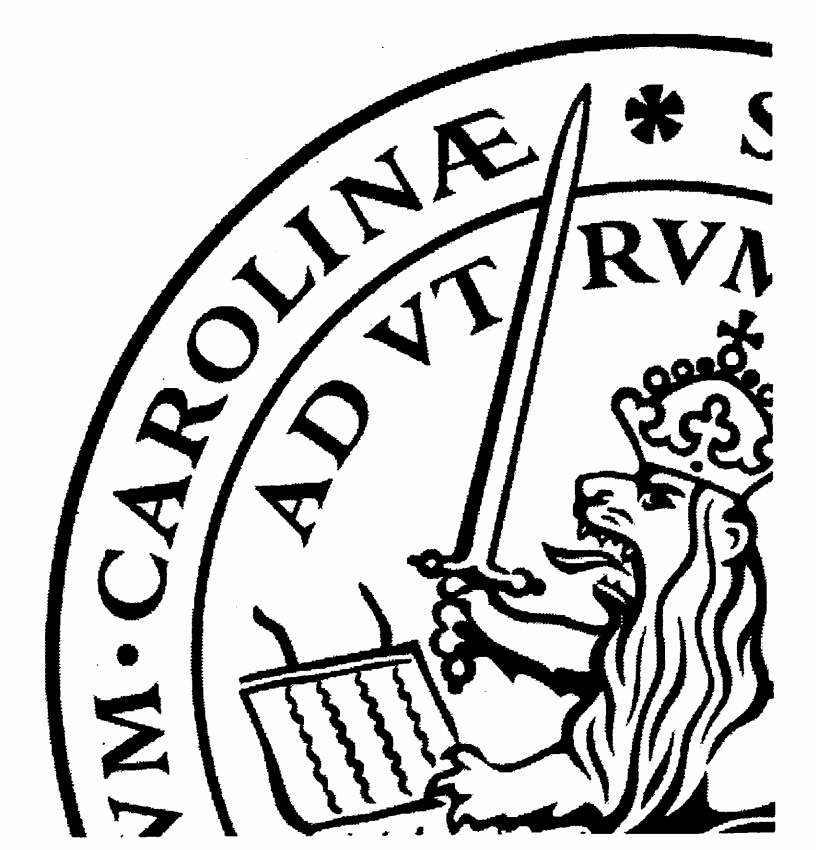
LUNDS UNIVERSITET Institutionen för Informatik

Spyware - det dolda hotet

En enkätstudie angående medvetandegraden om spyware hos hemanvändaren



Kandidatuppsats
INF 003
Våren 2005

Handledare
Anders Svensson

Henrik Isaksson 781118
Kristofer Nordin 810928

Abstrakt

Under de senaste åren har användandet av Internet ökat snabbt i världen och om man tittar på hur stor andel av befolkningen som har tillgång till Internet i hemmet är Sverige ett av de ledande länderna. Alla datorer med en uppkoppling till Internet kan bli smittade av spyware, men trots detta är inte många användare medvetna om riskerna som spyware innebär. Syftet med denna studie är att ge en bred bild av vad spyware är och vilka hot det innebär. Vidare vill vi undersöka hur medveten om dessa problem hemanvändaren är.

För att uppnå syftet har vi använt en kvantitativ metod genom att skicka ut enkäter till användare av PC-datorer i hemmet. Vi har också använt en kvalitativ metod genom att studera litteratur och artiklar för att göra kopplingarna klarare.

Spyware är program som övervakar en datoranvändares aktiviteter och fångar upp data om användaren som skickas till tredje part. Spyware varierar i design och risknivå för användaren, det finns allt från vanliga cookies till associerade cookies och applikationsbaserad spyware. Det finns flera antispywarelösningar. De vanligaste verktygen är brandväggar, antivirusprogram och antispyware-program, men en kombination av alla tre är att föredra. Ytterligare en viktig säkerhetsåtgärd är medvetande och tekniskt kunnande hos användaren.

De som framstår som mest medvetna om spyware är den grupp som använder andra webbläsare än Internet Explorer, de som någon gång har varit utsatt för spyware och yngre personer, speciellt män.

NYCKELORD: Spyware, Cookies, Hemanvändare, Skydd, Integritet

Innehållsförteckning

Figurförteckning

Tabeller

BILAGA

Förkortningar

AGPL	Affero General Public License
BBB	Better Business Bureau
DRM	Digital Rights Management
EG	Europeiska Gemenskapen
EkomL	Lagen om elektronisk kommunikation
ELIN	Electronic Library Information Navigator
EU	Europeiska Unionen
EULA	End User License Agreement
EXE	Executable
GUID	Globally Unique Identifier
IE	Internet Explorer
NAT	Network Address Translation
P2P	Peer to Peer
PHP	Hypertext Preprocessor
PTS	Post & Telestyrelsen
PuL	Personuppgiftslagen
SCB	Statistiska Centralbyrån
SFS	Svensk Författningssamling
SOU	Statens Offentliga Utredningar
SR	Sveriges Radio
SVT	Sveriges Television
UCCASS	The Unit Command Climate Assessment and Survey System
UMDAC	Umeå Universitets datorcentral

1. Inledning

> *My little three-year-old daughter loves to visit her personal screensaver, Disney's Sleeping Beauty. She sighs every time it opens……Then, one day, it happened. We sat down as usual, started the computer, clicked her user account, and it opened to a tremendously explicit adult pop-up. I was so caught off guard I shrieked, and my daughter yelled, too! …..… I'm not sure how it happened, but somehow a pornographic advertisement had hijacked Internet Explorer's default page. I can honestly admit I don't surf such sites nor open unknown e-mail, although it's possible another user could have opened a message or a link to a porn site by mistake. It also could have been one of those sneaky pop-ups that reverse the Yes and No buttons, so you're really installing something even if you think you've opted out. I got rid of it by manually scanning the registry …..…During that period, I had to restart, reset my home page, and empty the Recycle Bin many, many times. It took more than a week and countless hours of my time. (Download.com 2005)*

Ovanstående scenario är ingen ovanlighet. Spyware[1] har idag blivit allt vanligare och drabbar allt fler. I en undersökning som gjordes i USA år 2004, där 650 000 datorer granskades, fann forskarna att var tredje dator var smittad av spionapplikationer och sammanlagt hittades 18 miljoner spionprogram (The Computer Bulletin 2005:18). Forskare förutspår att år 2005 kommer att bli ännu värre (Soat 2005).

Vad är då spyware? Det finns ingen klar definition, men i denna uppsats kommer vi fortsättningsvis att avse ”program som utan användares vetskap installerar eller exekveras[2] på användarens dator och på olika sätt samlar eller sprider personlig information om användaren” när vi talar om begreppet (PTS 2005:9). Förutom olika program som installeras på datorn kommer vi även att räkna in cookies[3] som spyware.

Det finns många olika varianter av spionapplikationer som är mer eller mindre farliga, den gemensamma nämnaren är att de kränker den personliga integriteten. Vissa ändrar inställningarna i webbläsaren, detta utgör egentligen inte någon större risk för

[1] För att underlätta för läsaren och för att undvika upprepningar kommer vi i denna uppsats att använda oss av spyware, spionprogram och spionapplikationer som samma sak.
[2] Allmän benämning på *köra* eller *utföra*. I IT-sammanhang talar man om körbara program som då har filtypen EXE (Pagina.se 2005).
[3] Textfil med information som läggs in och sparas på den egna datorns hårddisk när man besöker vissa webbplatser på Internet (Nationalencyklopedin 2005a).

säkerheten, däremot utnyttjas datorns resurser vilket leder till att den blir instabil och långsam. Andra registrerar varje tangenttryckning användaren gör för att sedan skicka vidare informationen till upphovsmannen av spionprogrammet, det är den här sortens spionapplikationer som utgör de största hoten för säkerheten. (Messmer 2004)

Samtidigt som folks medvetenhet om datorvirus har ökat och hemanvändaren i allmänhet brukar vara någorlunda skyddad mot dessa, har spyware som begrepp gått förvånansvärt tyst fram och etablerat sig som en stor riskfaktor. Men på grund av att definitionen är så bred, är det svårt för allmänheten att få en uppfattning om spionprograms innebörd, hur de sprids och vad användaren kan göra för att minimera risken att bli smittad.

Vi vill undersöka hur medveten hemanvändaren är om dessa problem. Vi finner detta nödvändigt då spionapplikationer har potential att omintetgöra fördelarna med att medverka i stora nätverk, till exempel Internet, genom vilka många av spionprogrammen sprids (Boldt *et al*. 2004).

1.1. Bakgrund

År 2001 beräknades 498 miljoner av jordens cirka 6 miljarder människor ha tillgång till en Internetanslutning i hemmet, en siffra som antas ha ökat de senaste åren (Newsfactor Network 2005). Enligt Statistiska Central Byrån (SCB) hade drygt 5 miljoner personer i åldrarna 16–74 år tillgång till Internet i hemmet i Sverige år 2004 (SCB 2004b:33). Detta gör Sverige till ett av de länder i världen med störst andel av befolkningen som har tillgång till Internet (SCB 2004b).

Internet gör det enkelt att handla, sköta bankärenden och kommunicera, men användaren utsätts också för risken att någon gör intrång på datorn. Det som gör hemanvändaren intressant i det här avseendet är att det inte existerar några säkerhetsprocedurer runt en vanlig hemdator, vilket det oftast gör på företagsnätverk (McCardle 2003). I bästa fall har datorn en brandvägg och ett uppdaterat antivirus-program installerat, men detta utgör ändå inga garantier för att undgå att bli smittad av spyware. Det är endast genom att förstå hur spionprogram fungerar och hur de sprids som det går att minska risken att datorn blir infekterad (Gaskin 2005).

1.2. Syfte

Syftet med uppsatsen är:

- Att ge en överblick över vad spyware är, hur det fungerar och dess konsekvenser.
- Visa hur användaren kan skydda sig mot spyware.
- Kartlägga medvetandegraden om spyware hos hemanvändaren.

1.3. Frågeställningar

I avsikt att uppfylla den sista punkten i syftet samt att begränsa undersökningens omfattning ställer vi oss följande frågor:

– Upplever hemanvändaren spyware som ett hot?
– Känner hemanvändaren att spyware kränker den personliga integriteten?
– Hur skyddar sig hemanvändaren mot spyware?

1.4. Avgränsningar

Spyware är ett stort datafenomen och det är omöjligt att inkludera alla relevanta områden inom ämnet i en uppsats. Insamlandet av material, utförandet av den empiriska studien, nedskrivandet av resultat samt analysen blir också mycket lättare om gränser är satta och studiens syfte är tydligt (Svensson & Starrin 1996). Därför måste vissa avgränsningar göras.

På grund av svårigheterna att komma i kontakt med företag som erbjuder antispyware-verktyg samt en begränsad tidsram har vi valt att koncentrera vår studie på hemanvändare av PC-datorer som har Windows som operativsystem och någon form av Internetuppkoppling. Detta gjordes med hjälp av en webbenkät som lades ut på Internet. Anledningen till att vi har valt att enbart titta på Windows-användare beror på att spionprogram nästintill enbart angriper detta operativsystem (Gaskin 2005).

Att enkäten är skriven på svenska är även detta att betrakta som en avgränsning mot möjliga respondenter. Frågeformuläret var utlagd på Internet under en period på tolv dagar, därutöver gjordes inga försök att aktivt försöka nå andra respondenter.

2. Metod och Material

I det här kapitlet redogörs de metoder som uppsatsen är baserad på. Kapitlet inleds med en diskussion om metodval med respektive för- och nackdelar. Avsnitt två tar upp det material som använts i studien. I den tredje delen diskuterar vi den empiriska undersökningen. Stycket börjar med en presentation om webbenkäten, följt av hur enkäten utformats och val av respondenter. Slutligen tas uppsatsens validitet och reliabilitet upp.

