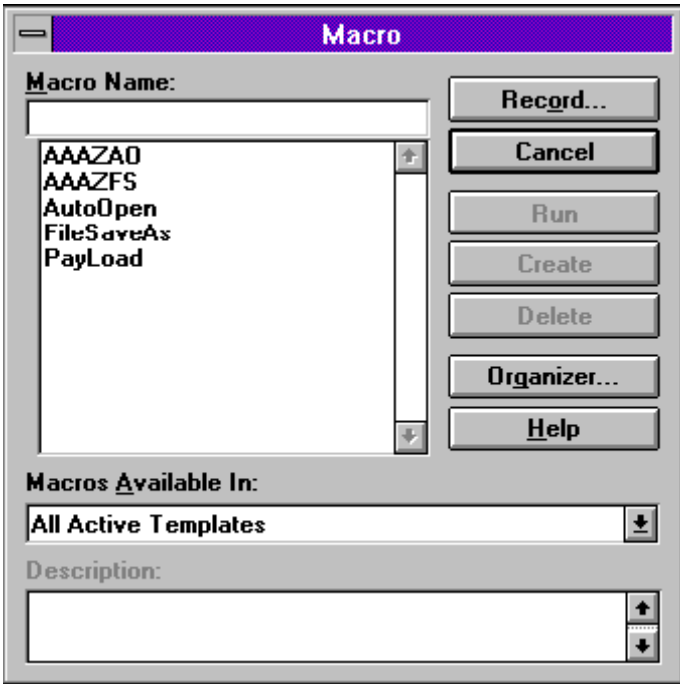
Nagu kohane infoühiskonnale, on teadmine jõud. Ja just suuremad teadmised arvutiviiruste levikust ja toimimisest aitavad arvuti nakatumist ära hoida. Kindlasti on vajalik antiviirustarkvara kogu aeg arvutis töötamas hoida. Viiruste tõrjumisel ei tasuks aga lootma jääda ühele kindlale firmale, vaid kasutama vaheldumisi mitut antiviirust. Tuleb suhtuda kriitiliselt igasugusesse arvuti veidrasse käitumisse. Ettevaatusest hoolimata ei ole aga keegi meist kunagi täielikult arvutiviiruste vastu kaitstud.

Makroviirus (macro virus)

Makroviirused on rakendusprogrammi makrokeeles kirjutatud makrod, mis nakatavad

vastavate rakenduste dokumendifaile. Mõned aastad tagasi peeti dokumendifaile viiruste leviku mõttes ohututeks, ehkki esimesed makroviirused kirjutati katseks juba 1980te aastate alguses. Tänapäevaks on see viiruse tüüp peaaegu välja surnud.

Suurima rühma moodustasid 1996. a. keskel Microsoft Wordi makroviirused; neid on teada paarkümmend, tuntuimad on Concept (esimene tegelik makroviirus, ilmus sügisel 1994), Nuclear, DMV, Colors, Hot, Atom ja Xenixos. Levinuim on Concept, mis nakatab MS Wordi (v. 6.0 jj) dokumendi- ja mallifaile (tavaliselt laienditega .DOC ja .DOT) kõigil ta platvormidel. Kuna viirus on kirjutatud Wordi makrokeeles, ei saa ta toimida teistes tekstiprotsessorites, mis Wordi dokumente loevad ja konverteerivad (WordPerfect, AmiPro). Viirus koosneb makrodest AAAZAO, AAAZFS, AutoOpen, FileSaveAs ja PayLoad (vt joonis 3). Nakatatud dokumendi avamisel installeerib viirus end globaalsesse makroteeki (kui teda seal veel ei ole), mis harilikult asub failis NORMAL.DOT. Pärast seda nakatatakse iga dokument või mall, mis salvestatakse käsuga Save As.



Joonis 3. Wordi makroviirus (allikas: alpha1.fmarion.edu).

Juulis 1996 ilmus MS Exceli makroviirus ExcelMacro/Laroux, mis on kirjutatud VBA-makrokeeles ning koosneb kahest moodulist: *auto_open* (*PERSONAL.XLS!auto_open, BOOK1!auto_open*) ja *check_files* (*PERSONAL.XLS!check-files, BOOK1!check_files*). Viirus toimib alates Exceli versioonist 5, ta ei nakata varasemates ega ka *Macintoshi* versioonides.

