Blekinge Tekniska Högskola
Institutionen för Programvaruteknik och Datavetenskap
Informationssystem 120p

# SÄKERHETSHOT OCH LÖSNINGAR FÖR PRIVATPERSONER MED BREDBAND

KANDIDATUPPSATS I DATAVETENSKAP
VT – 2001

| Författare: | Handledare: | Examinator |
| --- | --- | --- |
| Carolina Bilan IS98<br>Carl Hedberg IS98 | Kerstin Ådahl | Håkan Grahn |

# ABSTRACT


**Title:** Security threats and solutions for people with broadband.

**Authors:** Carolina Bilan and Carl Hedberg

**Problem description:** As more and more people gain access to broadband in their properties, the security threats get bigger. A lot more people also have so called "personnel buy computers", where they store important information concerning the company. The information is very easy to retrieve for a person with the knowledge and the will to do it. Very few people have any knowledge of how to protect themselves from these threats.

**Question:** What kind of security threats are there?
Are there any protections against these threats?
Which solutions are most suitable?

**Conclusion:** When people start using broadband, the time when people are connected to the Internet, the security threats get higher. There are different kind of threats such as viruses and hacking attempts. Virus spread very fast by the use of e-mail, but also with cd: s and discs. The help of a Trojan horse performs the most common form of intrusion. There are ways that you can protect yourself, such an example is by installing a firewall.


**Keywords:** Broadband, Firewall, Security, Virus, Antivirus, Personal Firewall, Hacking, Hackers.

# SAMMANFATTNING

**Titel:** Säkerhetshot och lösningar för privatpersoner med bredband

**Författare:** Carolina Bilan och Carl Hedberg

**Problemområde:** Nu när allt fler människor börjar få tillgång till bredband i sina fastigheter ökar även säkerhetsriskerna. Allt fler människor har också så kallade personalköpdatorer, där de kanske har viktig information som rör företaget. Viktig information lagras ofta på hårddisken utan att säkerhetskopieras, där den är lättillgänglig både för förstörelse och för stöld. Många användare sitter uppkopplade mot Internet utan kunskaper om säkerhet och hur de skyddar sig mot intrång och virus. Därför kan datorn bli väldigt lättillgänglig för människor med viljan och kunskaperna att komma åt den.

**Frågeställning:** Vad finns det för säkerhetshot?
Vad finns det för skydd mot dessa hot?
Vilka lösningar är mest lämpliga?

**Slutsats:** I samband med att bredband används blir uppkopplingstiderna längre vilket leder till att hoten ökar. De hot som finns mot privatpersoner är olika former av virus och intrång. Virus sprids väldigt snabbt med hjälp av e-post, men sprids även via disketter och cd-skivor. Den vanligaste formen av intrång är med hjälp av trojanska hästar. De lösningar som finns mot hoten är att installera antivirusprogram och någon form av brandvägg.

**Nyckelord:** Bredband, Brandvägg, Säkerhet, Virus, Antivirus, Personlig Brandvägg, Hackning, Hackare.

# INNEHÅLLSFÖRTECKNING

# INLEDNING

*”Plötsligt glider luckan till din cd-spelare upp, bara för att stängas igen några sekunder senare, utan att du rört någon knapp på datorn. Sedan börjar filer byta plats på hårddisken och ditt e-postprogram skickar iväg e-brev med elaka meddelanden till alla i din adressbok. Har din dator fått eget liv? Förmodligen inte, men någon har tagit sig in i din dator med hjälp av en trojansk häst och styr nu exakt vad som händer på din bildskärm. Det enda du kan göra är att rycka ut strömsladden och hoppas att hackaren inte förstört något av värde.”* [1]
– utdrag ur artikeln “Brandväggen skyddar dig mot hackare”, *PC för Alla*, nr 2 2001

Situationen som beskrivs är påhittad, men varje dag sker liknande intrång i privatpersoners datorer.

Virus och intrång är stora säkerhetshot, såväl med modemuppkoppling som med bredbandsuppkoppling. Med bredband är risken större att användare utsätts för intrång i sitt datorsystem eftersom tiden datorn är uppkopplad mot Internet oftast blir längre.
En bredbandsuppkoppling är ett mycket välkommet alternativ till modem. Detta för att bithastigheten är mycket högre och för att det blir smidigare för användaren eftersom tiden det tar att koppla upp sig är minimal. För en fast summa i månaden kan användaren vara uppkopplad hur länge den vill. Även om bredbandsuppkoppling innebär att användarens dator alltid är uppkopplad innebär det också att datorn alltid är exponerad för människor som vill försöka ta sig in i den.[2]

Allt fler människor har också så kallade personalköpdatorer, där de kanske har viktig information som rör företaget. Viktig information lagras ofta på hårddisken utan att säkerhetskopieras, där den är lättillgänglig både för förstörelse och för stöld. Många användare sitter uppkopplade mot Internet utan kunskaper om säkerhet och hur de skyddar sig mot intrång och virus. Därför kan datorn bli väldigt lättillgänglig för människor med viljan och kunskaperna att komma åt den.

Uppsatsen är det sista momentet på programmet Informationssystem vid Blekinge Tekniska Högskola för att få en kandidatexamen i datavetenskap. I samband med den snabba utvecklingen av bredband har nätsäkerheten blivit en viktig fråga. Uppsatsen är skriven för att ge en inblick i problemet och de säkerhetshot som finns samt visa på lösningar. Utifrån problembeskrivningen har följande frågeställning formulerats, vilka skall besvaras i uppsatsen.

- Vad finns det för säkerhetshot mot privatpersoner?
- Vad finns det för skydd mot dessa hot?
- Vilka säkerhetslösningar är mest lämpliga?

[1] Joakim Bergström, ”Brandväggen skyddar dig mot hackare”, *PC för Alla*, nr 2 2001
[2] Cassimir Medford, “Security – You can get there fast – but is it safe?”, *PC Magazine*, 6 februari 2001

Uppsatsen riktar sig mot privatpersoner med bredbandsuppkoppling och som vill veta mer om ämnet säkerhet. Därmed frånsägs inte att andra intressenter utöver de nämnda kan ta del av uppsatsen. En ordlista med de vanligaste datortermer som förekommer i uppsatsen har utformats för att även personer med liten datorkunskap skall kunna ta till sig innehållet i uppsatsen.

Uppsatsen kommer framför allt avgränsas till säkerhetshot som kommer från Internet, undantaget virus och trojanska hästar som utöver via e-post kan spridas med hjälp av disketter, cd-skivor och zip-skivor.
Avgränsningar kommer även att göras för inriktning på säkerhetshot rörande operativ-systemet Windows. Eftersom det redan finns tester av säkerhetsprogram utförda av oberoende tredje part, som visar att det inte är större skillnader på programmen vad gäller säkerhet. Därför kommer vi inte att testa detta utan rikta in oss på administration och konfiguration av programmen.

# BAKGRUND

Med dagens användarvänliga intrångsprogram kan i princip vem som helst ta sig in i oskyddade datorer. För att slippa obehagliga överraskningar när användare är uppkopplad mot Internet, bör de använda skydd mot hackarnas intrångsförsök.

Per Albinsson, som är säkerhetsexpert på datasäkerhetsföretaget Atremo menar att för att få riktigt bra skydd behövs både ett antivirusprogram och en personlig brandvägg installerad på datorn. Men när väl de här programmen har installerats, måste de underhållas och uppdateras. Bara för att programmen är installerade, betyder det inte att skyddet varar för evigt. Antivirusprogrammets virusdefinitioner måste uppdateras ofta och brandväggen måste ställas in så att den verkligen stoppar intrången.[3]

I samband med att allt fler får bredbandsuppkoppling ökar användandet av Internet. Det medför större risk för virusattacker, trojanska hästar och intrång. Attacker med hjälp av trojanska hästar via e-post och webbsidor är de vanligaste tillvägagångssätten vid intrång menar Cassimir Medford, författare till artikeln "Security - you can get there fast – but is it safe?". [4] I dagens samhälle när allt fler människor börjar jobba hemifrån kommer förmodligen fler koppla in sina företagsdatorer, med viktig information rörande företaget, hemma och för att vid ett annat tillfälle koppla in den i företagets nätverk. När datorn kopplas in hemma kan skyddet vara näst intill obefintligt och informationen blir på så sätt lättiljänglig för förstörelse och stöld. Det blir helt upp till användaren att vidta åtgärder för att skydda sig.

I artikeln tar Cassimir Medford även upp att i ett nyligen upptäckt intrång i Microsofts dator- system misstänkts en trojansk häst vara inblandad. Den trojanska hästen kom in i företagets nätverk via en ovetande anställd som kopplat in sin bärbara dator i sin bredbandsuppkoppling hemma där datorn troligtvis hade infekterats av den trojanska hästen. När datorn sedan kopplades in i företagets nätverk kunde hackers lätt ta sig in bakvägen i företagets system med hjälp av den trojanska hästen. Hade den anställde haft sitt antivirus program aktiverat hade det här kanske inte hänt.[5]

Vidare menar Cassimir Medford att Internettjänster via bredband, speciellt via kabelmodem och telefonnätet, är ökända för sina svagheter med säkerheten. Detta på grund av att de tillhandahåller en "Always on Connection" som inte är säkrad av en central brandvägg. Statiska IP adresser hjälper till att öka säkerhetshoten och skapar ett vidöppet hål för hackers.[6]

Jonathan James säger i en intervju i Mikrodatorn nr 5 2001[7] att när fler personer väljer bredbandsuppkoppling väljer de också att använda olika tjänster som kan öka risken för

[3] Joakim Bergström, "Brandväggen skyddar dig mot hackare", *PC för Alla*, nr 2 2001
[4] Cassimir Medford, "Security – You can get there fast – but is it safe?", *PC Magazine*, 6 februari 2001
[5] Ibid.
[6] Ibid.
[7] Mikael Söderlind, "Hemdatorer är intressanta för hackare" Intervju med Jonathan James", *Mikrodatorn* nr 5 2001, sid 82

intrångsförsök[8]. Exempel på sådana tjänster är webb-, FTP- och e-postserver. Enligt Jonathan James ökar säkerhetsriskerna vid användandet av dessa tjänster. Ju längre uppkopplingstiden är desto större är risken för en attack. Vid användandet av bredband tillhandahålls oftast en statisk IP adress från leverantören, till skillnad från modemuppkoppling där ny IP adress tilldelas vid varje ny uppkoppling. Detta leder till att risken är större för intrångsförsök, då samma IP-adress existerar och är åtkomlig hela tiden datorn är på. När datorn sätts på igen tilldelas datorn samma IP-adress, och det är väldigt lätt för en hacker att ta sig in i systemet igen.[9]

Om fil- och skrivardelningen är påslagen i Windows medför det enligt Brian Robinson, författare till artikeln ”low-end broadband security may need to clamp down as hackers start tearing holes in these networks”, att en hackare lättare kan ta sig in i en annan användares system Den här tjänsten har funktion enbart på ett bredbandsnät med LAN lösning, då alla i samma byggnad kan komma åt varandras filer lagrade på hårddisken. [10] LAN lösning beskrivs i Appendix A.