2.1. Metodval

Enligt Idar Holme och Bernt Solvang (1997) är forskarens val av metod kritisk för analyserandet av undersökningsmaterialet, då den metodologiska utgångspunken påverkar vad forskaren uppfattar som ett problem, i vilket sammanhang problemet undersöks och hur undersökningsfrågorna utformas. Svaren till det undersökta kommer att inskränkas av dessa ramar men kommer också att förtydliga eller dölja omständigheterna som forskaren undersöker. (Holme & Solvang 1997) Knut Halvorsen (1992) säger att metoden är ett systematiskt tillvägagångssätt för att undersöka verkligheten. Att det är en utförandeform för att nå ny kunskap, inte enbart de tekniker som används för datainsamling och analys, men även ett sätt att förstå problemet som ska undersökas och de grundläggande antagandena om verkligheten. (Halvorsen 1992) De ovanstående påståendena är värdefulla att ha i åtanke vid valet av metod, men i slutändan beror valet av metod till stor del på studiens syfte (Tranøy 1986).

Traditionella metoder är antingen kvantitativa eller kvalitativa i sin utformning. Det metoderna har gemensamt är att de på något sätt ska analysera och kartlägga olika fenomen i samhället, hur människor eller grupper av människor handlar och interagerar med varandra. Skillnaden mellan de båda är att den första beskriver medan den andra tolkar. (Bryman 1997, Holme & Solvang 1997)

Den kvantitativa metoden använder strukturerade frågor som verktyg för skapandet av empiri och har som målsättning att uttrycka information i siffror, mängd eller liknande (Halvorsen 1992). Respondenterna får i detta fall samma frågor och svarsalternativ. Den kvantitativa metoden generaliserar på så vis ett samhällsfenomen, den beskriver samt förklarar något allmängiltigt (Eklund *et al.* 2004). Insamlandet av information i den kvantitativa metoden sker från en mängd olika objekt, oftast i enkätform, vilket inte ger utrymme för djupare tolkningar av svaren. Den kvalitativa metoden fokuserar på egenskaper som är icke-kvantifierbara och tillåter forskaren att gå på djupet med sin frågeställning (Bryman 2002).

Enligt Alan Bryman *et al.* (1988) är det problematiskt att hitta bakomliggande mönster i en studie utan att använda ett kvantitativt tillvägagångssätt, medan en kvalitativ metod behövs för att ge en djupare insikt och förståelse för den verklighet som studeras (Bryman *et al.* 1988). Att använda en kombination av kvantitativa och kvalitativa metoder innebär således att fördelarna stärks och nackdelarna undviks eller försvagas med respektive tillvägagångssätt (Bryman 2002).

Det är av den här anledningen som vi har valt att använda en kombination av kvantitativ och kvalitativ metod i genomförandet av studien. Det som vi eftersträvar i den här uppsatsen är att ge bredare och djupare förståelse för vad spyware är och vilka hot det utgör. Uppsatsen är kvantitativ i den bemärkelse att huvuddelen av uppsatsen kommer att fokusera på en enkätstudie med fasta svarsalternativ. Denna kompletteras med en kvalitativ litteraturstudie för att ge en helhetsbeskrivning av det undersökta. (*ibid*.)

Studien kommer att använda sig av både ett deduktivt och induktivt tillvägagångssätt. En deduktiv metod innebär att undersökaren försöker göra förutsägelser och dra logiska slutsatser utifrån vad som framkommit (Lundahl & Skärvad 1999). Medan ett induktivt arbetssätt kännetecknas av att forskaren studerar objektet och därefter, utifrån insamlad information, försöker formulera en teori (Freeman *et al.* 2003). Kvantitativa studier är deduktiva, där forskaren är mer bunden till de ursprungliga frågorna (Svensson & Starrin 1996). Kvalitativ analys är en induktiv process där motiv utvecklas allt eftersom det undersökta analyseras. På så sätt återkommer forskaren hela tiden till sin data med nya frågor och förändrade perspektiv under analysprocessen. (Freeman *et al.* 2003)

2.2. Material

Litteratur har använts för att komplettera och ge uppsatsen teoretisk vikt. Vi inledde vår informationsinsamling med litteraturstudier där vi granskade sekundärdata i form av befintligt material inom det aktuella ämnesområdet. Då spyware är ett relativt nytt begrepp har det varit svårt att hitta böcker inom ämnet, vi har istället till stor del fått förlita oss till vetenskapliga artiklar. Materialet har vi hittat genom sökning i olika databaser för böcker och tidskriftsartiklar, exempelvis ELIN (Electronic Library Information Navigator) och LIBRIS. Vi har även gjort sökningar genom olika sökmotorer på Internet, till exempel Google. Vi vill framhålla att sökningar på Google ställer höga krav på aktiv källkritik.

Eftersom vårt underlag till stor del består av artiklar från olika författare/organisationer kan de till viss del vara partiska, det går nämligen inte att utesluta att dessa inte värderar informationen på samma sätt. För att inte begränsa uppsatsen till enkätstudien samt att undvika att endast få en författares syn på problemet, har därför ett flertal publikationer använts. Detta har bidragit till att vi fått problemet belyst ur olika synvinklar. Att litteraturkällorna är aktuella är naturligtvis viktigt när dessa används för att analysera det empiriska materialet. Målet med den litteratur som nyttjats har därför varit att ha den senast publicerade. (Esaiasson *et al.* 2002)

2.3. Enkätstudie

Den data som ligger till grund för studien har samlats in genom en enkätundersökning. Webbenkäten lades upp på adressen http://www.isen.se/enkat/survey.htm den 4:e maj 2005 och togs ner den 16:e maj. Valet att genomföra en enkätundersökning grundar sig i att vi på en kort tid behövde komma i kontakt med ett flertal människor (Bryman 2002). Vidare tyckte vi att en webbenkät var ett passande verktyg att använda då vår uppsats avgränsas mot Internetuppkopplade privatpersoner.

Genom att använda oss av en webbenkät hoppas vi kunna komma åt vår målgrupp på ett effektivt sätt. Om enkäten hade skickats per post skulle det både ha gått åt tid och varit kostsamt att frakta enkäten fram och tillbaka. Enkäterna hade heller inte kommit tillbaka direkt, utan det hade kunnat ta flera veckor innan de återsändes. Genom att svaren

returnerades till servern, efter det att respondenten svarat på frågorna, minimerades även risken för att den intervjuade skulle glömma bort att fylla i eller slarva bort enkäten. (*ibid*.)

Nackdelarna med en enkätundersökning är bland annat att det inte finns någon intervjuare närvarande som ställer frågorna utan respondenterna måste själva läsa igenom uppgifterna. Risken finns då att frågeformuläret upplevs som tråkig och opersonlig, vilket kan leda till låg svarsfrekvens. En annan negativ faktor kan vara att respondenten inte förstår eller missuppfattar frågorna. (*ibid*.) Detta har vi försökt motverka genom att noga följa Alan Brymans (2002) riktlinjer om hur en enkät utformas med tydligt formulerade frågor (Bryman 2002:150-153).

2.3.1. Utformning

Enkäten, se bilaga 1, bygger inte på någon enskild enkät från tidigare undersökningar. I stället är enkätfrågorna speciellt utformade för den aktuella situationen och grundar sig på den kunskap som inhämtats av tidigare forskning inom området.

Verktyget vi använde för att skapa, publicera och administrera frågeformuläret finns tillgängligt under AGPL[4]-licens (Affero General Public License) för gratis nerladdning från ”open source” nätverket Sourceforge[5] och heter UCCASS (The Unit Command Climate Assessment and Survey System) 1.8.0. UCCASS är uppbyggt i PHP[6] (Hypertext Preprocessor) och alla datalagring sker mot en MySQL databas (Sourceforge 2005). UCCASS underlättar analysen av enkätsvaren eftersom man kan filtrera svaren.

Enkäten består av 20 slutna frågor, uppdelade på sju sidor, och är konstruerad enligt Alan Brymans (2002:150-153) rekommendationer för enkätutformning. Frågeformuläret börjar med ett försättsblad, där vi förklarar vilka vi är och syftet med undersökningen. Enkätfrågorna följer Brymans turordning där de lättaste och minst kontroversiella frågorna kommer först för att sedan öka i ”svårighetsgrad”. Valet av antalet frågor är baserat på Brymans åsikt om att för många frågor avskräcker människor att svara på enkäten. (Bryman 2002) Exakt vilka frågor som ska besvaras av

[4]Mjukvarulicens för öppen källkod (affero 2005).
[5] www.sourceforge.net
[6] Ett populärt programspråk som främst används för att utveckla webbapplikationer.

varje respondent bero på hur användaren ställer sig i vissa frågor, enkäten kan på så vis automatiskt hoppa över någon fråga eller gå direkt till slutet. Anledningen till att vi valde slutna frågor var att vi inte kände något behov av öppna frågor för att svara på vårt syfte (Hayes 2000).

2.3.2. Enkätfrågor

Följande avsnitt är sammanställt för att ge en översikt över varför enkätens frågor är ställda som de är. Se bilaga 1 för att se frågorna och svarsalternativen i sin helhet.
De första två frågorna i enkäten är ställda för att ta reda på hur våran urvalsgrupp ser ut i fråga om ålder och kön. För att sortera bort de som inte är intressanta för vår studie ställde vi frågorna tre och fyra. Den femte frågan ställs för att ta reda på om respondenten använder Internet Explorer, som är inbyggt i Windows, eller har valt att installera en annan webbläsare. Anledningen till att vi ställer fråga sex är för att ta reda på hur lång tid dagligen användarens PC är exponerad mot Internet.

Frågorna sju till och med tretton tar reda på vilken sorts programvara användaren kör på sin dator. Fråga fjorton och femton är ställa för att ta reda på om användaren söker igenom sin dator aktivt efter spyware, och om han eller hon någon gång har hittat något spyware på datorn.

De sista fem frågorna är konstruerade med hjälp av en Likertskala[7] där frågor ställs i form av påståenden som ska besvaras på en femgradig skala, från ”Instämmer helt” till ”Instämmer inte alls”. Några frågor är formulerade i positivt ordalag och några i negativt. Anledningen till detta är att undvika enkla tendenser i svarandet, som att rakt igenom svara "instämmer helt". (Patel & Davidson 2003)

Fråga 16 är ställd för att ta reda på om användaren är medveten om de hot och säkerhetsrisker som spyware utgör. För att undersöka i hur hög grad respondenten känner att den personliga integriteten kränks av spyware ställs fråga 17. I fråga 18

[7] Attitydskala. Skalan innehåller ett antal påståenden som man genom förstudier kunnat visa avspeglar attityden till något eller någon. Den person vars attityd man vill mäta får ta ställning till varje påstående eller *Likert-item* och ange hur starkt han/hon instämmer i eller tar avstånd från dess innehåll. (Nationalencyklopedin 2005b)

vänder vi på fråga 16 och frågar om användaren känner att spyware snarare utgör ett irritationsmoment än en säkerhetsrisk. Fråga 19 är ställd för att ta reda på hur stor andel av respondenterna som läser igenom hela EULA innan de installerar ett nytt program. Den sista frågan i enkätundersökningen, fråga 20, är ställd för att få ett mått på användarens rädsla för spyware genom att använda ett konkret exempel.

2.3.3. Urval

För att nå deltagare har vi använt oss av ett snöbollsurval, det vill säga att en deltagare ber sina vänner att fylla i enkäten som i sin tur ber sina vänner (Robson 2002). Detta för att på ett enkelt sätt nå en så stor deltagargrupp som möjligt. Sammanlagt fick vi 98 svar. Med tanke på studiens omfång tycker vi att detta är ett tillräckligt stort urval för att avspegla verkligheten. Enligt Karin Dahmström (2000) räknas urvalet som ett ”självval” då deltagandet i enkäten är frivilligt. Vidare menar hon att det inte går att dra några säkra slutsatser från ett resultat när studien bygger på självval eftersom respondenten själv har valt om han/hon vill delta eller ej. Eftersom kriterierna för alla respondenter som deltar i studien är att de måste ha Windows som operativsystem samt någon form av Internetuppkoppling, menar vi att vår studie redan är avgränsad på ett sådant sätt att frågan om självval blir mindre viktig i detta sammanhang. (Dahmström 2000)

2.4. Validitet och Reliabilitet

Validitet och reliabilitet är två viktiga aspekter att ha i åtanke vid forskningsstudier för att ge läsaren en uppfattning om materialets kvalité och tillförlitlighet (Bryman 2002).