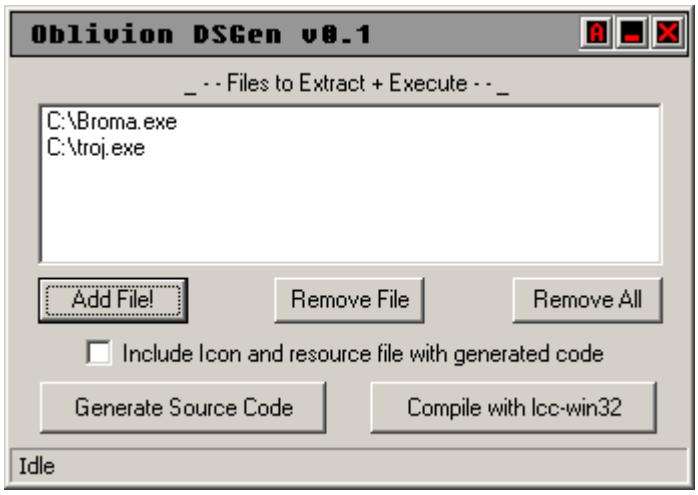
Jaanuaris 1996 avastati Lotus AmiPro makroviirus Green Stripe, mis loob iga SAM-faili juurde samanimelise SMM-makrofaili ja lingib selle SAM-failiga.

Põhimõtteliselt saab makroviiruseid kirjutada kõigile makrokeelt sisaldavatele rakenduspakettidele.

(Viide: Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit „Infosüsteemide turve I osa - Turvarisk“, 1997, lk 29-30)

Pipett (dropper)

Pipett on programm, mis kirjutatud ainult selleks, et see installeeriks rünnatavasse arvutisse vastava ründetarkvara. Teda ennast ei saa viiruseks nimetada, kuigi ta kannab endas viiruse koodi. Pärast arvutisse paigutamist leiab dropper koodilõigule tema jaoks mõeldud koha ja istutab selle sinna sisse (vt joonis 4). Viirusetõrje programmid ei tunnista pipetti kui viirust, kuna pipett sisaldab kõigest selle kurja tegevat koodilõiku, millel pole viiruse tunnuseid küljes.



Joonis 4. Pipeti Oblivion peaaken (allikas: http://www.pestpatrol.com).

5. Kuidas ennetada rünnakuid?

Arvutite, arvutivõrkude ja infosüsteemide turvamiseks kasutatakse organisatsiooniliste meetmete kõrval tark- ja riistvaralisi vahendeid ning nende kombineerimist. Hakates otsima ideaalset lahendust ja meetodeid pahavara vastu võitlemiseks ja kahjude ära hoidmiseks, siis võib hämmastusega avastada, et ideaalset lahendust sellele probleemile ei olegi. Kõik sõltub ikkagi konkreetsest infrastruktuurist ja majanduslikest võimalustest. Sellegipoolest on olemas tüüpilised pidepunktid, mida järgides on võimalik hoida oma arvutisüsteem maksimaalselt kaitstud. Autor leiab, et spetsiifilisema lahenduse peaks välja töötama konkreetse asutuse IT-spetsialistid vastavalt asutuse töötajate turvateadlikkusele ja IT osakonna poolt juba rakendatud turbelahendustele.

Lähtudes sellest, et enamus asutusi on oma aruvitsüsteemid ehitanud üles Windows operatsioonisüsteemi baasile, võib tuua välja järgmised pidepunktid, mida tuleks lõppkasutajatega tegeledes ja neid instrueerides silmas pidada.

1. Lõppkasutajal ei tohi olla rohkem õigusi kui Restricted User Groupil. Reegel ei kehti sülearvuti kasutajatele, kellel võiks olla Network Operator õigused. Piiratud kasutusõigus tagab süsteemifailide puhtuse ja korra. Kasutajal puudub ka õigus installeerida oma äranägemise järgi programme ja ründetarvara juhuslik installeerimise risk lokaalsesse arvutisse on minimaalne. Network Operator õigused on põhimõtteliselt samad, lisaks on ainult võrguseadete muutmise võimalus (traadivaba internetiga ühendumine nõuab neid õigusi).
2. Paroolide pähe õppimine on rohkem kui kohustuslik juba esimesel tööpäeval. Paroolid peab määrama IT-spetsialist. Tavakasutaja väljamõeldud paroolid on tihtipeale väga lihtsad ja seetõttu ei tohiks neid iseseisvalt muuta. Paroolimurdmisprogrammid lahendavad lihtsaid paroole ilma mingisuguse probleemita.
3. Keelata ära Internet Exploreri kasutamineja kasutada soovitavalt vabavarana allalaaditavat Mozilla Firefox'i. Internet Explorer lubab vaikimisi käivitada Javascripti ja ActiveX komponente, mis võivad olla pahalase kirjutatud ja halvemal juhul võimaldatakse kaugpääs kogu kõvakettale. Vältida MSN IM kasutamist ja võtta kasutusele alternatiivina näiteks Skype (samuti tasuta veebist allalaaditav), mille sõnumid on vaikimisi krüpteeritud.
4. Lõpetada Windows XP tulemüüri kasutamine ja asendada see vabavarana allalaaditava tulemüüritarkvaraga, näiteks Comodo Firewall'iga, mis 2006 aasta lõpus tehtud tulemüüritestide järgi sai esimese koha (Windows XP tulemüür viimase).
5. Tugevdada spamfiltreid ja teadvustada töötajaid e-mailiga saabuvate manuste võimalikest

ohtudest, sest manuste avamisega tõmmatakse kõige rohkem kõikvõiamlikku pahavara oma arvutisse. Spamfiltreilahendusi on tänapäevaks välja arendatud väga palju - mõned riistavaralised, mõned tarkvaralised. Millise lahenduse juurde jääda on iga ettevõtte IT-spetsialistide eneste otsustada.