## VAD ÄR BREDBAND?

Enligt en definition utfärdad av regeringen är bredband ett sammanfattande begrepp för överföring av information digitalt, med överföringshastigheter på över två megabit per sekund (2 Mbit/s). Mbit/sekund innebär att överföring av data kan ske med 250 000 tecken per sekund. Ett vanligt modem klarar högst 7000 tecken per sekund[11].

Med hjälp av bredband går det att skicka stora mängder information över såväl korta som långa avstånd. Det är alltså möjligt att överföra olika typer av information samtidigt. Datorn kan till exempel vara uppkopplad mot Internet samtidigt som det är möjligt att tala i telefon. Vilken typ av information det är spelar ingen roll. Bredbandstjänster levereras antingen över fasta eller mobila data- eller telefonnätverk och kräver bredbandsanslutning. Ett bredbandsutbud är en kombination av bredbandsåtkomster och bredbandstjänster som optimerats för höghastighetsleverans, oavsett om de är integrerade eller sammansatta av flera olika leverantörer till ett komplett paket[12]. Det finns en hel del olika tekniker tillgängliga på marknaden, lösningarna skiljer sig en del åt när det gäller hastigheten och tillgängligheten, det vill säga om tjänsten erbjuds på bostadsplatsen. De vanligaste bredbandsteknikerna är Internet via kabel TV-nätet, eller via telenätet.[13] I bostadsrättsföreningar och radhusområden erbjuds även LAN lösningar.[14]

---

[8] Mikael Söderlind, ”Hemdatorer är intressanta för hackare” Intervju med Jonathan James”, *Mikrodatorn* nr 5 2001, sid 82

[9] Brian Robinson, “low-end broadband security may need to clamp down as hackers start tearinbg holes in these networks”, *Tele.Com* 26 Juni 2000

[10] Ibid.

[11] Bredband för tillväxt i hela landet, SOU 1999:85

[12] http://www.telia.se/bredband, 2001-02-20

[13] http://www.f.kth.se/~f97-ali/bredband1.pdf, 2001-02-20

[14] Se Appendix A Olika tekniker

# TEORI

## OLIKA SÄKERHETSHOT

### DATORVIRUS

I artikeln ”Viruses the generation” beskriver författaren Kim Zetter att ett virus är en bit kod, som instruerar datorn att göra något, såsom att formatera hårddisken eller kopierar sig självt tills minnet i datorn tar slut[15]. Det finns även virus som inte orsakar någon skada, utan de kan till exempel bara skriva ut ett meddelande på skärmen. Kim Zetter beskriver även ett virus med att det förökar sig självt. Det smittar systemet genom att infektera nya program, dokument eller systemfiler, på samma sätt som ett biologiskt virus förökar sig självt och attackerar organen i kroppen. Vidare berättar Kim Zetter att när ett virus väl har infekterat filerna kan dess effekt visas när som helst. En del virus är datum styrda vilket innebär att dess effekt visas vid ett specifikt datum. Andra virus kan visa sin effekt när till exempel ett Word dokument öppnas.[16] Olika virusformer beskrivs i Appendix B.

Virus kan spridas antingen via e-post eller med externa medier, såsom disketter, cd-skivor och zip-skivor. Viruset infekterar inte datorn förrän den smittade filen öppnas. Detta gäller oavsett om viruset finns som en bifogad fil till ett e-brev eller på en diskett. Oftast har ett virus som anländer vi e-post, något konstigt namn eller filändelsen till exempel .EXE eller .VBS. [17]

Enligt Cassimir Medford har virusattacker ökat explosionsartat de senaste åren. 1993 fanns det 3200 kända virus runt om i världen. Idag finns det mer än 40 000 kända virus, där 200-300 är aktiva. Mellan sex till tolv nya virus uppkommer varje dag.[18] Förr tog det månader eller år för ett virus att spridas, medan det idag sprids på endast ett par minuter via e-post. Två exempel på hur virus kan spridas över hela världen på ett par dagar är de kända visrusen LoveLetter och Melissa. På kort tid orsakade dessa virus stora skador hos datoranvändare världen över.[19] I samband med det ökade antalet virus och de intrång som begås idag är enligt Mary Mosquera brandväggar och antivirusprogram de bästa metoderna mot Internet relaterade hot.[20]

---

[15] Se Appendix B Olika virusformer
[16] Kim Zetter, “Viruses the generation”, *PC World*, December 2000
[17] Ibid.
[18] Kim Zetter, “Viruses the generation”, *PC World* , December 2000
[19] Se Appendix C LoveLetter viruset
[20] Mary Mosquera, ”Vigilance is key to Security, Experts say”, *Techweb*, 2001

## HACKNING

En hackare är en människa som olovligt tar sig in i datorsystem. Detta är den generella bilden av en hacker idag. Tidigare var definitionen av en hacker, en person som var duktig på programmering och som höll på att ”hacka” på tangentbordet. Olika beskrivningar av hackers återfinns i Appendix D.

Det finns olika sorters hackningattacker eller intrångsförsök beroende på vad hackaren är ute efter. Om hackarna är ute efter att samla in hemliga uppgifter eller förstöra dem kan de använda sig av en direkt attack eller en trojansk häst.[21] Är hackaren ute efter att förstöra till exempel slå ut en Webbplats eller en e-postserver kan hackaren använda sig av indirekta attacker.[22]

### *DIREKTA HACKNINGATTACKER*

Direkta hackningattacker innebär att hackaren tar sig in i systemet antingen med hjälp av att lösenord knäcks, stjäls eller genom att ett säkerhetshål i en programvara eller operativsystem utnyttjas. Det som skiljer en direkt attack från en indirekt attack är att med den direkta attacken är hackaren ofta ute efter att stjäla data eller för att förstöra, medan en indirekt attack ofta innebär att hackaren vill slå ut en viss tjänst. Ett sätt för an hacker att ta sig in i systemet är att hackaren skickar in en trojansk häst via e-post, som sedan ligger och sniffar trafiken efter kontonamn och lösenord. Hur en Trojansk häst fungera beskrivs nedan.

Ett program för att knäcka lösenord är L0phtCrack från LHI Technologies. Programmet har en inbyggd SMB paket sniffare som kan snappa upp krypterade lösenord när de färdas över nätet. Hackaren kan sedan i sitt egna system och knäcka lösenorden med hjälp av programmet. Programmet kan också användas för att kontrollera att det egna lösenordet inte är lätt att knäcka.[23]

### *INDIREKTA HACKNINGATTACKER*

Som nämnts tidigare i uppsatsen är det som utmärker en indirekt hackningsattack att hackaren inte är ute efter att förstöra information utan att förstöra för företag och för kunderna som vill använda sig utav deras tjänster. Det kan till exempel vara att hackarna förstör för människor som vill koppla upp sig mot Internet genom att de sänker Internetleverantörens router.

En vanlig form av indirekt hackningsattack innefattar användandet av en trojansk häst. En trojansk häst anländer oftast förklädd som något annat såsom en skärmsläckare eller ett spel. När spelet startas installeras den trojanska hästen i bakgrunden, vilken kan ha olika funktioner. Den kan den tillåta någon annan att ta kontrollen över systemet men

[21] Se Appendix D Olika hacker metoder
[22] Ibid.
[23] Crume, Jeff. *Inside Internet Security What hackers don't want you to know.* (Edingburgh:Addison-Wesley, 2000), 154

den kan också lagra intressant data såsom lösenord och användarnamn i en fil som sedan i smyg skickas iväg till avsändaren av den trojanska hästen via e-post.

Det finns många olika sätt att utföra indirekta hackningsattacker på. De vanligaste tillvägagångssätten beskrivs Appendix D.

# SÄKERHETSLÖSNINGAR

## BRANDVÄGGAR

En brandvägg är i datortermer en enhet som skyddar det lokala nätverket ifrån utomstående nätverk, såsom Internet. För att kunna komma ut på Internet måste all datatrafik passera genom brandväggen, likaså gäller för all trafik från Internet in mot det lokala nätet.

All trafik som passerar brandväggen kontrolleras och bara den godkända trafiken tillåts passera brandväggen. Konfigurationen av brandväggen är viktig. I tidningen ”Pc för alla” berättar Per Albinsson att det inte är alldeles enkelt att konfigurera en brandvägg så att den ger ett bra skydd, den bör kunna konfigureras så att en logg över nättrafiken erhålls. På så sätt fungerar brandväggen som en övervakningsstation.[24]

Det skiljs på två olika modeller av brandväggar oavsett om det är en hårdvaru- eller en mjukvarubrandvägg. Dessa är Application Gateway som jobbar på applikationsnivå[25] och Packet Filtrering som jobbar på nätverksnivå[26]. Detta gäller för både mjukvaru- och hårdvarubrandväggar.

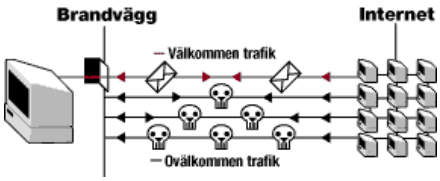


Bild 1 visar hur brandväggen filtrerar bort ovälkommen trafik. Bilden kommer från Tidningen PC för Allas webbupplaga.[27]

### *HÅRDVARUBRANDVÄGG*

Det skiljs också på hårdvarubrandväggar och mjukvarubrandväggar. De fungerar på samma sätt. All trafik filtreras genom brandväggen utefter de regler som är uppsatta. I en hårdvarubrandvägg ligger reglerna integrerade i chip. Hårdvarubrandväggen är inte beroende av något ytterligare operativsystem, eftersom det finns integrerat i chipen. Hårdvarubrandväggar är designade för att hantera mycket mer trafik än mjukvarubrandväggar. De är också snabbare och säkrare eftersom det integrerade operativsystemet ofta inte har lika många säkerhetshål som de operativsystem som används i mjukvarubrandväggar.[28]

---

[24] Snöbohm, Gustaf, ”Brandväggar – syfte, brister och hur kontrollerar man säkerheten”, Skövde: Skövde Högskola, Institutionen för datavetenskap, 1998,
[25] Se Appendix E Application Gateway
[26] Se Appendix E Paket Filtrering
[27] Joakim Bergström, http://pcforalla.idg.se/brandvaggar/hackarestal.htm, 2001-04-01
[28] Mikael Söderlind, ”Hemdatorer är intressanta för hackare” , *Mikrodatorn* nr 5 2001, sid 82

### *MJUKVARUBRANDVÄGG*

Det finns olika sätt att installera en mjukvarubrandvägg på. Tre olika sätt beskrivs i Appendix E. Det som utmärker en mjukvarubrandvägg från en hårdvarubrandvägg är att den kan installeras på en PC med ett vanligt operativsystem såsom Linux, Windows eller Unix. För att den skall fungera som en brandvägg krävs det att minst två nätverkskort finns installerade. Om en brandvägg skall konfigureras att tillåta rätt sorts trafik och stänga ute all oönskad, måste regel filer skrivas som används utav operativsystemet. Till vissa av operativsystemen finns det både gratisprogram att ladda ner från Internet och betalprogram att köpa för att grafiskt bestämma reglerna. Fördelen med att använda ett grafiskt program för att bestämma reglerna är att det är enklare än att skriva egna regler filer. En mjukvarubrandvägg: s uppgift är att skydda en eller flera bakomliggande datorer [29]

#### *PERSONLIG BRANDVÄGG*

En annan form av mjukvarubrandväggar som har blivit populära är de personliga brandväggarna. En personlig brandvägg är ett extra program som installeras lokalt på datorn ovanpå det vanliga operativsystemet. Reglerna för trafiken är redan definierade och användaren kan och behöver endast göra minimala inställningar själv. Den personliga brandväggen skyddar enbart den datorn det installerat på.[30]

### *VARFÖR BRANDVÄGG?*

Syftet med att installera en brandvägg är nästan alltid att skydda den enskilda datorn eller ett privat nätverk, mot olaga intrång, oavsett om det är en hårdvaru- eller mjukvarubrandvägg. Anledningen är att hindra obehöriga användare från att få tillgång till privat information och resurser.