Validitet definieras som en metods eller ett mätinstruments förmåga att mäta eller avbilda det som avses. Eftersom vi inte haft möjlighet att utföra en pilotstudie för att testa vårt verktyg är vår undersökning att betraktas som mindre god ur ett giltighetsperspektiv. Vi har försökt öka undersökningens validitet genom att noga följa Alan Brymans (2002) direktiv om hur ett frågeformulär utformas med tydligt formulerade frågor (Bryman 2002:150-153).

Ett problem med validiteten uppstår när forskaren arbetar på två olika nivåer, en teoretisk och en empirisk. Problemet ligger i att syftet och frågeställningarna formuleras

på en teoretisk nivå medan den empiriska studien görs i verkligheten. (Esaiasson *et al.* 2002) I vår uppsats knyter den teoretiska ramen, kapitel tre, samman teorin med det empiriska resultatet genom att relatera den till vår frågeställning, kapitel ett. På så sätt minskas avståndet mellan teori och praktiskt utförande.

Med *reliabilitet* menas undersökningens grad av tillförlitlighet, vilket bekräftas genom att undersökningen kan upprepas med likartat resultat (Eriksson & Wiedersheim-Paul 1991). Reliabilitet påverkas av olika faktorer, såsom vilket mätinstrument som används, personen som utför mätningen, omgivningen kring mätningen och objektet som undersöks (Bryman 2002).

Reliabiliteten i vår webbundersökning beräknar vi vara relativt hög då vi tror att samma svar skulle fås om undersökningen gjordes på nytt. Detta grundar vi på att vi inte kunnat påverka respondenterna då enkäten hämtats via en webbsida och vi aldrig haft någon personlig kontakt med dem. Eftersom svaren samlats in elektroniskt från respondenterna minimeras även de fel som annars ofta uppkommer vid inmatning på grund av överföring från ett media till ett annat, exempelvis vid renskrivning av inspelad intervju. (*ibid*.) Som vi nämnde ovan har vi därför följt Alan Brymans (2002) anvisningar om hur en enkät utformas (Bryman 2002:150-153). Respondenterna har heller inte haft möjlighet att läsa igenom hela enkäten innan de besvarade frågorna utan var tvungna att svara på frågorna i nummerföljd (Hayes 2000). Vidare har respondenterna besvarat enkäten när de har tid och befinner sig i en bekant miljö. En omständighet som kan leda till lägre reliabilitet är om respondenterna skulle ändra åsikt vid nästa undersökningstillfälle på grund av att de samlat på sig nya kunskaper. (Bryman 2002)

3. Teoretisk ram

I detta kapitel kommer det teoretiska ramverket för uppsatsen att presenteras. Ramverket är uppdelat i fyra delar; den första delen redogör för begreppen integritet och personlig integritet. Den andra delen diskuterar integritet på Internet, följt av en beskrivning om vilka lagar som skyddar integriteten. Avslutningsvis tar vi upp hur spyware kränker integriteten. Teorin kommer att utgöra grunden för analysen beträffande medvetandegraden om spyware hos hemanvändaren.

3.1. Integritet

Ordet integritet kommer från det latinska orden *integritas*, helhet, orörlighet, och *integer*, hel, orörlig. Nationalencyklopedin definierar integritet som ”rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp”. (Nationalencyklopedin 2005c)

3.1.1. Personlig integritet

Termen personlig integritet används för att beteckna olika slags integritet, såväl kroppsliga som psykologiska, och grundar sig på att människan är en självständig individ med karakteristiska egenskaper såsom viljor, känslor och vanor (Liljestrand & Lindgren 2003). Enligt Göran Collste (1997) måste de uppgifter som sprids vara integritetskänsliga för att en kränkning ska kunna ske. Det kan röra sig om allt från privata uppgifter, politiska åsikter och sexuell läggning till önskningar och speciella kunskaper. Innebörden av den personliga integriteten skiftar därför beroende på tillfälle och omständigheter. (Collste 1997)

Beroende på begreppets komplexitet kommer vi fortsättningsvis, när vi talar om personlig integritet, att använda oss av följande definition: ”personlig integritet avses

här vara att personlig och privat information inte skall behandlas eller delges andra utan individens vetskap eller samtycke” (PTS 2005:7).

3.1.2. Integritet och Internet

Integritet har alltid gått hand i hand med teknologins utveckling. Redan år 1890 skrev Samuel Warren och Louis Brandeis hur de fruktade att portabla kameror skulle kunna hamna i händerna på amatörer, vilket skulle kränka andras integritet genom att bilder togs på dem (Warren & Brandeis 1890). Den vanligaste debatten idag rör istället frågan om användare verkligen har rätt till integritet på Internet. Följdfrågan blir, om svaret på den första frågan är ja, var gränsen för en integritetskränkning ska sättas (Klang 2004).

Internets uppkomst har skapat svåra utmaningar för vår intuitiva känsla för integritet. Hur mycket privatliv vi har/kan förvänta oss beror på de lagar och förordningar och de underliggande värderingar som finns i vårt samhälle. Åtgärder för att skydda den personliga integriteten måste ta hänsyn till de teknologiska framsteg som gjorts och den sociala kostnaden för att tillhandahålla ett sådant skydd. Inom de områden där de sociala kostnaderna är relativt låga och tekniken redan finns tillgänglig, exempelvis läkarjournaler, är det rimligt att förvänta sig en ökad integritet. I de fall där kostnaderna är höga och teknologin som krävs komplicerad, så som skydd angående privat e-post, förväntas minskad integritet. (McArthur 2001)

3.1.3. Lagar som skyddar integriteten

Personuppgiftslagen

Sverige var det första landet i världen som fick en datalag för att skydda den personliga integriteten. Datalagen kom 1973 och ersattes den 24 oktober 1998 av PuL (Personuppgiftslagen) (Datainspektionen 2005a).

PuL bygger på ett EG-direktiv (Europeiska Gemenskapen) och är till för att öka skyddet för individens personliga integritet gällande elektronisk information om individen som finns lagrad i olika register. Främst omfattar PuL flera sorters hanteringar av

personuppgifter[8]. Krypterade uppgifter och olika slag av elektroniska identiteter innefattas även av lagen, men detta gäller enbart om uppgifterna direkt eller indirekt kan hänföras till fysiska personer. PuL talar om två typer av informationsskyldighet, den första rör information som självmant ska lämnas ut av den personuppgiftsansvarige[9], den andre information som lämnas ut efter ansökan av den registrerade. (SFS 1998)

PuL reglerar även överföringen av personuppgifter till tredje land. Det är endast tillåtet att överföra personuppgifter till andra stater som har ett tillräckligt skydd för informationen, men harmlös information får publiceras på Internet utan att den berörda personen kontaktas eftersom sådana uppgifter inte kräver något skydd. Vad som betraktas som harmlösa uppgifter bedöms från fall till fall. Om en person har gett sin godkännande är det tillåtet att publicera uppgifter på nätet. Den registrerade[10] ska ha fått utförlig information om publiceringen, så att han eller hon kan bedöma för- respektive nackdelar. (*ibid.)*

Privat behandling av personuppgifter innefattas inte av PuL. Publicering på nätet kan aldrig betraktas som en privat behandling eftersom uppgifterna blir allmänt tillgängliga över hela världen. (*ibid.)*

Lagen om elektronisk kommunikation

EkomL (Lagen om elektronisk kommunikation), som infördes juli 2003, tillkom efter ett direktiv i EU (Europeiska Unionen) för att ge enskilda personer och myndigheter tillgång till säkra och effektiva elektroniska kommunikationer (PTS 2005, SFS 2003). Det intressanta med lagen är att den har valt att lyfta fram frågan om integritet i ett eget kapitel, kapitel sex.

> *Elektroniska kommunikationsnät får användas för att lagra eller få tillgång till information som är lagrad i en abonnents eller användares terminalutrustning endast om abonnenten eller användaren av den personuppgiftsansvarige får information om ändamålet med behandlingen och ges tillfälle att hindra sådan behandling.(SFS 2003: kap 6 § 18)*

[8] All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (SFS 1998:3§).
[9] Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (SFS 1998:3§).
[10] Den som en personuppgift avser (SFS 1998:3§).

När lagen trädde i kraft hamnade cookies, som används av många webbplatser, i fokus. Detta eftersom det nu blev lagstadgat att användaren skulle informeras om Internetsidan som besöktes använde sig av cookies. (PTS 2005) Vad som inte framgick lika tydligt var att paragrafen även reglerade andra program som används för att ”lagra eller få tillgång till information som är lagrad i en abonnents eller användares terminalutrustning”, som till exempel spionprogram (SFS 2003: kap 6 § 18).

EkomL ger direktiv om hur information får lagras på en användares dator och hur denna information kan användas. Lagen säger att elektroniska kommunikationsnät endast får hämta eller lagra information på en användarens terminalutrustning om användaren informerats om detta samt har givits tillfälle att hindra användningen. Bestämmelsen förbjuder alltså inte att hämtning eller lagring av information från en användares dator sker, men kräver däremot att användaren informeras om detta. Upplysningen behöver inte äga rum i förhand utan det räcker att den sker i anslutning till aktiviteten. (SFS 2003)

Informationen från programmet måste framträda klart och tydligt och inte vara gömd på ett sådant vis att den kan missas av användaren. Det räcker inte att en viss terminal visat meddelandet en gång, genom exempelvis en pop-up ruta som sedan aldrig dyker upp mer, oavsett om information ska lagras eller hämtas. Information om cookies eller andra spionprogram, deras syfte samt om hur en användare kan gå tillväga för att neka åtkomsten, ska alltid finnas tillgänglig på en webbplats. Anledningen till detta är att det är den enskilde användaren, inte terminalen, som skyddas enligt lagen. (*ibid.)*

Distinktion mellan PuL och EkomL

Det kan vara svårt att få en uppfattning om när PuL eller EkomL ska användas eftersom de två lagstiftningarna i vissa fall är tillämpliga på samma områden. Mycket förenklat kan det sägas att EkomL reglerar olika former av kommunikation men inte vad som kommuniceras. Så länge meddelanden är under transport ska EkomL användas, när det gäller förbud mot avlyssning, reglering om cookies med mera. PuL tillämpas när kommunikationens innehåll på olika sätt hanteras, till exempel lagring av meddelanden. (SFS 2003)

3.1.4. Hur spyware kränker den personliga integriteten

Det som gör att spyware kränker den personliga integriteten är att den samlar in och sänder information om datoranvändaren utan dennes vetskap och/eller visar reklam i pop-up fönster[11] som användaren inte själv valt att se.

Enligt Johan Wieslander *et al*. (2003:2) kan spyware kränka integriteten genom en eller flera av följande punkter:

- Information om datorn eller datoranvändare som samlas in och skickas vidare utan användares medgivande. Exempel på sådan information kan vara hårdvarukonfiguration, operativsystem, mjukvara som är installerad på datorn och användarnamn.

- Information om filer användaren har på datorn samlas in och skickas vidare utan användares medgivande.

- Information från webbläsarens cache[12], cookies eller andra filer på hårddisken samlas in och skickas vidare utan användarens medgivande.

- Information från andra anordningar som är kopplad till datorn samlas in och skickas utan användarens medgivande.

[11] Är mindre fönster som ”poppar upp” när man använder sin webbläsare. Många gånger handlar det om reklam som dyker upp utan att man har bett om det.
[12] Översta nivån i datorns minnessystem där datorn lägger viss information för att ha den snabbt tillgänglig (Nationalencyklopedin 2005d)

4. Spyware

Följande kapitel är till för att ge läsaren en överblick över vad spyware är och hur det fungerar. Avsnittet kan även ses som ett bakgrundskapitel till den empiriska analysen. Kapitlet inleds med en bakgrund till begreppet. Detta följs av olika definitioner av spionprogram. Avslutningsvis för vi en diskussion angående frågan om etik och säkerhet runt spyware.