6. Töötada välja korralik võrguressursside ja arvutikasutamise reeglistik. Sülearvuti ja lauarvutikasutajatel peavad olema eraldi nõuded ja reeglid. Sülearvuti kasutajatel on suurem oht sattuda rünnaku alla, sest nad kasutavad tihti lahtisi traadita võrgu ressursse (lennujaamad, tanklad, pubid)ja jätavad traadita võrgu tööle isegi siis kui nad seda ei vaja .
7. Hinnata uute töötajate arvutitundmist – vajadusel instrueerida. Praktika on näidanud, et koolitus ei mõju suurele massile. Lõppkasutajatele on reeglite selgeks tegemine võimalik väikeste gruppide kaupa, ideaalne oleks individuaalne juhendamine.
8. Hankida antiviiruse programm ja seadistada selliselt, et uute viiruste nimekirja uuendataks vähemalt igapäevaselt, mis enda viiruste nimekirja iga päev uuendaks.

6. Kokkuvõte

Pidev tarkvaraarendus IT maailmas toob endaga kaasa pideva arengu ka ründetarkvara valdkonnas. Tänapäeva ründetarkvara vastases sõjas ei saa enam loota ainult spetsialistide abi peale vaid peab keskenduma pigem kasutajate informeerimisse neid ohustavatest programmidest. Õnneks on sellega viimastel aastatel tegelenud väga hoogsalt arvuteid edasi müüvad asutused, kes annavad arvutiga kaasa peale muu tarkvara ka antiviiruse programmi. Kuid nagu eelnevast võib järeldada, ei saa tänapäeval enam ka antiviiruse programmide peale loota. Kui lõppkasutaja on ikka naiivne ja liiga usaldav, siis suure tõenäosusega kubiseb tema arvuti juba varsti kõikvõimalikest ründetarkvara komponentidest, mis tekitavad ohtliku turvaaugu tema arvutisse ja hõlpsama ligipääsu tema informatsioonile. Elektroonilise posti ja *peer-to-peer* (MSN, Kazaa jne) failivahetusteenuste kaudu, mille kasutamine on viimaste aastate jooksul väga suure hoo sisse saanud, liiguvad viirused ilma igasuguse kontrollita. Nad on suutelised ennast varjama teistes failides, tänu millele võivad kasutajad üksteisele viiruseid täiesti pahaaimamata levitada. Täiesti segamatult hiilivad nad mööda ka tulemüüridest. Riski vähendamine on kogu infoturbe lõppeesmärk. Riski täielik kõrvaldamine on põhimõtteliselt võimatu, riski peaaegu täielikult kõrvaldamine võib aga minna ülemäära kulukaks. Maksimaalne panus, mida saaks lõppkasutaja riskide vähendamiseks teha oleks pidev kontroll oma failide ja nende liikumise üle ning igapäevaselt täiendatud turvameetmed personaalarvutis tagavad kaitse ründetarkvara eest.

Leian, et seminaritöö täidab oma eesmärgi, kui see aitab kaasa IT-spetsialistidel oma ettevõtete arvutite turvalisust tõsta, annab kerge ülevaate tavakasutajatele ja huvilistele ründetarkvara omadustest ja ohtlikkusest ning tõstab lugejate turvateadlikkust. Käsitlemata jäid teemad, mis puudutavad laiemalt koht- ja laivõrkude turvalisust ja üldist ründprogrammide komplekti - rootkit. Tulevikus on soov pühenduda laiatarbe tarkvara nõrkuste ja turvaaukude uurimisele.

7. Kasutatud kirjandus

1. http://www.microsoft.com/eesti/security/home/antivirus/lifecycle.mspx
2. http://www.epl.ee/?artikkel=54343
3. http://www.secunia.com
4. http://www.net-security.org/
5. http://www.kakupesa.net:8080/akadeemia/arhiiv/IBK/loengud/loeng8
6. Kevin Beaver, "Hacking for Dummies", Wiley Publishing, Inc., 2004
7. Margus Sakk, "Arvutiviirused", 2004
8. Lance Spitzner, "Honeypots: Tracking Hackers", Addison Wesley, 2002
9. Seymore Bosworth, M.E. Kabay, "Computer Security Handbook", John Wiley & Sons, Inc., 2002
10. Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit „Infosüsteemide turve I osa - Turvarisk“, 1997