På företag är det i dag vanligt med en central brandvägg. Det är en dator som alla andra datorer på företaget är ihopkopplade med. De flesta Internetoperatörer har däremot ingen central brandvägg, vilket innebär att säkerhetsansvaret läggs på dig som användare. Detta beror på att en brandvägg inte bara skyddar utan också kan skapa vissa problem för användarna att ta sig ut på nätet. Eftersom användare använder sig av Internet på olika sätt kan brandväggen bli mer av ett hinder än ett skydd, därför överlämnas säkerheten åt användaren. [31]

Enligt Tom Powledge, produktchef för Norton Internet Security på Symantec ger dagens personliga brandväggar ett bra skydd mot direkta hackningsattacker, däremot ger de personliga brandväggarna inget bra skydd mot trojanska hästar. Anledningen till detta är att de personliga brandväggarna är förinställda på att låta vissa program kommunicera

[29] Mikael Söderlind, ”Hemdatorer är intressanta för hackare” , *Mikrodatorn* nr 5 2001
[30] Ibid.
[31] Joakim Bergström, http://pcforalla.idg.se/brandvaggar/hackarestal.htm, 2001-04-01

mot Internet. Vidare menar Tom Powledge att om komplettering görs med antivirusprogram förhöjs säkerheten avsevärt.[32]

Virus är en annan aspekt än trojanska hästar som brandväggar inte ger något tillfredsställande skydd emot. Komplettering av ett fullgott antivirusskydd bör därför alltid göras.[33] Detta gäller i första hand de personliga brandväggarna, eftersom de installeras och exekveras på den lokala datorn och dess operativsystem.

## ANTIVIRUSPROGRAM

Antivirusprogram som även kallas skanningprogram letar efter virus på två sätt. Det ena sättet är att antivirusprogrammet letar efter virusets signatur[34] i viruslistan. Viruslistan innehåller namnen på de virus som är kända för företagen som utvecklar antivirusprogrammen. Om viruset finns med i antivirusprogrammens viruslistor finns det oftast ett botemedel mot viruset. När viruset hittats sätts botemedel in mot viruset och den infekterade filen desinfekteras.

Det andra sättet är att antivirusprogrammet utför en s.k. heuristisk skanning. En heuristisk sanning utförs för att leta efter virus som inte finns med i antivirusprogrammens viruslistor. En heuristisk sanning går till så att antivirusprogrammet letar efter misstänkta virusaktiviteter. När virus hittats sätts det i karantän för att det inte ska fortsätta att smitta systemet. Beroende på hur konfigurationen av antivirusprogrammet ser ut tas viruset bort eller frågar användaren vad som skall göras med viruset. Alla virus går ej att bota utan de filer som blivit infekterade måste tas bort från systemet.[35]

### *VARFÖR ANTIVIRUSPROGRAM?*

Antivirusprogram bör installeras, dels för att det framför allt skyddar mot virus, dels för att det i kombination med en brandvägg även skyddar systemet mot trojanska hästar. Mary Mosquera anser att en kombination av antivirusprogram och personlig brandvägg ger det bästa skyddet för ett enskilt system.[36]

---

[32] Artikel Effective Freeware Firewall, Computerselect Web 2001-01-19, Jim Boyce
[33] http://www.dsv.su.se/~e-holm/brandv.htm 2001-03-27, Olika brandväggskonfigurationer
[34] En unik sträng med bytes som identifierar viruset, likt ett fingeravtryck.
[35] Kim Zetter, ”How Antivirus Software Works”, *PC World*, 13 Oktober 2000
[36] Mary Mosquera, ”Vigilance is key to Security, Experts say”, *Techweb*, 2001

# INTERVJUER

Intervjuerna presenteras så att det inte framgår vilket företag som har sagt vad.

Inget av de intervjuade företagen tillhandahåller idag någon form av säkerhetslösning såsom brandvägg eller viruskontroll som kontrollerar trafiken för alla användare. Hos företag B finns det möjlighet att köpa personlig brandvägg och antivirusprogram för en mindre summa. Företag C erbjuder gratis nerladdning av en personlig brandvägg.

Företag B anser att deras säkerhetslösning som erbjuds är väldigt säker och företag C anser att deras säkerhetslösning är så säker den kan vara. Alla företagen rekommenderade både personliga brandväggar och antivirusprogram om kunden själv frågade efter det. Inget utav företagen informerar om riskerna vid användandet av bredband. Kunderna kan själva ta reda på riskerna på företag A, B och C webbplats. Hos företag D får kunderna information i samband med tecknande av abonnemang.

Alla företagen erbjuder teknisk support där kunderna kan få rekommendationer om lämpliga säkerhetslösningar. Företag B erbjuder även support vid nyinstallation av program där den tekniska supporten hjälper till med konfiguration av program.

Vid frågan om företagen tillhandahåller dynamisk eller statisk IP-adress var det endast företag B som tillhandahöll statisk IP-adress. Giltighetstiden på den dynamiska IP-adressen skiljer sig åt mellan företagen. Hos företag A är giltighetstiden tre till fyra dagar, hos företag C är giltighetstiden en till två dagar.

Tre av fyra företag anser att det bästa sättet deras kunder kan skydda sig på är att skaffa sig kunskap om hoten samt att skaffa sig rutiner för hanteringen va e-post.

# TESTER

Testerna presenteras så att det inte framgår vilka personer det är som har sagt vad.

Majoriteten av testpersonerna tyckte att programmen var lätta att installera, en person tyckte att Tiny Personal Firewall var svår att installera. Två personer tyckte att Sygates gränssnitt var lättast att förstå, en tyckte att ZoneAlarms var trevligt och en tyckte att Tiny Personal Firewall gränssnitt var rörigt. Av antivirusprogrammen tyckte de flesta att Panda antivirus gränssnitt var lättast att förstå. Det tyckte att InoculateIT var rörigt och vCatch gränssnitt var väldigt svårt att förstå.

De meddelande rutor som kommer upp tyckte de ovana användarna var svåra att förstå. Brandväggarnas hjälpfunktion var i regel ganska lätt att förstå. ZoneAlarms hjälp var lättast, där behövdes det bara klicka på ikonerna för att få upp det relevanta hjälpavsnittet. Hos antivirusprogrammen fungerade hjälpfunktionen lika bra hos alla programmen. De brandväggar som enligt testpanelen var bäst var Sygate och ZoneAlarm. Och de antivirusprogram som testpanelen föredrog var Panda antivirus.

Att administrera programmen det vill säga att göra rätt inställningar så att programmen ger så hög grad av skydd som möjligt tyckte majoriteten av testdeltagarna var svårt.

# GENOMFÖRANDE

## TESTER

För att få ytterligare information för att kunna svara på frågeställningen har tester utförts. Syftet med testerna var att få fram hur lätt det är att installera och administrera personliga brandväggar och antivirusprogram.

Testpanelen bestod utav fem personer. De valdes slumpmässigt ut efter deras datorvana. Tre av testdeltagarna hade liten datorvana och två stycken hade mycket datorvana.

Ett kriterium som testprogrammen var tvungna att uppfylla var att de kunde laddas ner gratis från Internet. Programmen som valdes ut har laddats ner från *www.download.com* . Sökorden som använts är ”firewall” och ”antivirus”. Mjukvarukraven som ställdes på testprogrammen var att de skulle fungera under operativsystemet Windows. Samtliga tester utfördes på en PC med en AMD Athlon processor på 900 MHz, 256 MB internminne, 30.7 GB hårddisk, Geforce 2 MX grafikkort och ett 3Com nätverkskort. Operativsystemet som var installerat var Microsoft Windows Millenium.

De personliga brandväggar som användes i testet var ZoneAlarm 2.6, Tiny Personal Firewall 2.0.13 och Sygate Personal Firewall 4.0. Vid användning av en uppkoppling på 56 kbps tog det cirka 6 min att ladda ner ZoneAlarm 2.6, cirka 3 min att ladda ner Tiny Personal Firewall 2.0.13 och cirka 8 min att ladda ner Sygate Personal Firewall 4.0.

De antivirusprogram som användes i testet var InoculateIT Personal Edition 5.2.9, vCatch Virus Catcher 3.5.2.8 och Panda Antivirus Platinum 6.23. Vid användning av en uppkoppling på 56 kbps tog det cirka 9 min att ladda ner InoculateIT Personal Firewall 5.2.9, cirka 2 min att ladda ner vCatch Virus Catcher 3.5.2.8 och cirka 28 min att ladda ner Panda Antivirus Platinum 6.23.

De fick börja med att installera programmet samtidigt som de svarade på frågor med anknytning till installationen. Alla i testpanelen fick svar på samma fördefinierade frågor. Därefter fick de ”lära känna” programmet en stund för att kunna svara på de frågor som gällde administrationen av programmet. Olika inställningar prövades för att se vilken effekt de hade.

# INTERVJUER

Intervjuerna genomfördes för att få reda på Internetleverantörernas informationsgrad om hoten som finns vid användandet av bredband gentemot sina kunder. Samt om de erbjuder några former av säkerhetslösningar mot hoten. Den intervju metod som användes i uppsatsen var en kvantitativ metod. En kvantitativ metod innebär att det som studeras kan göras mätbart och resultatet kan presenteras numeriskt.[37]

Företagen valdes ut till intervju beroende på vilken sorts bredbandslösning de tillhandahöll samt att de var kända för författarna. De personer som intervjuades var kunniga inom ämnet och valdes ut av företaget själv. Intervjuerna genomfördes per telefon där samma ställdes till dem som intervjuades. De tog mellan tio till tjugo minuter att genomföra.