4.1. Bakgrund

För att förstå vad spionprogram är måste vi först känna till adware. En programmerare tjänar sina pengar genom att tillverka två versioner av samma program. En version som är reklamfri och som användarna måste betala och en annan som innehåller reklam för ett eller flera företag. Företagen har betalat utvecklaren till programmet för att få ha med reklam, antigen genom pop-up fönster eller banners[13]. Det är den sistnämnda versionen som kallas för adware. (Wieslander *et al*. 2004)

Att lägga in reklamen direkt i mjukvaran var en bra affär för både tillverkaren, som fick betalt för sina program, och för användarna som kostnadsfritt fick tillgång till programmet. Detta var tidigare ett vanligt sätt att sälja program, tills marknaden i USA upptäckte tendenser som förde in adware på ett nytt spår. Marknadsundersökningar hade visat att reklamen i programmen inte gav så mycket som väntat. Riktad Internetreklam gjorde däremot människor mer intresserade. Slutsatsen som drogs var att skräddarsydd Internetreklam skulle skapa nya möjligheter för marknadsföring av produkter och tjänster. Allt som behövdes var ett verktyg som övervakade användarnas aktiviteter på Internet. Det var här adware kom in i bilden. Programmen gick från att vara ett ofarligt sätt för företag att göra reklam för sina produkter, till att övervaka användare så att de kunde ge dem reklam som låg inom deras intresseområden. (Townsend 2003)

[13] Annons på webbsida på Internet, vanligen rektangulär och placerad över, under eller vid sidan av en sidas huvudsakliga innehåll (Nationalencyklopedin 2005e)

Ofarliga former av adware finns fortfarande kvar och det är viktigt att skilja mellan detta och spyware. Adware kör reklam och erbjudanden i programmet och användaren är medveten om detta när han/hon installerar programmet. Spyware å andra sidan samlar information om datoranvändaren som sedan skickas vidare till en tredje part, utan att användaren är medveten om det. (Wieslander *et al*. 2004)

4.2. Olika typer av spyware

Det finns många olika sorters spyware. Allt från enkla cookies som lagrar information för att användaren ska slippa fylla i den nästa gång han/hon besöker webbplatsen, till cookies som spårar användarens aktiviteter på Internet och skickar dem till upphovsmakaren tillsammans med ett unikt identifikationsnummer. Denna information kan sedan användas i marknadsförningssyfte, för att anpassa erbjudanden till konsumenten, eller för att helt enkelt spionera på användaren. (Ames 2004)

Om datorn arbetar långsammare än tidigare, oväntade annonser poppar upp från webbläsaren, webbläsarens startsida ändrats eller om datorn helt enkelt inte svarar på de kommandon som den ska, är risken stor att datorn drabbats av spyware. Men eftersom poängen med spionapplikationer är att stjäla information, körs de i det tysta och chansen är liten att användaren upptäcker själva programmet. (Tauson 2005)

Wes Ames (2004) delar in spyware i tre risknivåer: enkla cookies, associerade cookies och applikationsbaserade spionprogram.

4.2.1. Enkla cookies

En cookie är en liten fil som placeras på användarens system när denne besöker en webbserver och har som uppgift att komma ihåg vad konsumenten gör på servern. När användaren återkommer till webbservern letas cookien upp på hans/hennes dator och läser in föregående inställningar. (McCardle 2003) Detta ger exempelvis e-handelssajter möjlighet att känna igen sina kunder och anpassa den presenterade informationen enligt användarens senaste önskemål (Ames 2004). Enkla cookies utgör på så sätt inte själva något hot utan ses oftast som användbara redskap (Hormozi 2005).

Som vi nämnt tidigare är det i Sverige, sedan den 25 juli 2003, lagstadgat att alla hemsidor måste upplysa sina besökare om att cookies används (PTS 2005).

4.2.2. Associerade cookies

Associerade cookies, eller tredjeparts cookies, utnyttjas av olika nätverk av webbplatser som samarbetar för att lagra information om användarna som besöker deras webbsidor. Informationen kopplas till konsumenterna med hjälp av en cookie som innehåller en GUID[14] (Globally Unique Identifier), vilken lagras på användarens dator. Denna innefattar uppgifter om användaren så som namn, gatuadress och e-post (Ames 2004). Liksom enkla cookies kan tredjeparts cookies också kartlägga användarens Internetaktiviteter i marknadsföringssyften (Hormozi 2005). Cookien kan även användas för att fånga upp och lagra känslig data, exempelvis användarnamn, lösenord och kreditkortsnummer, som utväxlas i interaktionen mellan användaren och deltagande webbplats (Ames 2004). En utmärkande egenskap med associerade cookies är att de med hjälp av ett utgångsdatum, som är satt till många år framåt i tiden, stannar kvar på datorn under en längre tid (McCardle 2003).

Storleken på dessa nätverk av samarbetande webbplatser illustreras av företaget DoubleClick, som administrerar ett av de största med 11 000 deltagande webbsidor från vilka de har samlat in data från 100 miljoner användare. DoubleClick är så stort att så gott som alla som har surfat på Internet, utan att blockera cookies, har företagets associerade cookies på hårddisken. (Hormozi 2005:55)

Det största problemet med associerade cookies är att allt sker helt utan användarens vetskap. Konsumenten har på så vis ingen möjlighet att avgöra vilken typ av information han/hon lämnar ifrån sig. Även om denna typ av cookie inte kan installera eller köra applikationer på värddatorn kan de exempelvis registrera och skicka vidare varje knapptryckning från ett tangentbord. Detta gör tredjeparts cookies till ett allvarligt säkerhetshot. (Ames 2004)

[14] Ett unikt id för att identifiera användare (Ames 2004).

4.2.3. Applikationsbaserad spyware

De två begreppen som diskuterats ovan bygger uteslutande på cookies, vilka enkelt kan raderas från hårddisken utan något specialprogram. Applikationsbaserad spyware kan dock vara betydligt svårare att bli av med och kan i värsta fall styra sig själva helt och hållet. (Ames 2004)

Applikationsbaserade spyware kan utan användarens vetskap starta när datorn sätts igång och exempelvis söka igenom systemet efter information för att skicka denna vidare till mottagaren. Den här typen av spionprogram är alltså inte beroende av att en användare ägnar sig åt någon specifik aktivitet. Den är inte heller begränsad till att samla in data, utan kan till exempel ladda hem uppgraderingar, installera andra program eller visa reklam utan att användaren gett sitt medgivande. (*ibid.)*

Det finns tre olika metoder för att installera applikationsbaserad spyware på användarnas dator: ”piggybacking”, utility-program[15] och genom exekvering av Java eller ActiveX[16] kod på en webbsida (*ibid.).*

Piggybacking innebär att spionapplikationen följer med ett program som användaren laddar ner och installerar. När den aktiverats konfigurerar den sig själv och körs utan användarens vetskap (*ibid*.). En programvara som ofta utsätts för piggybacking är fildelningsprogram, vars popularitet gör dem till ett perfekt sätt att infektera ett stort antal användare med spionprogram (Boldt *et al*. 2004).

Det andra sättet att installera applikationsbaserad spyware är förklä den i form av en tjänst, ett så kallat *utility-program*. Det kan exempelvis röra sig om extra verktygsfält till webbläsaren eller program för lagring och uthämtning av lösenord. Förutom att utföra dessa tjänster installerar de spyware som får total rörelsefrihet på datorn. (Ames 2004)

Java eller ActiveX applikationer är små program som ligger på webbsidor. När programmen körs, installeras det på användarens hårddisk. Konsumenten behöver alltså

[15] Insticksprogram (Ames 2004).
[16] En teknologi skapad av Microsoft för att dela information mellan olika applikationer (Ames 2004).

inte aktivt göra något för att bli smittad. Detta tillvägagångssätt är inte alls olikt exempelvis hur hackers kan bryta sig in på privata datorsystem. (*ibid.)*

4.3. Diskussion om etik och säkerhet runt spyware

Trots att etik är ett av de mer intressanta områdena när det gäller spyware, har vi valt att hålla diskussionen på en övergripande nivå. Detta beror på att vi anser att en djupare teoretisk bas behövs för att kunna föra ett resonemang om etik på ett vettigt sätt.

Den viktigaste frågan när det gäller spionprogram gäller hur långt det är tillåtet för företag och privatpersoner att gå i sin jakt på information. Var sätts gränsen mellan privat och offentligt? Men framförallt kan det diskuteras om det är etiskt riktigt att genom spionprogram inkräkta på den personliga integriteten.

I Rapports nyhetssändning den 29 maj 2005, klockan 19.30, berättades det om företaget Eurodex som säljer tre program, *Spector Pro*, *eBlaster och Spector*, vilka gör det möjligt att ha uppsikt över allt som händer i en eller flera datorer. Inslaget rörde den lagliga aspekten, det vill säga om det var lagligt för företaget att övervaka sina anställdas aktiviteter. (SVT 2005)

Spector Pro, eBlaster och Spector marknadsförs som övervakningsprogram för make/maka, arbetsgivare och föräldrar, se figur 4.1. Programmen fungerar som en gömd övervakningskamera eller videobandspelare i datorn och spelar in alla besökta webbsidor, använda program, spelade spel, varje tangenttryckning, konversationer och e-post som skickats och tagits emot. Till och med webbaserad e-post, så som Hotmail, Spray, Passagen, Yahoo etcetera, kan registreras. Det speciella med Spector Pro, eBlaster och Spector är att de kan fjärrstyras via mejl, övervakningen sker på så sätt utan användarens vetskap. (Eurodex 2005) Eftersom programmen registrerar användarens aktiviteter för att sedan skicka denna information till en tredje part utan datoranvändarens vetskap är vår åsikt att dessa tre program är spionapplikationer.

Figur 4.1 Eurodex:s program Spector Pro, eBlaster och Spector (Eurodex 2005).

Enligt Datainspektionen får AB Svensk Pantbelåning, Pantbanken, inte registrera uppgifter som visar att personer har lämnat in stöldgods eller uppträtt hotfullt mot andra kunder. Däremot får bolaget registrera uppgifter om kunder, till exempel spelmissbrukare, som själva har bett att företaget ska hindra dem från att lämna in gods. (Datainspektionen 2005b) Vi ser inget som säger att programmen som Eurodex säljer skulle vara annorlunda, i avseendet att registrera uppgifter om användare, och anser att programmen starkt kränker den personliga integriteten genom att överskrida gränsen när det gäller vad som är privat och offentligt. Vad en person gör eller lagrar på sin dator är dennes privata handlingar/dokument tills han/hon väljer att offentliggöra det.

Hans-Olov Lindblom på Datainspektionen säger att det finns många begränsningar i hur en arbetsgivare får spionera på sina anställda. Vidare menar han att Spector Pro, eBlaster och Spector överskrider dessa begränsningar eftersom de övervakar de anställda utan deras vetskap. Men säger han, det som är skrämmande är att lagstiftningarna inte når in i det som sker i hemmet. (SR 2003) Vi anser däremot att EkomL, som säger att ”program endast får hämta eller lagra information på en användarens terminalutrustning om användaren informerats om detta samt har givits tillfälle att hindra användningen”, också borde gälla när det handlar om att använda programmen i privat syfte (SFS 2003).

Vi tycker därför att program som Spector Pro, eBlaster och Spector borde förbjudas eftersom övervakningen sker utan användarens vetskap. Eller som i fallet med Linköping Kommun, där programmet installerades på de anställdas datorer utan deras kännedom. Datainspektionen bestämde i detta fall att alla anställda måste informeras individuellt om att programmen installerats, hur de fungerar samt syftet med dem, för att programmen skulle få användas (SVT 2005). Exemplet visar att lagstiftningen är bristfällig när det gäller spyware och hur det får användas. Vi anser därmed att mer detaljerade förordningar behöver införas.