# LITTERATURSTUDIER

Den stora mängden information som uppsatsen bygger på har samlats in från böcker som kan återfinnas på bibliotek och från granskade artiklar. Artiklarna återfinns i ComputerSelectWeb: s databaser. Böckerna valdes ut efter titelns, och innehållets relevans till ämnet. Litteraturen lästes igenom noga och den mest innehållsrika valdes ut.

Sökorden som användes vid artikelsökning var ”Virus”, ”Antivirus”, ”Firewall”, ”Security”, ”Antivirusprograms how it works”, ”How firewalls work”, ”Hacking”, ”Hacking + firewall”, ”Hackers”, ”Broadband”, ” Security for homeusers”, ”Firewall + personal”, ”Firewall + hardware” och ”Hackingattacks”

[37] http://www.masda.vxu.se/~per/Exjobb/R99-14.pdf, 2001-05-23, Metodbeskrivningar

# ANALYS

Hoten som finns i dagens läge mot bredbandsuppkopplade privatpersoner är olika former av virusattacker och intrångsförsök men Jonathan James menar att bredbandet i sig också kan vara ett hot. Med bredband blir uppkopplingstiderna längre och därmed ökar också riskerna för intrång. Förutom att människor är uppkopplade längre med bredband kan även en eventuell hacker ladda hem information snabbare.

Enligt Cassimir Medford ökar även riskerna för intrång då statiska IP-adresser används. Då en statisk IP-adress används tilldelas datorn samma IP-adress varje gång den kopplas upp mot Internet. Ju längre en dator har samma IP-adress desto lättare är det för en hackare att hitta samma dator på nytt. Intervjuerna visar på att Internetleverantörerna är medvetna om det här och tre av fyra företag tilldelar därför sina kunder dynamiska IP-adresser. Men intervjuerna visar också att även om dynamiska IP-adresser erhålles är de giltiga mellan ett till fyra dygn.

Enligt Cassimir Medford är Trojanska hästar vanligare former av intrång mot privatpersoner än direkta attacker. Detta påvisas i utredningen då en trojansk häst kan installeras i system enbart genom att en webbsida besöks. En anledning till att många intrång förekommer kan bero på privatpersoners dåliga kunskap och medvetenhet. Intervjuerna som genomförts visar på att inget utav Internetleverantörerna informerade kunderna om hoten och att det finns lösningar att tillgå om de inte självmant bad om den. Detta leder till att privatpersoner är uppkopplade mot Internet utan någon som helst kunskap om riskerna som finns. Tom Powledge och Mary Mosquera anser att en brandvägg är den bästa lösningen mot Trojanska hästar och intrång. Tom Powledge menar att om både ett antivirusprogram och en brandvägg används är risken för intrång inte så stor. Resultaten av intervjuerna visar att Internetleverantörerna själva anser att kunskap om hoten och egna rutiner för e-post hantering är ett bra sätt att skydda sig på.

Testerna visar att det inte är alldeles lätt för en person med liten datorvana att administrera de personliga brandväggarna, detta styrks utav Per Albinsson som menar att det inte är alldeles lätt att konfigurera en brandvägg på ett korrekt sätt. Vidare menar han att om den inte konfigureras på ett korrekt sätt ger den inte ett fullgott skydd. Testerna visar att ett enklet gränssnitt spelar stor roll för ovana datoranvändare. De program som testpanelen föredrar har enligt dem ett enkelt gränssnitt. Det finns olika sorters brandväggar hårdvaru- och mjukvarubrandväggar. En hårdvarubrandvägg lämpar sig bäst vid stor trafiklast och den är även snabbare än mjukvarubrandväggar, men kräver mer kunskap för att administreras på ett korrekt sätt. En personlig brandvägg lämpar sig bättre för privatpersoner eftersom reglerna redan är definierade.

Virus är ett hot som finns oavsett vilken Internetuppkopplingsmetod som används, det för att virus kan spridas via disketter, cd-skivor och via e-post. Enligt Kim Zetter kan virus spridas på bara några minuter vi e-post, eftersom det oftast skickar sig självt vidare

till alla adresser i adressboken, och därför är det ett allvarligt hot mot alla som använder e-post. Mary Mosquera anser att antivirusprogram är den bästa lösningen mot virus.

# RESULTAT

## SÄKERHETSHOT

Efter att en analys har gjorts har det framkommit att de säkerhetshot som finns för privatpersoner vid användandet av bredband är olika sorters intrångsförsök och virusattacker.

Ett intrång i ett datorsystem är när någon olovligt tar sig in i ett datorsystem. Det finns olika sorters intrångsförsök det vill säga direkta hackningattacker och indirekta hackningsattacker beroende på vad hackaren är ute efter. Den vanligaste formen av en indirekt hackningattack är trojansk häst. En trojansk häst ett är ett program som är utklätt till något annat till exempel ett spel.

Virus är inte bara ett hot då bredbandsuppkoppling används utan för alla som använder sig av Internet. Ett virus är en bit kod som instruerar en dator att göra något. Det finns olika sorters virus. Vissa virus kopierar sig självt och tar upp all plats i minnet. Andra förstör vissa speciella filer och skickar iväg sig självt via e-post till alla i adressboken i e-postprogrammet. Genom att de skickar iväg sig självt till alla i adressboken sprids virus otroligt snabbt. Virus sprids även via externa medier såsom disketter, CD-skivor och zip-skivor.

Användandet av Internet i sig är ett hot. Vid användandet av bredband blir uppkopplings tiderna längre vilket ökar säkerhetsrisken. En statisk IP-adress ökar hoten ytterliggare. Ju längre en och samma IP-adress användes desto längre tid har en hackare på sig att försöka ta sig in. i samband med bredbands användandet ökar även användandet av tjänster som FTP, e-post-servrar och webb servrar vilket också leder till minskad säkerhet.

## SÄKERHETSLÖSNINGAR

De säkerhetslösningar som framkommit under utredningens gång är brandväggar och antivirusprogram.

Brandväggar används för att stoppa intrång. De fungerar så att all trafik som passerar brandväggen kontrolleras och endast den godkända trafiken tillåts passera. Hårdvarubrandväggar är designade för att hantera mycket trafik. De är inte beroende av något externt operativsystem och har reglerna integrerade i chipen. De är också snabbare och säkrare än mjukvarubrandväggar eftersom det integrerade operativsystemet ofta inte har lika många säkerhetshål som de externa operativsystem som används i

mjukvarubrandväggar. I mjukvarubrandväggar finns reglerna definierade i filer till skillnad från hårdvarubrandväggar.

En personlig brandvägg lämpar sig bäst för användning av privatpersoner då de är lättare att administrera eftersom endast minimala inställningar behöver göras. Personliga brandväggar används då det bara är en dator som ska skyddas.

Antivirusprogram skyddar systemen mot virus. Men i kombination med en brandvägg skyddas systemen även mot Trojanska hästar. Programmet skannar systemet i jakt på virus. Programmen använder sig av två olika metoder för att leta efter virus beroende på om viruset är känt eller inte. Om det är känt finns det med i antivirusprogrammets viruslista och då letar den efter virusets signatur. Om viruset inte är känt letar programmet efter virusaktiviteter i systemet.

Genom att skaffa sig kunskap om hoten och rutiner för till exempel e-post hantering har början till ett gott skydd uppnåts.

## SLUTSATS

*Vad finns det för säkerhetshot mot privatpersoner?*

Det säkerhetshot som finns är olika former av virus och intrång. Den vanligaste formen av intrång mot privatpersoner är trojanska hästar. Ett stort hot med virus är att det sprids väldigt fort via e-post.

*Vad finns det för skydd mot dessa hot?*

De skydd som finns mot virus är antivirusprogram. Mot intrång är brandväggar det bästa skyddet. En kombination av ett antivirusprogram och en brandvägg ger ett bra skydd mot trojanska hästar. Kunskap om hoten och rutiner för till exempel e-post hantering ger ett bra skydd.

*Vilka säkerhetslösningar är mest lämpliga?*

De lösningar som är mest lämpliga för privatpersoner med liten datorvana är att installera ett antivirusprogram samt en personlig brandvägg. Säkerhetsprogram med enkla gränsnitt är de mest lämpliga säkerhetslösningarna för ovana datoranvändare.

# SLUTDISKUSSION

Med tanke på de många Internet relaterade hot som beskrivits i utredningen anser vi att alla Internetleverantörer borde erbjuda någon form av central säkerhetslösning. Anledningen till att de inte erbjuder någon sådan lösning är att det kan vara väldigt dyrt och svårt att konfigurera brandväggen så att den passa alla kunders behov samtidigt som den ska behålla hög säkerhetsnivå. Under intervjuerna framkom det att just säkerheten är ett viktigt ämne för Internetleverantörerna. Ett långsiktigt mål skulle kunna vara att Internetleverantörerna erbjuder både en personlig brandvägg och ett antivirusprogram vid tecknande av abonnemang. Eftersom det idag finns Internetleverantörer som kan erbjuda detta tror vi inte att kostnaden blir så stor för företagen. De företag som erbjöd säkerhetslösningar ansåg att de var väldigt säkra. Tidigare i uppsatsen har det kommit fram att brandväggarna endast ger hög grad av säkerhet om de är konfigurerade på rätt sätt. Våra tester visade att för ovana datoranvändare var det inte helt enkelt att konfigurera. En stor del av detta problem tror vi skulle kunna lösas om det fanns säkerhetsprogram på svenska. Detta skulle underlätta både installation och konfiguration samt att säkerhetsgraden skulle kunna ökas.
De här kommentarerna framkom under våra tester:

*”Överhuvudtaget svåra att förstå eftersom jag inte är van”*
*”Visste inte vad de handlade om”*
*”Kanske hade varit lättare om de hade varit på svenska”*

Under intervjuerna framkom det att inget utav de intervjuade Internetleverantörerna självmant informerade kunderna om riskerna vid användandet av bredband. På majoriteten av Internetleverantörernas webbplatser finns det information om hoten men i vissa fall var den väldigt svår att hitta vilket kan leda till att kunderna i sämsta fall aldrig får informationen. Som lösning på det här problemet anser vi att de borde skicka med information vid tecknande av abonnemang. Sedan är det upp till kunden att ta till sig den.

Vi tycker det är bra att majoriteten av Internetleverantörerna erbjuder dynamiska IP-adresser, det hade varit bättre om de bara var giltiga i ett dygn och inte som idag upp till fyra dygn.

Enligt Kim Zetter är medvetenheten om hot och kunskapen om hur man skyddar sig viktigt.[38] Är man bara medveten om att hoten finns, då har man redan en ganska hög säkerhetsgrad anser vi.

I framtiden skulle utredningen kunna utökas med en kvantitativ undersökning där det undersöks i hur stor utsträckning privatpersoner med bredband skyddar sig samt vilken kunskap de har om hoten och säkerhetslösningarna.

[38] Kim Zetter, “Viruses the generation”, *PC World*, December 2000

# ORDLISTA

| | |
|---|---|
| **Always on Connection** | Always on Connection innebär att man är uppkopplade hela tiden |
| **Applikation** | Ett tillämpningsprogram |
| **Bit hastighet** | Hur många tecken som kan skickas per sekund |
| **Bootsektor** | Den del på hårddiken där information står som behövs vid start av datorn |
| **Broadcast** | Information som skickas till alla datorer i ett nätverk |
| **Chip** | kiselbricka som finns i olika typer av integrerade kretsar |
| **Dator trafik** | Informationen som färdas mellan datorer |
| **Fildelning** | Filer som ligger på hårddiskar kan delas ut i ett Windows nätverk, så att andra kan komma åt dem |
| **FTP** | Protokoll för att överföra filer |
| **Gränssnitt** | Det som möjliggör kommunikation mellan människa och dator och utgörs bl.a. av det man ser på bildskärmen |
| **Hårddisk** | Benämningen gäller en minnesenhet som består av en skiva där informationen lagras magnetiskt. I persondatorer är hårddisken vanligen fast inbyggd |
| **Hårdvara** | Datorutrustningens hårda delar såsom tangentbord, hårddisk, grafikkort, bildskärm och mus |
| **Internminne** | Internminnet kan som regel inte behålla informationen när datorn är avstängd, men det är snabbt och därför lämpligt att använda under bearbetningen |

| | |
|---|---|
| **IP-adress** | IP-adress, en typ av numerisk adress som datorer använder när de kommunicerar med varandra över nätverk. Exempel: 130.237.222.66. |
| **Klient** | En vanlig användardator som kommunicerar med en server och utbyter data |
| **Konfiguration** | Inställningar, att konfigurera är att göra inställningar i program |
| **Logg** | En fil där händelser som har utförts på systemet sparas |
| **Mjukvara** | Datorprogram såsom Windows, Word och Excell |
| **Nätverk** | Datorer som är ihopkopplade med varandra för att kunna kommunicera kallas ett nätverk. Det mest kända nätverket är Internet. |
| **Paket** | Informationen som skickas mellan datorer går i paket. |
| **Protokoll** | Det "språk" som datorer använder för att kommunicera med varandra |
| **Server** | Dator som tillhandahåller gemensam servicefunktion i ett datornät, t.ex. datalagring och e-postkommunikation |
| **Session** | När två datorer kommunicerar med varandra startar de en session |
| **Skrivardelning** | Skrivare kan delas ut på nätverket, så att flera användare kan dela på en central skrivare |
| **Systemkrasch** | Om internminnet i datorn fylls kan det orsaka en systemkrasch och datorn stängs av |
| **Säkerhetshål** | Fel i program som gör att någon kan ta sig in i systemet med hjälp av felet |
| **TCP/IP** | Protokoll för överföring av data |

| | |
|---|---|
| **Telnet** | Program för fjärrinloggning, d.v.s. det går att logga in på en dator oberoende vart din dator befinner sig bara det finns en Internetuppkoppling |
| **VBA** | Visual Basic for Application |
| **ZIP-Skiva** | Annat sätt än disketter för lagring av information magnetiskt. Rymmer 100 eller 250MB |

# KÄLLFÖRTECKNING

## TRYCKTA KÄLLOR

Borgström, Håkan. *Säkerhet i lokala datornät*. Stockholm: Affärsinformation, 1993.

Bredband för tillväxt i hela landet, SOU 1999:85

Crume, Jeff. *Inside Internet Security What hackers don´t want you to know*. Edingburgh:Addison-Wesley, 2000

Bergström Joakim, ”Brandväggen skyddar dig mot hackare”, *PC för Alla*, nr 2 2001

Boyce Jim Artikel Effective Freeware Firewall, *Computerselect Web* 2001-01-19

Dalton, Curtis, ”Protect your PC-knowing your options can save you from the Internet never – do – wells”, *Network Magazine*, 2001

Medford Cassimir, “Security – You can get there fast – but is it safe?”, *PC Magazine*, 6 februari 2001

Mosquera Mary, ”Vigilance is key to Security, Experts say”, *Techweb*, 2001

Robinson Brian, “low-end broadband security may need to clamp down as hackers start tearing holes in these networks”, *Tele.Com* 26 juni 2000

Sandberg Dan, ”Varning Virus!”, *Nätverk och kommunikation*, nr 15 Oktober 2000

Söderlind Mikael, ”Hemdatorer är intressanta för hackare” , *Mikrodatorn* nr 5 2001

Zetter Kim, “Viruses the generation”, *PC World*, december 2000

Bilan Carolina, Broman Peter och Eklund Eva. ”Utredning om bredband.” Ronneby: Blekinge Tekniska Högskola, Institutionen för Programvaruteknik och Datavetenskap, 2000.

Snöbohm, Gustaf, ”Brandväggar – syfte, brister och hur kontrollerar man säkerheten”, Skövde: Skövde Högskola, Institutionen för datavetenskap, 1998,

## OTRYCKTA KÄLLOR

http://www.dsv.su.se/~e-holm/brandv.htm 2001-03-27, Olika brandväggskonfigurationer

http://www.masda.vxu.se/~per/Exjobb/R99-14.pdf, 2001-05-23, Metodbeskrivningar

www.bredbandsbolaget.se, 2001-05-21, Olika bredbands tekniker

http://www.telia.se/bvo/info/gen_info.jsp.html?OID=ADSL&CID=-23363, 2001-05-21, Olika bredbandstekniker

http://www.telia.se/bredband, 2001-02-20, Olika bredbands tekniker

http://www.f.kth.se/~f97-ali/bredband1.pdf, 2001-02-20, Bredbandsuppkopplingar

http://www.cultdeadcow.com, 2001-04-15, Cult of the Dead Cow

Anders Carlsson, ”Vem?”, Föreläsning i nätsäkerhet vid Blekinge Tekniska Högskola, Ronneby, 2001-04-27

# APPENDIX

## APPENDIX A

### KABEL TV-NÄTET

Hushåll som är anslutna till ett kabel-TV-nät kan få tillgång till höghastighetsöverföring till sin dator med hjälp av ett kabel-TV-modem. Genom modemet kan man komma upp i överföringshastigheter på upp till tio Mbit/s. Anslutningen sker direkt från datorn till kabel-TV-uttaget vilket gör att användaren kan vara uppkopplad utan att belasta det vanliga telenätet. I det här fallet ersätts det vanliga kabel-TV-uttaget med ett multimediauttag med sammanlagt tre uttag: ett för TV, ett för radio och ett för datorn. Se bild 2. Kabel-TV-modem har ingen begränsning i räckvidd, till exempel som ADSL-teknik kräver att man måste bo inom ett visst avstånd till en telestation. Däremot påverkas hastigheten av hur många användare som samtidigt utnyttjar kabel-TV-anslutningen eftersom användarna delar på en gemensam överföringskapacitet.[39]

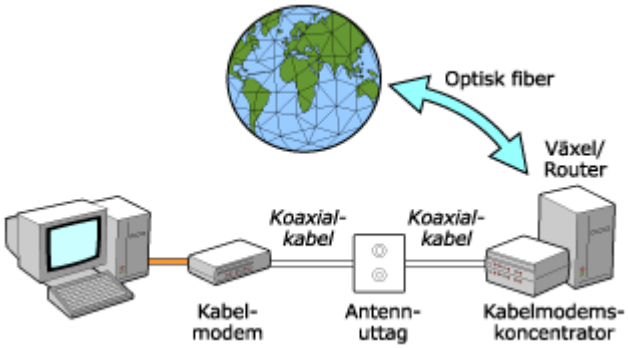


Bild 2 visar hur kabel-TV anslutningen ser ut. Bilden tagen från Bredbandsbolaget webbplats.[40]

### TELENÄTET (XDSL, ADSL, VDSL, ATM)

*XDSL*

XDSL står för Digital Subscriber Line och är ett samlingsnamn för de lösningar som använder den befintliga koppartråden i telenätet för att överföra data mellan användare och telefonstation. Användaren med DSL-teknik skickar datainformation från sin dator via telefonjacket och ett modem till telenätets närmaste station. ATM- teknik packar sedan datasignalerna och skickar dem vidare till mottagarens telestation, där

[39] Bilan Carolina, Broman Peter och Eklund Eva. "Utredning om bredband." Ronneby: Blekinge Tekniska Högskola, Institutionen för Programvaruteknik och Datavetenskap, 2000.
[40] www.bredbandsbolaget.se, 2001-05-21

informationen packas upp och skickas vidare till mottagaren med motsvarande DSL-teknik.[41]

### *ADSL*

ADSL är en teknik i DSL-familjen vars förkortning står för Asymmetric Digital Subscriber Line. Ordet "Asymmetric" antyder att kapaciteten är beroende på i vilken riktning information överförs. Med ADSL kan användaren ta emot information på upp till 8 Mbit/s och skicka information motsvarande 1 Mbit/s. ADSL använder, liksom övriga DSL-familjen, en modemteknik kopplad till det befintliga telenätet. Se bild 3. Koppartrådarna kan överföra mer information tack vare att det går att utnyttja ett högre frekvensområde för överföring. I och med att ADSL-kommunikationen sänds på en högre frekvens är telelinjen öppen även för vanliga telefonsamtal, vilka utnyttjar en lägre frekvens. Det som behövs är att telefonstationen och användaren förses med var sitt ADSL-modem och att datorn utrustas med ett nätverkskort. Med ADSL kan användare nå upp i hastigheter som tidigare varit förbehållna större företag som är anslutna med optisk fiber. För att ADSL skall komma till sin fulla rätt får det inte vara mer än tre kilometer mellan användaren och telefonstationen.[42]

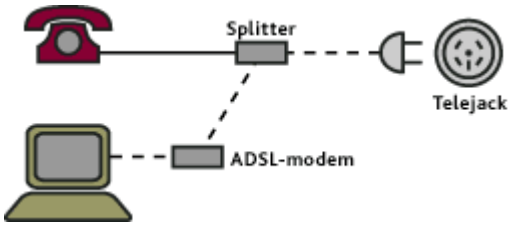


Bild 3 visar hur data trafiken skiljs från teletrafiken med ADSL uppkoppling. Bilden kommer från Telias webbplats[43]

### *VDSL*

VDSL står för Very High Speed Digital Subscriber Line och är den snabbaste lösningen inom DSL-familjen. Skillnaden mot ADSL är att VDSL utnyttjar ett ännu högre frekvensområde i koppartråden. Eftersom frekvensområdet för överföring är högt avtar signalen snabbt i styrka om den inte förstärks. Den maximala överföringshastigheten med VDSL är 50 Mbit/s vid 300 meters telefontrådslängd.[44]

---

[41] www.bredbandsbolaget.se, 2001-05-21
[42] Bilan Carolina, Broman Peter och Eklund Eva. "Utredning om bredband." Ronneby: Blekinge Tekniska Högskola, Institutionen för Programvaruteknik och Datavetenskap, 2000.
[43] http://www.telia.se/bvo/info/gen_info.jsp.html?OID=ADSL&CID=-23363, 2001-05-21
[44] Ibid.