En annan fråga som är intressant är problemet kring vilken part det är som har rättigheter och ansvar att bedöma vad som är spyware eller inte. Nyligen framförde företaget 180solution klagomål till flera antispyware-företag, vars antispyware-program tar bort deras sökassistent *Zango* som visar reklam för användaren. Företaget sa att deras spionapplikationer var harmlösa för användaren och att antispyware-företagen tjänade pengar på användarna genom att överdriva riskerna med spyware. (Messmer 2005) Andra företag har hittat mer aggressiva sätt att förhindra antispion-programmen. Mediaspelaren *RadLight version 3.03* letade till exempel upp Ad-Aware[17] på hårddisken och raderade dess programfiler som ett steg i sin installationsprocess (McWilliams 2002).

[17]Antispyware-program som finns att ladda ner gratis på Internet.

Det som är skrämmande med den sista historien är att avinstallationen av antispyware-programmet faktiskt stod med i EULA[18] (End User License Agreement), på så sätt var RadLight garderade mot lagliga efterföljder. Eftersom EULA oftast är medvetet svåra att tyda är det svårt att sätta gränsen för vad en användare kan tänkas förbinda sig till genom att trycka på ”Jag accepterar EULA” vid installation av ett program. Vi tycker därför att hårdare riktlinjer, för utformningen av dessa licensavtal, behövs för att göra de mer förståliga för användarna.

Situationen ser annorlunda ut när det gäller cookies. Det finns nämligen sällan någon möjlighet till att tacka nej till användandet av cookies, förutom valet att inte besöka webbsidan eller genom att låsa ute alla cookies. Internetanvändare kan dock utgå ifrån att webbsidor som har BBB (Better Business Bureau) och TRUSTe logotyp är säkra. BBB garanterar att webbsidan följer sin egen policy och standard. TRUSTe säkerställer att informationen som samlas in om användaren redovisas i företagets webbpolicy. (Hormozi 2005)

[18] Den sorts avtal som ger licens för användning av en programvara eller en tjänst som godkänns av en slutanvändare.

5. Skydd

Det finns olika metoder för att skydda sig mot spionprogram. Förutom att inte installera program annat än från erkänt seriösa programvaruleverantörer, så finns det program som både stoppar installationen av spyware och som kan leta igenom datorn efter redan installerade spionapplikationer (Tauson 2005). Metoderna kommer att beskrivas mer ingående längre fram i kapitlet. En viktig skyddsåtgärd är medvetenhet och tekniskt kunnande hos användaren. Avsnittet börjar med en diskussion om skyddsåtgärder ur ett allmänt perspektiv. Även detta avsnitt kan ses som ett bakgrundskapitel till analysen.

5.1. Skydd mot spyware

Spionprogram är ett problem som så gott som bara angriper operativsystemet Windows (Gaskin 2005). Berni Dwan (2005) påstår därför att det enda sättet att inte bli smittad av spyware är att byta till Apple Mac, vilken endast används av två procent av Internetanvändarna och därför inte ses som ett lönsamt mål (Dwan 2005:19).

För de som använder sig av Windows går det att skydda sig genom att skaffa rätt verktyg. Användaren behöver också vara försiktig när han/hon installerar så kallade ”freeware- och sharewareprogram”[19] som kan laddas ner från Internet. (McCardle 2003) Efterhand som attackerna blir mer invecklade ställs det även större krav på konsumentens förståelse för spyware (Levy & Arce 2004).

5.2. Brandväggar

Brandväggar utgör den första försvarslinjen i de flesta nätverk[20] (Greiner 2005). För att förstå hur en brandvägg kan skydda mot spionprogram måste vi först få en förståelse för hur den fungerar. En brandvägg har tre grundläggande regler: 1) All trafik från insidan

[19] Datorprogram som distribueras kostnadsfritt via Internet eller andra elektroniska medier (Nationalencyklopedin 2005f)
[20] Med ”nätverk” menas vi här allt från enskilda till flera sammankopplade datorer

till utsidan och tvärt om måste gå genom brandväggen, 2) Endast trafik som markerats som godkänd får lov att passera genom brandväggen, och 3) Brandväggsystemet är immunt mot penetration (Stallings 2003).

5.2.1. Brandväggar som skydd mot spyware

Idag används brandväggar ofta som ett av försvarsstegen mot spyware, eftersom de ger användaren möjlighet att bestämma vilka program som ska få åtkomst till Internet (Chow *et al.* 2004). Brandväggar skyddar alltså bara mot okänd trafik eller trafik som kan uppfattas som skadlig (McCardle 2003).

De spionapplikationer som använder sig av piggybackingmetoden, för att få åtkomst till en dator, kan vara svåra att blockera eftersom de maskerar sig som trafik från det ursprungliga programmet (Chow *et al*. 2004). Ett exempel på piggybacking är fildelningsprogrammet Kazaa, som enligt en undersökning av Johan Wieslander et al. (2004) är ett program som innehåller många spionapplikationer. När användaren ger Kazaa tillåtelse att passera genom brandväggen ges även alla spionprogram, som använder sig av piggybacking på programmet, tillträde att fritt röra sig förbi brandväggen. (Wieslander *et al*. 2004:9) Även om Kazaa skulle blockeras i brandväggen, kan spionapplikationerna, som redan installerats på datorn, hitta nya vägar ut på Internet genom att maskera sin trafik som något annat program som kräver Internetåtkomst, exempelvis Internet Explorer (Dwan 2005).

I vissa fall kan även brandväggar med NAT[21] (Network Address Translation) teknik, utgöra ett bra försvar. Genom att skriva in fel IP-adress i värdfilen[22] får inte spionprogrammen kontakt med servern och kan därför inte skicka den insamlade informationen vidare. (McCardle 2003)

[21] En funktion där ett lokalt nätverk använder interna IP-adresser som inte går att använda på Internet. När en dator på det lokala nätet vill skicka ett meddelande till Internet, översätts dess IP-adress av NAT-funktionen till en externt giltig IP-adress. När svarsmeddelande kommer tillbaka översätts adressen tillbaka så att meddelandet hittar till rätt dator på det lokala nätet. Utåt blir alltså bara en eller ett fåtal IP-adresser synliga.
[22] Värdfilen ansvarar för alla ipadresser som är blockerade av brandväggen.

5.3. Antivirus-program

Det kan vara svårt att skilja mellan spionapplikationer och virus. Vanliga antivirus-program spårar sällan spyware och de som gör det fångar inte upp alla former av spionprogram. I vissa fall inkluderas skydd mot spionprogram, men skyddet måste aktiveras vid installationen för att inkludera utökat hot. Anledning till detta är att det inte är så enkelt att avgöra vad som är spyware. Det enda som skiljer ett adware från ett spionprogram är ifall användaren informerats och samtycker till programmets funktioner. (PTS 2005) På grund av detta har virusprogram i allt högre omfattning även börjat inkluderar olika former av säkerhetshantering med avseende på såväl spionprogram som brandväggsfunktioner (The Computer Bulletin 2005).

5.4. Antispyware-program

Det finns ett flertal produkter, så kallade antispyware/antispion-program, som riktar in sig på att hindra installation eller att hitta och ta bort spionprogram. Exempel på antispion-program som kan laddas ner gratis från Internet är Ad-Aware och Spybot Search and Destroy. (PTS 2005)

En vanlig metod för att hitta spionapplikationer är ”signature scanning”, signaturigenkänning. Detta bygger på en databas med digitala signaturer över kända spionprogram, en sökmaskin jämför sedan det misstänkta programmets signatur med databasen. Om signaturen finns i databasen betraktas programmet som spyware. Problemet med den här tekniken är att endast kända spionprogram kan identifieras och blockeras. Det är därför viktigt att alltid ha en uppdaterad databas. (Chow *et al*. 2004)

Användaren bör köra och uppdatera antispyware-program regelbundet. Dessutom är det rekommenderat att köra mer än ett antispion-program åt gången. Detta på grund av att det finns så många olika sorters spionapplikationer att det är näst intill omöjligt för ett program att hitta alla. (Gaskin 2005)

6. Resultat och Analys

I det här kapitlet sammanställer vi och analyserar vårt empiriska material. Framställningen sker med hjälp av frågeställningarna som klargjordes i syftet, se kapitel 1:1. För att kunna göra korsjämförelser tog vi i enkätens inledande frågor med ett antal bakgrundsvariabler så som *ålder, kön* och *hur länge användaren har haft PC i hemmet* etcetera, se bilaga 1 fråga 1-6.

Tabell 6.1. Antal enkätdeltagare, efter internt bortfall, uppdelade på ålder och kön

Ålder	Totalt	Man	Kvinna
10-24	43	35	8
25-34	34	27	7
35-44	4	1	3
45-54	8	4	4
55-74	6	5	1
75+	0	0	0
Totalt	**95**	**72**	**23**

(Källa: Enkätstudie)

Det totala antalet som svarat på webbenkäten är 98 stycken, bland dem har vi fått ett internt bortfall på 3 personer. Bortfallet beror på att en person inte hade någon dator i hemmet och två personer använde sig av ett annat operativsystem än Windows. Eftersom vi har använt oss av snöbollsurval för att nå våra respondenter kan vi rimligen anta att ett externt bortfall har förekommit, detta anser vi dock inte vara av betydelse för att uppnå syftet med vår studie (Ejlertsson 1996).

Av de 95 respondenterna är tre fjärdedelar män och en fjärdedel kvinnor. Den största åldersgruppen är 10-24 år som utgör cirka 45 procent, tätt följd av gruppen 25-34 år som står för knappt 36 procent. Vi är väl medvetna om snedfördelning när det gäller kön och ålder för personer som använder hemdatorer, se tabell 6.1. Den ojämna fördelningen beror troligtvis på att vi i vår snöbollsteknik fångat upp en större andel yngre människor, och även en större andel män än kvinnor. Trots det tror vi inte att

resultatet kommer att ge en allt för missvisande bild av verkligheten. Detta stödjer vi med att SCB i sin rapport *Privatpersoners användning av datorer och Internet 2003* (2004a:8) säger att ju äldre personen är desto mindre tillgång har han/hon till en dator i hemmet. Personer i åldern 16-44 år är de som under tidsperioden 1994-2002 i störst utsträckning hade tillgång till en hemdator. År 2002 var det cirka 85 procent bland de i åldern 16-44 år som hade en PC i hemmet medan samma andel bland de i åldern 65-84 år var cirka 25 procent. Det som skulle kunna kritiseras är den stora svarsskillnaden mellan kvinnor och män. Men även här säger SCB att det finns en skillnad i användning. Cirka 66 procent kvinnor, i åldern 16-84 år, hade en dator medan samma siffra var cirka 74 procent för män. (SCB 2004a:8) För att inga missförstånd ska uppstå kommer vi inte att jämföra skillnaden mellan kvinnor och män i antal utan använda oss av procentandelar inom respektive grupp, det samma gäller för resultat mellan åldersgrupper.

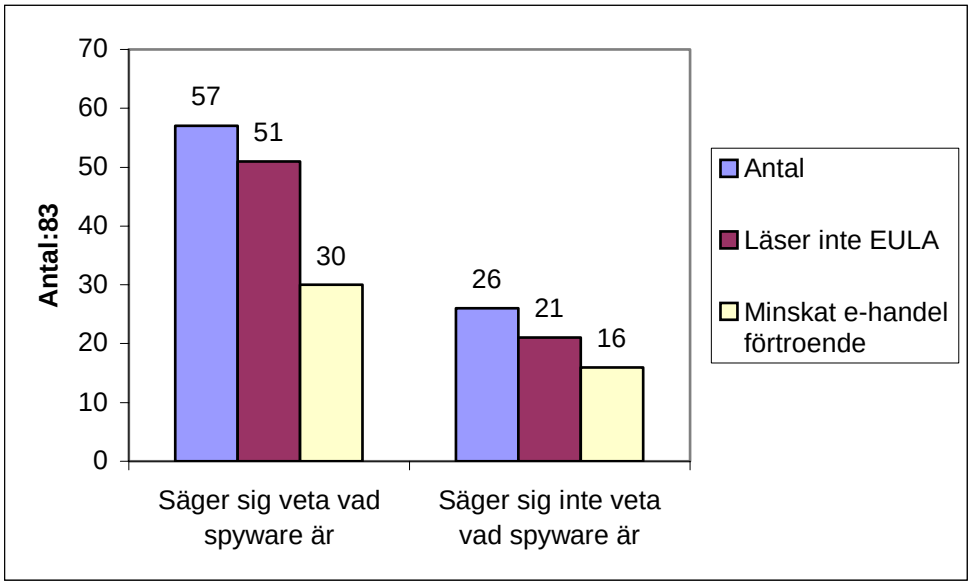
Datorvanan hos våra respondenter är mycket god, nästan 94 procent har haft tillgång till en hemdator i mer än fyra år. Den största gruppen, cirka 48 procent av samtliga tillfrågade, har haft en dator i hemmet i 8-15 år. Av de operativsystem som används har Windows XP en överväldigande majoritet, då det används av cirka 85 procent av de svarande. Bland de webbläsare som används är det två alternativ som utmärker sig, Internet Explorer med drygt 65 procent och Mozilla/Firefox med mer än 28 procent, se bilaga 2:3.