*ATM*

ATM står för Asynchronous Transfer Mode och är en viktig beståndsdel vid bredbandig DSL överföring. ATM-tekniken sitter i telenätets telestationer och tar hand om informationen och packar den innan den sänds till mottagarens station. Med hjälp av ATM packas informationen, som skickats från användarens dator, i så kallade celler. Dessa celler adresseras och skickas sedan till den mottagande datorn. Informationen från olika källor, till exempel bild, data, tal och video, fyller cellerna allt eftersom den produceras. ATM kan jämföras med en bostadsflytt där sakerna packas i flyttkartonger. För att flytten skall gå smidigt bör paketeringen ske planerat redan från början. Porslin och glas packas i en kartong, kläder i en annan, skivor och böcker i en tredje. Fler saker får plats i flyttkartongen eftersom paketeringen sker metodiskt och därmed får även fler kartonger plats i flyttbilen. Cellstrukturen inom ATM fungerar på samma sätt. Varje "kartong" består av en cell som packas med information som skall till samma adress. Med ATM som teknisk plattform kan man hantera överföring av ljud, bild, data och video i hastigheter på upp till 155 Mbit/s.[45]

*LAN*

HusLAN (Local Area Network) kallas det lokala nätverk som de flesta företag har i sina egna datornät idag. Det är LAN som i vardagstal har kommit att kallas bredband, men det är fel. Man kan använda bredbandstekniker i LAN.

LAN är lämpligast att använda i flerbostadshus och i större bostadsområden. Varje hus bildar ett nätverk där de olika lägenheterna kedjas ihop. För det krävs det att man drar nya fiberkablar i huset och alla datorerna länkas sedan ihop med en dator som finns någonstans i huset. Från den datorn dras sedan en kabel ut ur huset och länkar ihop med nätverk från andra hus i området i en ny dator. Se bild 4. Som i sin tur länkas ihop med andra bostadsområden i en tredje dator, för att till slut kopplas ut på Internet.[46]


Bild 4 visar hur LAN koppling går igenom ett eget uttag. Bilden kommer från Telias webbplats.[47]

[45] http://www.telia.se/bvo/info/gen_info.jsp.html?OID=ADSL&CID=-23363, 2001-05-21
[46] Bilan Carolina, Broman Peter och Eklund Eva. "Utredning om bredband." Ronneby: Blekinge Tekniska Högskola, Institutionen för Programvaruteknik och Datavetenskap, 2000.
[47] http://www.telia.se/bvo/info/gen_info.jsp.html?OID=ADSL&CID=-23363, 2001-05-21

# APPENDIX B

## BOOT-VIRUS

Boot-virus lägger sig i startsektorn (boot) på en disk, hårddisk såväl som en diskett, och därmed infekteras den del av disken som startar datorn. Boot-virus är extra farliga eftersom de laddas innan operativsystemet startas. Alla media som används efter startögonblicket kan därför smittas.

## STEALTH-VIRUS

Stealth-virus är en virustyp som placerar sig själv i internminnet och läser av antivirus programmens beteende. Om antivirus programmet sedan undersöker bootsektorn skickar stealth-viruset en bild av bootsektorn som den borde se ut, istället för en som är infekterad av virus.

## LOGISK BOMB

En tredje virus typ är logiska bomber. Det är program som ligger latenta, d.v.s. vilande, tills dess att en viss händelse inträffar. Bomben kan explodera till exempel när datorn startas för femte gången eller på fredagen den 13: e. När programmet aktiveras kan det ställa till mycket oreda som till exempel att formatera hårddisken eller radera alla DLL-filer.

## MAKROVIRUS

Makrovirus är datorvirus som skrivits i makrospråk, främst VBA, för ordbehandlare eller kalkylprogram kallas för ett makrovirus. De sprids när smittade filer flyttas mellan datorer. För närvarande är de mest utsatta applikationerna Word och Excel. Många makrovirus gör inget annat än att försöka sprida sig så mycket som möjligt. Vissa kan skriva över data, modifierar dokument och en del har förmågan att sända iväg dokument via e-post. Dessa virus kan även mutera eller ändra form. Makrovirus står idag för de flesta infektionerna.[48]

[48] Dan Sandberg, ”Varning Virus!”, *Nätverk och kommunikation*, nr 15 Oktober 2000

## MASK

En mask är ett program som kopierar sig självt och på det sättet till slut äter upp tillräckligt mycket systemresurser för en systemkrasch. Skillnaden på virus och mask är att virus ändrar på systemet permanent medan masken bara förstör tillfälligt. Masken sprider sig okontrollerat till andra datorer genom att göra kopior av sig självt, vanliga virus kan inte av egen kraft sprida sig till andra datorer. [49]

[49] Dan Sandberg, ”Varning Virus!”, *Nätverk och kommunikation*, nr 15 Oktober 2000

# APPENDIX C

## MELISSA

Det första makroviruset kom till 1995. Redan 1998 fanns det mer än tusen olika makrovirus. Hastigheten som virusen spreds med berodde på hur ofta människor delade på disketter och till hur många en smittad fil skickades. Om disketten eller filen inte skickades vidare spreds inte viruset. När Melissa viruset anlände 1998 var användare ingen viktig faktor för spridning av viruset.

Melissa viruset anlände som en bifogad fil med ett e-post meddelande. Viruset skickade sig självt vidare som e-post meddelande till de femtio första kontakterna i Outlooks adressbok så fort mottagaren av e-post meddelandet öppnade den bifogade filen. Mallarna i Word påverkades så att alla därefter skapade dokument infekterades. Melissa viruset började spridas på en fredag och redan på måndagen därefter hade 250.000 datorer infekterats.[50]

## LOVELETTER

Ett år efter Melissas ankomst, dök LoveLetter viruset upp. Det spreds på samma sätt som Melissa viruset med att undantag, det skickades vidare till *alla* kontakterna i Outlooks adressbok och inte bara de femtio första.

Den tredje maj 2000 anlände LoveLetter viruset. Viruset kom ursprungligen ifrån Filipinerna. Det kom som en bifogad fil till ett e-post meddelande med titeln ”I Love You”. Utöver att hämta hem den Trojanska hästen, skickade viruset sig självt som ett e-post meddelande till alla adresserna i Outlooks adressbok, samt att viruset raderade eller skrev över alla JPEG och MP3 filer.

Den fjärde Maj 2000 klockan 07:00 fanns det motmedel tillgängliga från de flesta antivirustillverkarna, men det var redan försent, på amerikanska ostkusten hade anställda redan börjat öppna sin e-post meddelande. Klockan 16:00 samma dag kom en ny variant av LoveLetter viruset. Istället för ”I Love You” som titel på e-post meddelandet, ändrades titeln till ”Very Funny Joke”. Klockan 18:40 hade minst 20 länder rapporterat om infekterade system. Dagen efter fanns det nio olika varianter av LoveLetter viruset.[51]

[50] Kim Zetter, “Viruses the generation”, *PC World*, December 2000
[51] Ibid.

# APPENDIX D

## INDIREKTA HACKNINGATTACKER

### *DENIAL OF SERVICE*

Denial of Service (DoS) attacker är något av de simplaste attackerna som hackaren kan utföra. Till skillnad från andra mera sofistikerade attacker, innebär DoS attacker en minimal penetration av målmaskinen. DoS attacker ger inte hackaren tillträde till kritiska system, ej heller stjäler hackaren viktig information. DoS attacker går ut på att hackaren vill slå ut en till exempel Webbsida eller något annat system, och hackaren tar sig ofta in på en oskyldig användares system för att därifrån avlossa attacken och därmed har hackaren skyddat sin egen identitet.[52]

### *E-POST BOMBER*

E-post bomber är till för att slå ut e-postserver. Hackaren lyckas med detta genom att sända ett onormalt stort e-post (till exempel 10 MB) till det tilltänkta målet. Om detta upprepas tillräckligt många gånger, lyckas hackaren med att översvämma e-post systemet genom att tvinga det att använda allt sitt lediga minnesutrymme med att hålla kvar kopior av den värdelösa datan som det mottar. Effekten av detta är att stänga ut all legitim e-post till e-postservern. E-post bombning kräver väldigt lite kunskaper om hackningstekniker och de kan väldigt lätt utföras. Sådana attackerare kan också dölja sina spår genom att använda sig av så kallade ”anonyma återpostare (anonymous remailers)”. Genom att förfalska sin avsändaradress eller genom att initiera attacken från flera av de gratis e-post tjänster som finns (till exempel Hotmail, Spray m.fl.).[53]

### *SYN ATTACK*

1996 fann Panix, ett New York baserat ISP (Internet Service Provider) företag, att deras påfartsramp till ”informations motorväg (Information Superhighway)” var helt blockerad. Ingen kunde komma in eller ut från sina datorer eller nätverk. Företag, konsumenter och privatpersoner hade blivit utestängda från Internet, och ingen visste varför. Till slut lyckades källan till problemet isoleras och diagnostiseras, en hacker stod att skylla.

Hackaren utnyttjade en svaghet i TCP/IP protokollet. Under en normal TCP session uppkoppling kallad ”tre vägs handskakning”, skickar initiativtagaren ett speciellt paket vilket synkroniserar sekvensnumret som kommer att användas av sessions parterna. Detta paket kallas SYN (**SYN**chronize) paket. När mottagaren erhåller SYN paketet reserverar systemet vissa resurser som är nödvändiga under sessions uppstarten och returnerar ett SYN/ACK **(SYN/ACK**nowledgement) paket till initiativtagaren. Systemet

[52] Crume, Jeff. *Inside Internet Security What hackers don´t want you to know.* (Edingburgh:Addison-Wesley, 2000), 156.
[53] Crume, *Inside Internet Security*, 156-158

väntar sedan på svar innan det fortsätter med resten av uppstartsprocessen. Hackaren insåg att om avsändar adressen var förfalskad från det första SYN paketet med en falsk IP-adress som inte existerade, skulle det attackerade systemet stå och vänta ett bra tag och lyssna efter svar på dess SYN/ACK, innan det fortsatte.

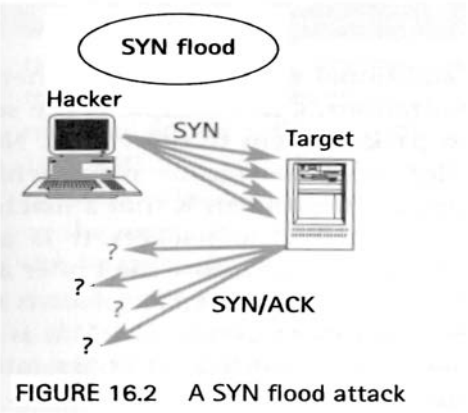

FIGURE 16.2 A SYN flood attack

Bild 5 visar en syn attack. Bilden kommer från Inside Internet Security.[54]

Eftersom det attackerade systemet hade blivit lurat att sända sin SYN/ACK till en icke existerande IP-adress, föll paketet helt enkelt ner i ett svart hål bara för att inte synas igen. Efter ett tag skulle systemet sluta vänta på svaret och frigöra de allokerade resurserna så att de kunde användas till någon annan process. Problemet var bara att väntetiden var för lång och antalet resurser allt för få. Hackaren insåg detta och skickade en flod av förfalskade SYN paket, vilka band upp alla tillgängliga resurser på systemet under en lång tid. Följderna var katastrofala för Panix och deras kunder. Tillslut togs det fram bugfixare till detta problem, men fortfarande är det långt ifrån alla som har uppdaterat sina system, eller som ens känner till att problemet existerar.[55]

### *PING OF DEATH*

Andra former av DoS attacker avslöjar fler svagheter i nätverksprotokollet eller i vanliga mjukvaror. Ett exempel är den så kallade Ping of Death attack där ett överdimensionerat paket sänds till offret. Routrar på Internet bryter ner det för stora paketet till mindre, mer lätthanterliga delar som offrets maskin lydigt sätter ihop igen i slutändan. Problemet är att en maskin som är sårbar för en sådan attack, inte inser att paketen som den sätter ihop är onormalt stora, och därför hotar att översvämma bufferten som är allokerad för att ta hand om hela processen. När det sista paketet är infångat kan maskinen komma att krascha, frysa eller starta om som en följd av attacken.[56]

[54] Crume, 159
[55] Crume, 158-159
[56] Crume, 160

*SMURF ATTACK*

En annan välkänd DoS attack involverar användandet av riktad broadcast. Med Smurf attack, exploaterar hackaren en speciell egenskap i TCP/IP protokollet, för att dirigera en flod av trafik till målmaskinen. Det fungerar så att ett Echo Request (Ping), ett oskyldigt paket för att få reda på om en maskin är levande, skickas till målmaskin. Istället för att rikta pingen till en mottagare, som de flesta Ping requests är, riktas den här till en nätadress som slutar på 0 eller 255. Detta får till följd att den vidarebefordras till alla maskiner på det nätet. Hackaren modifierar Ping paketet som sänds, så att det ser ut som om det kommer från den tänkta målmaskinen, och inte hackarens. Som en effekt av detta agerar det mellanliggande nätverket som en förstärkare för DoS attacken. Om det till exempel är tusen maskiner på det mellanliggande nätverket, kan hackaren lätt översvämma målmaskinen med enbart ett par illvilliga Ping paket, eftersom varje paket multipliceras tusenfalt. Smurf attacker kan stoppas väldigt lätt om nätverksadministratörer konfigurera routrarna så att IP-riktade broadcasts stängs av.

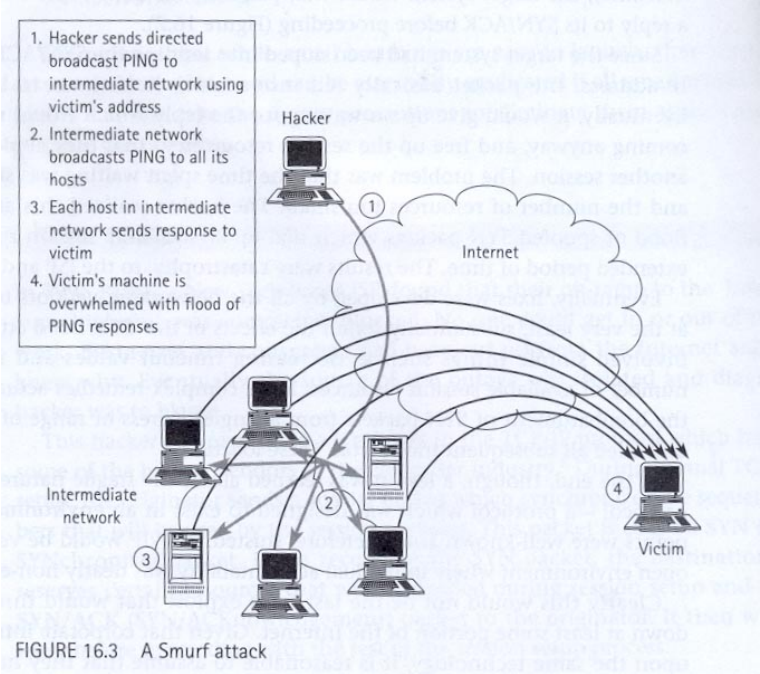

FIGURE 16.3 A Smurf attack

Bild 6 visar en smurf attack. Bilden kommer från Inside Internet Security.[57]

*TRIBE FLOODNET 2K*

Under de sista dagarna 1999 spred sig oron över TFN2K attacker som en löpeld. TFN2K kombinerade en skadande last, som utför något som förstör systemet, med en distribuerad förstärkareffekt likvärdig en Smurf attack, för att skapa en väldigt otrevlig DoS attack. Hackaren placerade först TFN2K server programvaran på de omedvetna mellanliggande datorerna, som ibland kallas ”zombies”. Sedan kunde hackaren från en klientprogramvara på sin egen dator instruera de olika TFN2K servrarna, att deltaga i

[57] Crume, 160

attacken. Resultatet blev vad som kallas en distribuerad DoS (DDoS) attack, och som inte enbart var farlig på grund av dess farliga last utan också för den stora volymen paket som genererades av de utsatta mellanliggande datorerna. Se bild 8. Det som gjorde att det var så svårt att försvara sig mot den här typen av attacker var att den kom från så många håll samtidigt.

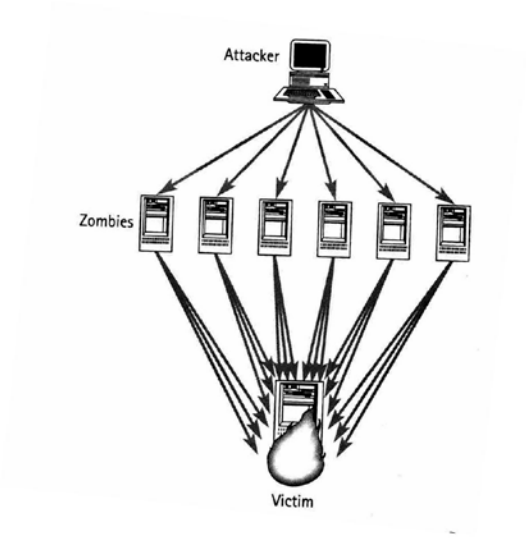


Bild 8 visar hur en Tribe FloodNet 2K utförs. Bilden är tagen från Inside Internet Security.[58]

Den förödande potentialen av DDoS attacker visade sig under en vecka i februari 2000, när några av Internets mest besökta Webbsidor attackerades av en översvämmande nätverkstrafik från många källor. Under en period av tre dagar attackerades Internets mest besökta sökmotor Yahoo, den största bokhandeln Amazon och den populära auktions sajten eBay. [59]

*TROJANSKA HÄSTAR*

Trojanska hästar har fått namnet från Iliaden och de antika grekernas försök att inta staden Troja, på 1100-talet före Kristus, genom att gömma soldater i en trä häst.

Till skillnad från virus förökar sig inte trojanska hästar utan de är en form av intrångsförsök. Det finns olika sätt för hur systemet kan infekteras av en trojansk häst, antingen kan den anlända via ett e-post meddelande, eller så kan systemet infekteras enbart genom att användaren besöker en webbsida och den trojanska hästen laddas automatiskt in i systemet. En trojansk häst anländer oftast förklädd som något annat såsom en skärmsläckare eller ett spel. Kommer den trojanska hästen via e-post kan den

[58] Crume, 162
[59] Crume, 162-163

vara svår att upptäcka eftersom den kommer förklädd som till exempel ett spel och har då ingen konstig filändelse. När programmet laddas ner i datorn kan den tillåta någon annan att ta kontrollen över systemet. Den kan också lagra intressant data såsom lösenord och användarnamn i en fil som sedan i smyg skickas iväg till avsändaren av den trojanska hästen via e-post.

På senare tid har två trojanska hästar fått mycket uppmärksamhet nämligen NetBus och Back Orifice 2000.

### *BACK ORIFICE*

Back Orifice är ett program skrivet utav Cult of the Dead Cow[60] en hackarorganisation. Back Orifice är ett sätt att göra narr av Microsofts kända Back Office svit. Back Orifice kan smugglas in genom bakdörren, av en hackare som bäddar in det i ett till synes helt ofarligt program. Allt som den ovetande personen ser kanske är en underhållande grafiksekvens eller ett spel, medan Back Orifice installeras i bakgrunden. Hackaren kan skicka programmet via e-post till många e-postadresser, och så fort någon öppnar den bifogade filen installeras programmet och skickar ett meddelande till hackaren med IP-adress på det smittade systemet., antingen via e-post eller via IRC. Back Orifice är en så kallad Trojansk Häst. Väl installerat, raderar programmet alla spår av sin existens. Till exempel i Microsofts Windows 95 eller Windows 98, syns det inte ens i listan över aktiva program som visas när tangentbordssekvensen Ctrl-Alt-Del trycks, fastän programmet faktiskt ligger och exekverar i bakgrunden. Det hackaren kan göra med Back Orifice är bland annat att övervaka alla inslagna tangenter på tangentbordet, inklusive de ”dolda” fälten som döljs av stjärnor, få upp samma skärmbild på sin egen dator som den hackade har, exekvera kommandon och program efter eget tycke, byta namn, kopiera och ta bort filer på den hackades hårddisk och koppla upp sig mot andra system via Telnet eller FTP från den hackades system. [61].

[60] cDc, www.cultdeadcow.com, Cult of the Dead Cow 2001-04-15
[61] Crume, 154-155

# APPENDIX E

## APPLICATION GATEWAY

Application Gateway kallas ibland för proxy server. En proxy server är en applikation som exekveras på en fristående dator mellan Internet och den lokala datorn. All trafik mellan Internet och den lokala datorn måste passera genom den fristående. Om användaren vill använda telnet mot en dator som befinner sig på Internet, exekveras Telnetprogrammet i själva verket på proxy servern, som i sin tur kommunicerar med datorn på Internet. För användaren blir det ingen skillnad. Om FTP server används på den lokala datorn och en dator på Internet försöker anropa den, kommer den att kommunicera med proxy servern. Datorn kommer inte att veta om det utan tror att den kommunicerar med den riktiga datorn. Proxy servern ligger helt transparent och kontrollerar allt som skickas och tas emot.

För att man skall kunna implementera en proxy server, krävs det att det finns en proxy server och en eller flera proxy klienter, som exekveras på den lokala datorn. Proxy servern ligger på en fristående dator, och proxy klienterna ligger på de lokala datorerna. En proxy klient kör en speciell version av det riktiga kommunikationsprogrammet. Detta program kommunicerar i sin tur med proxy servern istället för datorn ute på Internet. Proxy servern kontrollerar begäran och om det tillåtet, utför den själv händelsen och skickar tillbaka svaret till den berörda klienten.