Enligt vår enkätstudie är det oväntat många, hela 52,5 procent av de tillfrågade, som är uppkopplade mot Internet mer än fem timmar dagligen. Jämförs resultatet med SCB:s studie (2004a:61 tabell 33.3) över hur många timmar personer använt Internet per vecka i januari-mars 2003 ser vi att motsvarande siffra är betydligt lägre. Detta tolkar vi som att vår fråga: ”Ungefär hur lång tid är du uppkopplad mot Internet dagligen?”, troligtvis har misstolkats. Vi var intresserade av hur länge respondenterna ”aktivt” utnyttjar Internet per dag, men då det räcker att datorn bara är igång för att den ska vara uppkopplad, kan detta ha bidragit till ett annat svar än vad vi hade tänkt oss. På grund av detta har vi valt att bortse ifrån den här frågan när vi analyserat vårt material.

De sista fem frågorna är konstruerade med hjälp av en Likertskala och har ställts i form av påståenden som ska besvaras på en femgradig skala, från ”Instämmer helt” till

”Instämmer inte alls”, se bilaga 1 fråga 16-20. För att underlätta för läsaren har vi valt att tolka de två svaren som ligger på den övre halvan ”Instämmer helt” och ”Instämmer delvis” som positiva och de på den undre halvan ”Instämmer till viss del” och Instämmer inte alls” som negativa. Vi har också valt att bortse från de som har svarat ”Varken eller” i enkäten på grund av att de är svårt att tolka dessa svar detta medför att antalet i diagrammen kan variera, men fullständiga svar finns tillgängliga i bilaga 2.

6.1. Upplever hemanvändaren spyware som ett hot?



Figur 6.1 Användarnas uppfattning om spyware (Källa: Enkätstudie).

När det gäller användarnas medvetenhet om spyware säger 60 procent av de tillfrågade sig veta vilka hot spionprogram utgör, se bilaga 2:12. Bland dem som säger att de är medvetna om vad spyware är borde också många känna till att spionprogram ofta förekommer i shareware- och freewareprogram. Trots detta är det inte många som läser igenom EULA. Drygt 89 procent av dem som påstod sig vara medvetna om vad spionapplikationer är uppgav att de inte läser EULA, se figur 6.1. När vi frågade samma grupp ifall deras förtroende för e-handel minskat på grund av spyware, framhöll 53 procent att spyware påverkat deras förtroende för e-handel negativt, se bilaga 2:16.

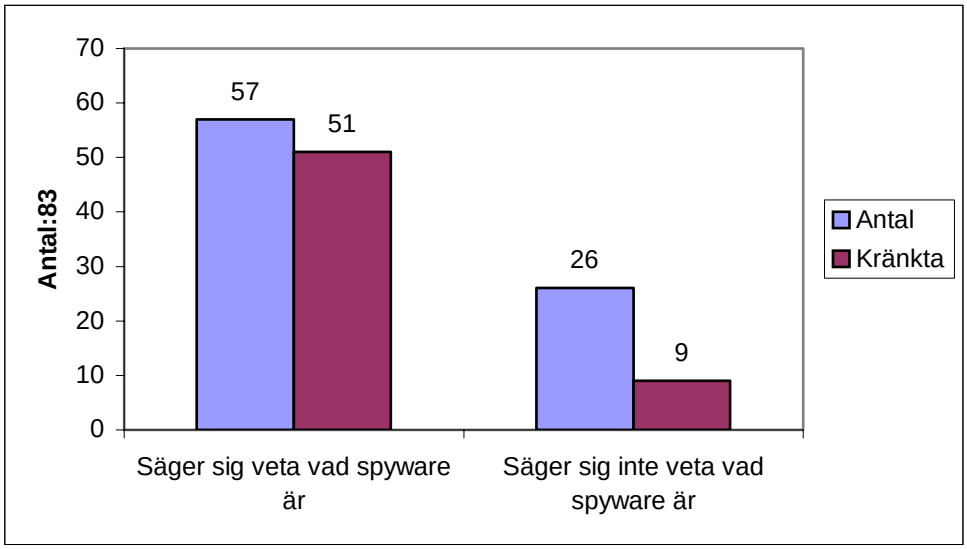
Det var 27 procent av de tillfrågade som sa att de inte visste vilka risker spionprogram medför. Eftersom de inte är medvetna om innebörden av spyware är det inte så konstigt att 81 procent av dem inte läser EULA. Däremot verkar deras förtroende för e-handel

minskat drastiskt, hela 62 procent har fått minskat förtroende för e-handel på grund av spionprogram, se figur 6.1.
Ur ovanstående resonemang drar vi slutsatsen att de flesta människors medvetenhet om spyware är låg. Att förtroendet för e-handel minskar om användaren har större medvetenhet om riskerna med spyware, är inte så egendomligt. Men att samma personer samtidigt säger att de inte läser EULA är motsägelsefullt. Frågan är därför om dessa användares medvetenhet är så stor som de säger att den är.

Det är underligt att förtroende för e-handel hos dem som inte är medvetna om spionapplikationers risker har minskat hos pass så många som 62 procent av dess respondenter. Förklaringen till detta kan vara att många medier pekar ut Internetanvändning som en stor säkerhetsrisk med datavirus som ett återkommande tema. Eftersom spyware är ett negativt laddat begrepp så är det lätt att påverkas av det, utan att egentligen veta vad det innebär.

Av det totala antalet i undersökningen hade 73 procent någon gång varit smittad av spionprogram. Jämför vi denna grupp mot dem som säger att de aldrig varit smittade, ser vi att de som har varit infekterade i högre utsträckning använder sig av antispyware-verktyg och anser sig veta mer om risker och hot, än de som aldrig varit infekterade av spyware.

6.2. Hemanvändaren och integritet

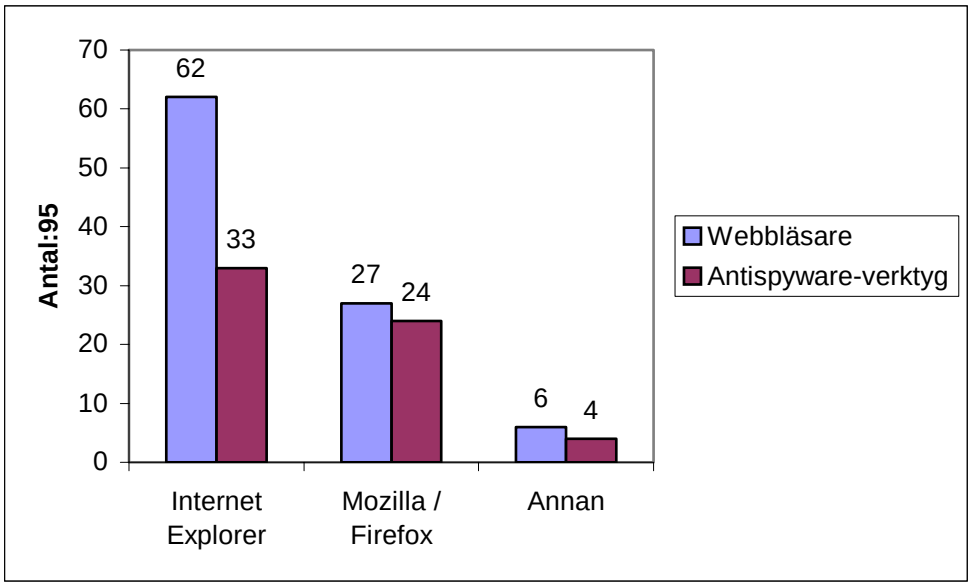


Figur 6.2 Användarnas uppfattning om spyware och integritet (Källa: Enkätstudie).

När det gäller integritetsfrågan ser vi att hela 89 procent av den grupp som är medvetna om spyware och dess effekter känner att spionapplikationer hotar deras personliga integritet. Medan den grupp som inte vet vad spionprogram innebär, inte heller verkar känna att deras personliga integritet hotas nämnvärt, endast cirka 35 procent säger att de känner att spionapplikationer kan kränka deras integritet. Se figur 6.2. Dock är antalet som svarat att de inte vet vad spyware innebär och sedan svarat ”Varken eller” på frågan om integritet relativt stort. Detta tyder på att de inte är tillräckligt insatta i ämnet för att ta ställning i frågan.

En annan intressant aspekt är att nästan tre av fyra personer av dem som säger att deras personliga integritet hotas av spionapplikationer använder sig av antispyware-program. Detta medan bara var tredje person som inte känner sig hotade av spyware nyttjar antispion-program.

6.3. Hur skyddar sig hemanvändaren mot spyware?



Figur 6.3 Webbläsare och antispyware-verktyg hos användarna (Källa: Enkätstudie).

IE (Internet Explorer) utgör en stor säkerhetsrisk och är den webbläsare som utsätts för flest attacker av virus och spyware (Hamm 2005, Gaskin 2005). Trots detta visar vår undersökning att IE är den webbläsare som har flest användare, av de 95 personer som

deltar i undersökningen använder sig 62 stycken av den. Av dessa är det många som använder sig av traditionella skydd, cirka 77 procent anger att de är skyddade av en brandvägg och nästan 84 procent har ett antivirus-program installerat.

Drygt hälften av IE-användarna har ett eller flera antispyware-verktyg, se figur 6.3, vilket gör att nästan varannan person saknar skydd mot spyware. Det här tolkar vi som att IE-användarna är medvetna om de risker virus utgör och är noga med att skydda sig mot dessa, medan spionprogram ännu inte ses som ett allvarligt hot mot säkerheten. Detta styrker vi med hjälp av svaret på frågan ifall de tillfrågade vet vilka hot och risker spionapplikationer utgör, se bilaga 2:12. Där 42 procent av IE-användarna svarar att de är medvetna om hoten från spionprogram medan 40 procent säger att de inte är det.

Den grupp som använder Mozilla/Firefox visar ungefär samma goda tendenser som IE-användarna i fråga om traditionella skydd, med 75 procent som har antivirus-program och cirka 88 procent som använder brandvägg. Det är när vi kommer in på frågan om användningen av antispyware-program som vi ser en markant skillnad mot de som använder IE, se figur 6.3. Hela 89 procent av Mozilla/Firefox-gruppen har ett eller flera antispyware-program på sin hemdator. Vi tyder detta som att Mozilla/Firefox-användaren i hög grad är medveten om vilka hot som spionapplikationer utgör. Detta grundar vi på att 96 procent av dessa användare anger att de inser riskerna med spyware. Samma diskussion gäller för de användare som har andra webbläsare än de vi diskuterat ovan.

Rent generellt så har män och kvinnor samma skydd när det gäller brandväggar och antivirus-program. Vår enkätundersökning visar dock att män i högre utsträckning än kvinnor använder sig av antispyware-program. Hela 75 procent av männen har ett eller flera antispion-program installerade medan samma siffra för kvinnor är drygt 30 procent. Av de som har antispyware-program på datorn, görs aktiva sökningar efter spionapplikationer ungefär lika sällan av både kvinnor och män. De flesta söker igenom sin dator mindre än en gång i veckan. Lite drygt två tredjedelar av männen säger sig veta vilka risker spyware utgör, siffran hos kvinnorna är en tredjedel. Vår tolkning är därför att män är något mer riskmedvetna än kvinnor när det gäller spyware.