En proxy server är en mjukvarulösning. Det finns olika avancerade versioner av proxy servers, vissa kan konfigureras så att till exempel FTP bara tillåts från vissa IP-adresser, andra kan inte konfigureras på det sättet. En nackdel som dock alla proxy servrar delar är att de inte är flexibla eftersom de kräver specialversioner av alla program som skall kommunicera mot Internet. De är även ganska svårinstallerade och svåra att konfigurera.[62]

## PAKET FILTRERING

Med paket filtrering analyseras all nätverkstrafik genom IP-paketen. Data behandlas på transportlagret, fjärde lagret i OSI-modellen. Varje IP-paket undersöks för att se om det matchar någon regel som definierar det tillåtna dataflödet. Om en matchande regel inte finns stoppas paketet. I annat fall släpps paketet igenom. Paradigmen för paket filtrering är: Det som uttryckligen inte är förbjudet är tillåtet. Detta därför att de flesta paketfiltrerings brandväggar implementeras på routers. En routers uppgift är att hålla kommunikationen mellan nätverk så genomskinlig som möjligt. En användare på dator A i ett nätverk som är uppkopplad mot en dator B i ett annat nätverk, genom en eller flera routers skall inte veta om hur många routers datatrafik passerar. Paket filtrering går alltså

[62] http://www.dsv.su.se/~e-holm/brandv.htm 2001-03-27, Olika brandväggskonfigurationer

ut på att oönskade tjänster stängs av i routern, detta medför att paketfiltrerings brandväggar är mycket snabba och genomskinliga för användaren.[63]

Paket filtrerings system skickar och tar emot paket mellan interna och externa datorer, men paketen väljs ut selektivt. De tillåter eller stoppar speciella typer av paket beroende på administratörens policy. Används routern som en paket filtrerings brandvägg kallas den screening router. En vanlig router tittar bara på destinationsadressen i varje paket och sänder sedan vidare paketet till den destinationsadressen. Routern fattar enbart beslut hur paketet skall behandlas grundat på destinationsadressen. Det finns två möjligheter, routern vet vart paketet skall sändas, eller så vet routern inte vart paketet skall sändas och det returneras via ett destination host unreachable meddelande. En screening router tittar lite mer noggrant på paketet och bestämmer inte bara om paketet skall skickas till sin destination utan också om paketet kan skickas. Vilka beslut routern tar bestäms av hur routern har blivit konfigurerad. En screening router kan enbart sitta mellan ett internt nätverk och Internet. Detta placerar en enorm börda på routern, inte bara behöver routern utföra alla routingbeslut utan den är även den enda säkerhetspunkten. Skulle routern sänkas av en attack exponeras hela nätverket. En screening router kan konfigureras att filtrera paket i båda riktningarna, alltså både ut mot Internet och det vanligaste från Internet mot det lokala nätverket.[64]

## SCREENED HOST

En screened host är en kombination av de båda ovanstående sätten att installera en brandvägg. Ut mot Internet sätts först en screening router upp, och innanför den sätts en applikations gateway upp som en ytterligare säkerhets aspekt. I den här konfigurationen filtreras all trafik från Internet genom screening routern och den trafik som är tillåten enligt de regler som är uppsatta, släpps igenom till applikations gatewayn. Den här typen av konfiguration medför en större säkerhet på grund av att det inte bara är en säkerhetsdetalj trafiken skall passera utan två. En nackdel med konfigurationen är att de båda komponenterna måste konfigureras så att de är samspelta och kan arbeta ihop.[65]

## PERSONLIG BRANDVÄGG

En personlig brandvägg är ett litet program som installeras på den datorn som skall skyddas. En personlig brandvägg fungerar på så sätt att programmet lägger sig mellan TCP/IP protokollet och drivrutinerna för hårdvaran i nätverksstacken. Detta gör att den blir den första och sista försvarslinjen både för inkommande trafik och för utgående. Antingen kan man låta brandväggen starta automatiskt när uppkoppling sker mot Internet, eller så kan brandväggen startas manuellt när som helst. Det första alternativet

[63] Snöbohm, Gustaf, ”Brandväggar – syfte, brister och hur kontrollerar man säkerheten”, Skövde: Skövde Högskola, Institutionen för datavetenskap, 1998
[64] Ibid.
[65] Ibid.

är att rekommendera eftersom det alltid ger ett fullgott skydd när datorn är uppkopplad. Personliga brandväggar fungerar lite olika beroende på vilken produkt som används. Vissa stänger alla portar direkt vid installation, och när applikationerna sedan försöker få tillgång till Internet, frågar programmet om det är tillåtet. Samma sak gäller om någon applikation försöker kontakta datorn utifrån. Alla intrångsförsök loggas och skrivs ofta till en fil som kan kontrolleras vid ett senare tillfälle och som kan användas vid spårning av den som utförde attacken.
Andra personliga brandväggar fungerar så att alla utgående paket kontrolleras och destinationsadressen noteras samt mottagar porten. Programmet undersöker sedan alla inkommande paket för att avgöra om paketet var begärt, annars slänger programmet det.[66]

[66] Dalton, Curtis, ”Protect your PC-knowing your options can save you from the Internet never – do – wells”, *Network Magazine*, 2001

# APPENDIX F

## OLIKA BENÄMNINGAR PÅ HACKERS

En hackare är en människa som olovlig tar sig in i datorsystem. Det är den generella bilden av en hackare idag. Tidigare var definitionen av en hackare, en person som var duktig på programmering och som höll på att ”hacka” på tangentbordet. Men under rådande omständigheter har betydelsen kommit att betyda en annan. Enligt Håkan Borgström, författaren till boken ”Säkerhet i lokala datornät” är en hackare någon som via tele- och datanät försöker komma åt otillgänglig information hos företag eller privatpersoner. Hackers kommunicerar oftast via uppringda förbindelser för att försvåra spårning av dem.[67]

### *HACKER*

En hackare är en person som vill lära sig så mycket som möjligt om datorer. Hackaren älskar att utforska brister och dolda funktioner i datorsystem för att kunna utnyttja dessa för egen vinning och få beröm från andra hackare. [68]

### *CRACKERS*

En cracker är en person som uppvisar de flesta egenskaper som man brukar förknippa med hackare med den skillnaden att en cracker inte drar sig för att elektroniskt bryta sig in i andras datorer, eller blockerar åtkomsten till dessa eller deras resurser. En del vill även förstöra de systemen som de har tagit kontrollen över. Ett vanligt sätt är att förändra webbsidor för företag.[69]

### *HEMLIGA CYBERPUNKARE*

De försvarar stridsvilligt rätten att vara anonym på nätet, rätten att skicka e-post som inte avlyssnas. De ligger ofta steget före internationell lagstiftning.[70]

---

[67] Borgström, Håkan. *Säkerhet i lokala datornät*. Stockholm: Affärsinformation, 1993.
[68] Anders Carlsson, ”Vem?”, Föreläsning i nätsäkerhet vid Blekinge Tekniska Högskola, Ronneby, 2001-04-27
[69] Ibid.
[70] Ibid.

*VIRUS CODERS*

Virus coders är de personer som skapar de självepliker ande programmen med ofarliga eller destruktiva egenskaper, som benämnes som virus.[71]

*HARD THINKERS*

Så brukar de personer kallas som hackar hårdvara. De undersöker och försöker ta sig förbi säkerhetssystem.[72]

*SPAMMERS*

Spammers e-postbombar ofta kommersiella aktörer och privatpersoner med reklam, ofta för företag inom porrindustrin. De sprider kedjebrev och reklam, men det förekommer även extremistisk propaganda.[73]

*CARDERS*

De använder sig av nätet för att sprida och utnyttja kreditkortsnummer som har stulits vid något intrång på en e-handels plats eller avlyssnat på nätet. De stjäler ofta kreditkortsnummer och utpressar sedan företaget på pengar för att inte släppa numren fria.[74]

*SCRIPT-KIDDIES*

De är ofta väldigt unga och oförstående, skolkar från skolan och har funnit sina själsfränder bland likasinnade på Internet. De saknar ofta de grundläggande kunskaperna om datorsystem och dess konstruktion. De använder sig istället utav program som erfarna crackers, coders och hackers har utvecklat. Programmen finns att ladda ner gratis från Internet. Script-kiddies samlar även på information om äldre hack, och när de hittar en dator som är sårbar för det attacksättet, försöker de med dessa äldre verktyg och metoder ta sig in. Den största faran med script-kiddies är det stora antalet och att ingen speciell kunskap behövs för att utföra attackerna.[75]

[71] Anders Carlsson, ”Vem?”, Föreläsning i nätsäkerhet vid Blekinge Tekniska Högskola, Ronneby, 2001-04-27
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.

*CYBER TERRORISTER*

Använder nätet för att skada och slå ut så mycket av samhället som möjligt. James Adams, head of Infrastructure defense, beskriver en cyber terrorist som:
*”18 åring som tillbringar 20-24 timmar om dygnet bakom datorn och får en adrenalinkick utav att ta sig in i andras datorer.”*[76]

*”Cyber terrorister blir ofta uppfångade utav den organiserade maffian eller utav andra extremistiska rörelser. De är ofta ute efter att stjäla hemligt företagsmaterial, antingen för att säljas till konkurrenter eller för att användas för utpressning.”* [77]

– Citat från Anders Carlsson, ”Vem?”, Föreläsning i nätsäkerhet vid Blekinge Tekniska Högskola.

[76] Anders Carlsson, ”Vem?”, Föreläsning i nätsäkerhet vid Blekinge Tekniska Högskola, Ronneby, 2001-04-27
[77] Ibid.

# APPENDIX G

## INTERVJUFRÅGOR

1) Tillhandahåller ni någon form av säkerhetslösningar till era kunder?

2) Informerar ni om riskerna som finns vid användandet av bredband?

3) Erbjuder ni någon form av teknisk support d.v.s. kan ni hjälpa till att hitta lämpliga lösningar?

4) Om en dynamisk IP adress tilldelas, hur länge gäller IP adressen?

5) Hur säkra är de lösningar ni erbjuder?

6) Får kunderna betala extra för dem eller ingår de i priset?

7) Rekommenderar ni era kunder att använda någon form av säkerhetslösning?

8) Vilka säkerhetslösningar anser ni att era kunder själva kan ta?

# APPENDIX H

## TESTFRÅGOR

1) Är installationen svår att förstå eller är den lätt att förstå?
2) Första intrycket av gränssnittet?
3) Är ”popup” rutorna med frågor lätta eller svåra att förstå?
4) Hur fungerar hjälpen?
5) Egna kommentarer om intrycket
6) Vilken personligbrandvägg/antivirusprogram tycker du har varit enklast och bäst, tycker du?