Det finns även en skillnad i ålder när det gäller frågan om skydd mot spionprogram. I åldersgruppen 10-34 använder sig 71 procent av antispyware-verktyg medan samma siffra för de i åldersgruppen 35-75+ endast är 33 procent. Det här tolkar vi som att medvetenhetsgraden om riskerna med spyware är större hos yngre människor. Detta bekräftar vi med hjälp av svaret på frågan ifall de tillfrågade vet vilka hot och risker spionapplikationer utgör, se bilaga 2:12. Där 68 procent i den yngre åldersgruppen svarar att de är medvetna om hoten från spionprogram samtidigt som enbart 22 procent i den äldre åldersgruppen säger att de är det.

Det finns två antispyware-verktyg som utmärker sig mer än andra bland användarna, cirka 57 procent använder sig av Ad-Aware och ungefär 23 procent av Spybot Search & Destroy, se bilaga 2:9.

6.4. Kapitelsammanfattning

Internet Explorer är den webbläsare som utsätts för flest attacker av spyware, ändå är det den som enligt vår undersökning har flest användare. Detta tyder på en låg medvetandegrad hos dessa användare. Resultatet befästs ytterligare då nästan varannan person saknar skydd mot spyware och 40 procent säger att de inte vet vilka hoten från spionprogram är. De som verkar ha högst medvetandegrad om spionapplikationer är de grupper som använder Mozilla/Firefox eller annan webbläsare utöver IE. Här är medvetandegraden så hög som 96 procent och hela 89 procent har skydd mot spyware.

En skillnad mellan kvinnor och män är noterbar, där män i högre grad än kvinnor använder sig av antispyware-program. Drygt två tredjedelar av männen och en tredjedel av kvinnorna säger sig veta vilka risker spyware utgör. Detta leder oss till slutsatsen att män är något mer riskmedvetna än kvinnor när det gäller spyware.

Spionprogram förekommer ofta i shareware- och freewareprogram därför är det viktigt att kontrollera innehållet i EULA. Dessvärre är det hela 86 procent av alla svarande som inte läser igenom licensen, även fast många av dem säger att de är medvetna om vilka risker spyware kan utgöra. Detta leder oss därför till att tro att många användares medvetenhet inte är så stor som de säger att den är.

Den som inte förstår innebörden av spyware känner inte heller något hot mot den personliga integriteten. Det gör däremot de personer som påstår sig vara medvetna om riskerna med spionapplikationer. En stor grupp personer har valt att svara ”Varken eller” på frågan om integritet. Vi tolkar det som att dessa personer inte är tillräckligt insatta i ämnet för att ta ställning i frågan, vilket indirekt tyder på en låg medvetenhet om spionprogram hos respondenterna.

De som någon gång har varit smittad av spyware använder i högre utsträckning sig av antispion-program och anser sig veta mer om risker och hot, än de som aldrig haft spywareinfektion. Tolkningen vi gör av detta är att smitta måste ske innan spyware upplevs som ett hot.

7. Diskussion

I det här kapitlet kommer vi att diskutera resultaten av våran studie samt ge förslag på framtida forskning inom området.

Torsdagen den 26 maj fanns det ett reportage i tidningen Metro som handlade om ”52 program som gör din dator till en racer”. Artikeln inleddes med följande stycke: *Har du tröttnat på att lägga patiens på datorn? Känns din burk mer som en övergödd skrivmaskin än som ett väloljat vidunder? Med de här programmen får du ut mer av din dator – utan att behöva betala ett öre.* Det första som presenterades var program som var användbara när användaren var ute på Internet, här nämndes bland annat Ad-Aware, Firefox och Opera. Lite längre fram i reportaget gavs det förslag på fildelningsprogram, en programvara som vi tidigare nämnt utsätts ofta för piggybacking, här presenterades bland annat programmen Lime Wire och Kazaa. Övrig information rörde bland annat program för spel, foto, kommunikation och mediaspelare. (Persson 2005:18-19)

Datoranvändaren uppmanades alltså för det första att ladda hem freeware- och sharewareprogram, vilka ofta innehåller spyware. Dessutom framhålls Kazaa som ett bra fildelningsprogram, något vi inte håller med om då Kazaa är ett program som innehåller många spionapplikationer. Det positiva med artikeln är att användaren uppmanas att använda antispyware-programmet Ad-Aware och webbläsare som är säkrare än IE. Men då det enda som tas upp om spionprogram är en liten paragraf, längst ner på sidan, som sa: *Var försiktig med vad du laddar hem när du använder program för fildelning. Virus och spionprogram kan dölja sig i många filer*, är det inte säkert att personen som läser artikeln är så pass insatt i ämnet att han/hon förstår hur allvarligt problemet med spionapplikationer är. Dessutom kanske användaren enbart är intresserad av ett fildelningsprogram och eftersom spyware inte förklaras mer ingående, struntar i att ladda hem Ad-Aware som kan upptäcka en eventuell smitta. (*ibid.)*

Diskussioner som rör spionprogram, datorsäkerhet och integritet existerar på grund av den tekniska utvecklingen och på ett plan verkar det som om det Samuel Warren och Louis Brandeis (1890) befarade har slagit in (Warren & Brandeis 1890). Internet har gjort att vi behandlar information och uppgifter på ett annat sätt. Det är enbart eftersom uppgifterna finns tillgängliga på en dator uppkopplad mot Internet som spionapplikationerna kan komma åt informationen. Hade en annan person gått in i någons hem/kontor och öppnat och läst deras post eller satt in en gömd videokamera hade detta ansetts som olagligt och kränkande mot den personliga integriteten.

Enligt Brottsbalken räknas stöld som: *Den som olovligen tager vad annan tillhör med uppsåt att tillägna sig det, dömes om tillgreppet innebär skada för stöld till fängelse i högst 2 år. Är brott som i 1 § sägs att anse som grovt, skall för grov stöld dömas till fängelse, lägst 6 månader och högst 6 år* och egenmäktigt förfarande som*: Den som, i annat fall än särskilt i detta kapitel omförmäles, olovligen tager och brukar eller eljest tillgriper något, döms för egenmäktigt förfarande till böter eller fängelse i högst 6 månader. Det samma skall gälla, om någon utan tillgrepp, genom att anbringa eller bryta lås eller annorledes, olovligen rubbar annans besittning eller och med våld eller hot om våld hindrar annan i utövning av rätt att kvarhålla eller taga något* (SFS 1962, kap 8 § 1 & 8).

Internetanvändare skyddas genom EkomL som säger att: *Elektroniska kommunikationsnät får användas för att lagra eller få tillgång till information som är lagrad i en abonnents eller användares terminalutrustning endast om abonnenten eller användaren av den personuppgiftsansvarige får information om ändamålet med behandlingen och ges tillfälle att hindra sådan behandling. (SFS 2003: kap 6 § 18)* Skulle någon göra sig skyldig till ovanstående döms *den som med uppsåt eller av oaktsamhet bryter mot förbud enligt 6 kap. 17 eller 18 § …… till böter, om ansvar för brottet inte är stadgat i brottsbalken. I ringa fall skall inte dömas till ansvar.* (SFS 2003: kap 7 § 15)

Ovanstående lagtexten visar på att det rättsliga skyddet för användaren är väldigt litet. Den som begår stöld döms till fängelse upp till 2 år, skulle brottet vara grovt kan straffet bli så långt som upp till 6 år. För brott mot stöld av information på en användares dator blir straffet som högst böter, i värsta fall åtalas inte ens den skyldige.

Det är därför vikigt att inte ta allt för lätt på användningen av Internet eller datorer. Att surfa på nätet, framförallt för IE-användare, utan en bra brandvägg och ett bra antivirus- och antispyware-program är ungefär det samma som att lämna dörren olåst när du går hemifrån. Tyvärr tyder det på, i vår undersökning, att användaren måste ha blivit smittad av ett spionprogram, innan han/hon får upp ögonen för problemet och vidtar nödvändiga åtgärder. En stor del av skyddet mot spyware ligger därför i att skaffa sig kunskap. Även om det inte är nödvändigt att bli expert på området, är det viktigt att ha en förståelse för riskerna med spionapplikationer samt att använda Internet med en god portion skepticism och sunt förnuft.

Informationen om spionprogram till allmänheten måste även bli bättre, här har media en viktig roll. Dessutom måste allmänheten sätta mer press på regeringen om att användarens rättigheter och skydd ska säkras tydligare genom lag. Företag som säljer bredbandsanslutningar borde också inkludera ett antispion-program utöver brandvägg och antivirus-program, som börjar bli allt mer standard.

Men i slutändan är det ändå du själv som har ansvaret för vad som körs på din dator, om du förblir omedveten om konsekvenserna av spionprogrammen kommer du att få handskas med dessa problem i framtiden.

7.1. Fortsatta studier

Det finns otroligt många intressanta detaljer och frågor som har dykt upp under undersökningens gång. Dessvärre kan vi i den här uppsatsen inte gå in närmre på dem, en del kommer vi inte ens att kommentera. De kan dock vara värt att nämna några av dem, kanske kan de ge idéer till kommande uppsatser.

Det skulle vara intressant att gå in djupare på hur spionapplikationer fungerar tekniskt. Både hur programmen sprids och installeras samt hur de samlar in och sedan skickar information från den smittade datorn.

Ett annat område som vi inte hunnit beröra tillräckligt är lagstiftningen som rör spyware. Framför allt hur, eller om, lagarna efterlevs av spyware-företagen. Hur pass

internationella är lagarna? Finns det sätt för företagen att kringgå lagarna? Samt hur långt kan företagen gå utan att bryta lagen?

I takt med att nedladdning av laglig digital media som musik och film sprider sig, blir DRM[23] (Digital Rights Management) mer intressant att titta på. Frågan inom detta ämne är hur antispyware-företagen får sina program att skilja adware från spyware och hur vi förhindrar att spionapplikationer inte utnyttjar de säkerhetsluckor som DRM öppnar. (Gaskin 2005)

Ett mycket intressant område hade även varit att titta närmre på spyware-företagen. Hur insamlat material hanteras, genom vilka kanaler det sprids och vilka vinster detta genererar.

[23]Tekniska lösningar som syftar till skydda rättigheterna, främst upphovsrätten, till ett verk i digital form, till exempel kopieringsskydd.

8. Sammanfattning

Med den här uppsatsen har vi hoppats på att kunna ge en bredare bild av vad spionprogram är och vilka hot de utgör. Vidare ville vi undersöka hur medveten hemanvändaren är om dessa problem. Spyware är program som utan användares vetskap installeras eller körs på användarens dator och på olika sätt samlar eller sprider personlig information om användaren. Det kan röra sig om allt från enkla och associerade cookies till applikationsbaserade spionprogram. Eftersom själva poängen med spionprogram är att stjäla information, kan det vara svårt att upptäcka om datorn blivit smittad.

De vanligaste verktygen för att skydda sig mot spionprogram är med hjälp av en brandvägg, ett antivirus- eller ett antispion-program. Spyware förekommer ofta i shareware- och freewareprogram det är därför viktigt att kontrollera innehållet i EULA. Andra enkla åtgärder är att byta webbläsare, om Internet Explorer används, eller att inaktivera Java och ActiveX. En stor del av skyddet mot spionprogram ligger dock i att användaren ökar sin medvetenhet inom ämnet.

De grupper som verkar vara mest medveten om spyware är de med andra webbläsare än Internet Explorer, de som någon gång varit utsatta för smitta samt yngre personer, framförallt män.

9. Referensförteckning

Affero (2005) http://www.affero.org/, 2005-05-22

Ames, Wes (2004) Understanding Spyware: Risk and Response. *IT Professional* vol. 6, nr. 5, ss. 25-29.

Boldt, Martin – Carlsson, Bengt & Jacobsson, Andreas (2004) *Exploring Spyware Effects.* School of Engineering, Blekinge Institute of Technology, Ronneby, Sweden.

Bryman, Alan - Bresnen, Michael - Beardsworth, Alan & Keil, Teresa (1988) Qualitative Research and the Study of Leadership. *Human Relations,* vol. 41, Nr. 1, ss. 13-30.

Bryman, Alan (1997*) Kvantitet och kvalitet i samhällsvetenskaplig forskning*. Studentlitteratur, Lund.

Bryman, Alan (2002) *Samhällsvetenskapliga metoder*. Liber ekonomi, Malmö.

Chow, Sherman S.M. – Hui, Lucas C.K. - Yiu, S.M. – Chow, K.P. & Lui, Richard W.C. (2004) *A generic anti-spyware solution by access control list at kernel level.* Department of Computer Science and Information Systems, The University of Hong Kong, Hong Kong.

Collste, Göran (1997) Personlig integritet - Integritet Offentlighet Informationsteknik. I *SOU 1997:39, bilaga 4.*

Dahmström, Karin (2000) *Från Datainsamling Till Rapport –Att Göra En Statistisk Undersökning*. Studentlitteratur, Lund.

Datainspektionen (2005a) http://www.datainspektionen.se/lagar/pul.shtml, 2005-05-18.

Datainspektionen (2005b) http://www.datainspektionen.se, 2005-05-30.

Download.com (2005) http://www.download.com/1200-2023-5139070.html, 2005-05-15.

Dwan, Berni (2005) Pervasive spyware. *Network Security*, vol. 2005, nr. 1, s. 19.

Ejlertsson, Göran (1996) *Enkäten i praktiken – En handbok i enkätmetodik.* Studentlitteratur, Lund.

Eklund, Johan - Josefsson, Markus & Nilsson, Marcus (2004) *Beslutsprocessen under anskaffning & implementation av verktyg för business intelligence*. Institutionen för Informatik, Lunds universitet.

Eriksson, Lars T. & Wiedersheim-Paul, Finn (1991) *Att utreda, forska och rapportera.* Liber ekonomi/Almqvist & Wiksell, Malmö.

Esaiasson, Peter - Gilljam, Mikael - Oscarsson, Henrik & Wängnerud, Lena (2002) *Metodpraktikan, Konsten att studera samhälle, individ och marknad*. Norstedts Juridik, Stockholm.

Eurodex (2005) http://www.eurodex.se/spector/, 2005-05-30.

Freeman, Ted - Mikkelsen, Britha - Bonde, Ane – Forti, Sarah – Huda, Mirza – Keller, Bonnie – Possing, Susanne – Schoeman, Kgotso – Serote, Pethu & Woroniuk, Beth (2003) *Reflection on Experiences of Evalutation Gender Equality.* Elanders Novum, Stockholm.

Gaskin, James (2005) 10 ways to STOP spyware. *Network World*, vol. 22, nr. 12, ss. 16-18.

Greiner, Lynn (2005) Playing With Firewalls. *Computing Canada*, vol. 31, nr. 1, ss. 18-19.
Halvorsen, Knut (1992) *Samhällsvetenskaplig metod.* Studentlitteratur, Lund.
Hamm, Steve (2005) Move Over, Internet Explorer. *Business Week*, s. 89.
Hayes, Nicky (2000) *Doing Psychological Research: Gathering and Analysing Data*. Open University Press, Buckingham.
Holme, Idar M. & Solvang, Bernt K. (1997) *Forskningsmetodik*. Studentlitteratur, Lund.
Hormozi, Amir M. (2005) Cookies and Privacy. *Information Systems Security*, vol. 13, nr. 6, ss. 51-59.
Klang, Mathias (2004) Spyware -- the ethics of covert software. *Ethics and Information Technology*, vol 6, nr. 3, ss. 193-202.
Levy, Elias & Arce, Iván (2004) More Bang For the Bug - An Account of 2003's Attack Trends. *IEEE Security & Privacy*, vol. 2, nr. 1, ss. 66-68.
Liljestrand, Tia & Lindgren, Karin (2003) Personlig integritet i arbetslivet. Institutionen för Informatik, Handelshögskolan, Göteborgs Universitet.
Lundahl, Ulf & Skärvad, Per-Hugo (1999) *Utredningsmetodik för samhällsvetare och ekonomer*. Studentlitteratur, Lund.
McArthur, Robert L (2001) Reasonable expectations of privacy. *Ethics and Information Technology*, vol. 3, nr 2, ss. 123-128.
McCardle, Michael (2003) *How Spyware fits into Defense in Depth*. SANS Institute.
McWilliams, Brian (2002) Anti-Spyware Program Targeted By Multimedia Player – Ad-Aware. *Newsbytes News Network*, April 23.
Messmer, Ellen (2004) Debating what is spyware. *Network World*, vol. 2, nr. 45, s. 14.
Nationalencyklopedin (2005a) http://www.ne.se/jsp/search/article.jsp?i_art_id=147107&i_word=cookie, sökord: cookie, 2005-05-16.
Nationalencyklopedin (2005b) http://www.ne.se/jsp/search/article.jsp?i_art_id=241333&i_word=Likertskala, sökord: likterskala, 2005-05-16.
Nationalencyklopedin (2005c) http://www.ne.se/jsp/search/article.jsp?i_art_id=212289&i_word=integritet, sökord: integritet, 2005-05-18.
Nationalencyklopedin (2005d) http://www.ne.se/jsp/search/article.jsp?i_art_id=140026&i_word=cache, sökord: cache, 2005-05-20.
Nationalencyklopedin (2005e) http://www.ne.se/jsp/search/article.jsp?i_art_id=495270&i_word=banner, sökord: banner, 2005-05-23.
Nationalencyklopedin (2005f) http://www.ne.se/jsp/search/article.jsp?i_art_id=174815&i_word=freeware, sökord: freeware/shareware, 2005-05-23.
Newsfactor Network (2005) http://www.newsfactor.com/perl/story/16664.html#story-start, 2005-05-15.
Pagina.se (2005) http://www.pagina.se/itord/default.asp?id=5086, 2005-05-15.
Patel, Runa & Davidsson, Bo (2003) *Forskningsmetodikens grunder: Att planera, genomföra och rapportera en undersökning*. Studentlitteratur, Lund.
Persson, Anders (2005) 52 program som gör din dator till en racer. *Metro Skåne*, 2005-05-26, ss.18-19.
Post & Telestyrelsen (2005) *Spionprogram och andra närliggande företeelser*. Rapportnummer PTS-ER-2005:15.
Robson, Colin (2002) *Real World Research. 2nd Edition.* Maden, Blackwell Publishing.
Statistiska Central Byrån (2004a) *Privatpersoners användning av datorer och Internet 2003*. Statistiska Centralbyrån, Stockholm.
Statistiska Central Byrån (2004b) *Privatpersoners användning av datorer och Internet 2004*. Statistiska Centralbyrån, Stockholm.

Svensk Författningssamling (1962) *Brottsbalken*. SFS 1962:700.
Svensk Författningssamling (1998) *Personuppgiftslagen*. SFS 1998:204.
Svensk Författningssamling (2003) *Lagen om elektronisk kommunikation*. SFS 2003:389.
Soat, John (2005) The FCC, VoIP, And Spyware-Oh, My! *InformationWeek*, s. 55.
Sourceforge (2005) http://sourceforge.net/index.php, 2005-05-05.
Stallings, William (2003) *Network Security Essentials – Applications and Standards*. Prentice Hall, Upper Saddle River.
Svensson, Per-Gunnar & Starrin, Bengt (1996) *Kvalitativa studier i teori och praktik*. Studentlitteratur, Lund.
Sveriges Radio (2003) Spana på älskare och arbetstagare. *Sveriges Radio - Efter 12*, med Päivi Kotka. Sveriges Radios sändning den 2 februari 2003.
Sveriges Television (2005) http://svt.se/svt/jsp/Crosslink.jsp?d=30624, 2005-05-30. Rapports nyhetssändning den 29 maj 2005, klockan 19.30.
Tauson, Maria (2005) Spyware håller koll på dina datorvanor. *DATUM*, Umeå Universitets datorcentral, nr.118.
The Computer Bulletin (2005) Put Spyware on the security. *The Computer Bulletin*, vol. 47, nr. 1, ss.18-19.
Tranøy, Knut E. (1986) *Vitenskapen: samfunnsmakt og livsform.* Universitetsforlaget, Oslo.
Townsend, Kevin (2003) *Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security.* Technical White Paper, Pest Patrol.
Warren, Samuel D. & Brandeis, Louis D. (1890) The right to privacy. *Harvard Law Review*, vol. 4, ss. 193-220.
Wieslander, Johan – Boldt, Martin & Carlsson, Bengt (2003) *Investigating Spyware on the Internet.* Dept. of Software Engineering and Computer Science, Blekinge Institute of Technology, Ronneby, Sweden.
Wieslander, Johan – Boldt, Martin & Carlsson, Bengt (2004) *Privacy-Invasive Software In File-Sharing Tools*. School of Engineering, Blekinge Institute of Technology, Ronneby, Sweden.

Bilaga 1:1

Lunds Universitet Institutionen för Informatik

Hej
Vi är två studenter vid namn Kristofer Nordin och Henrik Isaksson som studerar Informatik på Lunds Universitet. Vi håller just nu på att skriva vår kandidatuppsats som handlar om Spyware och vilka risker och hot detta innebär för hemmanvändare av PC-datorer.

Syftet med denna enkät är att ta reda på hemmanvändares medvetandegrad, riskmedvetande och attityd mot Spyware. Enkäten består av 20 enkla frågor, uppdelade på sju sidor och tar mellan tre och fem minuter att fylla i. Beroende på hur du svarar på vissa frågor kan enkäten automatiskt hoppa över någon fråga eller gå direkt till slutet, detta är helt normalt.

Dina svar kommer hanteras med anonymitet i åtanke, och lagras i en databas som inte tillåter åtkomst åt data som gör det möjligt för oss att peka ut enskilda personer i undersökningen.

För att svara på enkäten, följ följande länk:
http://www.isen.se/enkat/survey.php?sid=28
Glöm inte avsluta enkäten genom att trycka på "Finish"

Frågor, kommentarer och synpunkter tas gärna emot via e-mail:
websurvey@isen.se

Vi uppskattar verkligen att du tar dig tid för att svara på våran enkät, då den är till stor hjälp för oss under vårat arbete.

Tack på förhand!
/Kristofer och Henrik

Verktyget som används för webenkäten är nedladdat gratis från open source communityt Sourceforge och heter UCCASS v.1.8.0

För att hålla reda på vem som redan svarat på enkäten eller inte använder vi oss av en enkel cookie

Serverplatsen är utlånad av den idéella spelföreningen ISEN.

Bilaga 1:2

Spyware enkät

1. [*] Kön?

- ☐ Man
- ☐ Kvinna

2. [*] Ålder?

- ☐ 10-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-74
- ☐ 75+

3. [*] Hur länge har du haft en PC i hemmet?

Ange hur länge, har du inte tillgång till en PC i hemmet kommer du tas direkt till slutet av enkäten.

- ☐ 0 - 6 månader
- ☐ 6 månader - 2 år
- ☐ 2 - 4 år
- ☐ 4 - 8 år
- ☐ 8 - 15 år
- ☐ över 15 år
- ☐ Har inte tillgång till PC hemma

Bilaga 1:3

4. [*] Vilket operativsystem använder du?

Ange vilket operativsystem du använder mest. Om du inte använder Windows tas du direkt till slutet av enkäten.

- ☐ Windows 95 / 98 / ME
- ☐ Windows XP
- ☐ Windows NT / 2000
- ☐ Använder Windows men vet ej vilken version
- ☐ Använder ej Windows

5. [*] Vilken webläsare använder du?

Ange vilken webläsare du använder, använder du flera så välj den du använder mest.

- ☐ Internet Explorer
- ☐ Netscape Navigator
- ☐ Mozilla / Mozilla Firefox
- ☐ Opera
- ☐ Annan
- ☐ Vet ej

6. [*] Ungefär hur lång tid är du uppkopplad mot Internet dagligen?

- ☐ 0 - 30 minuter
- ☐ 30 minuter - 1 timme
- ☐ 1 - 2 timmar
- ☐ 2 - 3 timmar
- ☐ 3 - 5 timmar
- ☐ Mer än fem timmar

7. [*] Har du något antivirusprogram installerat på din hemdator?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

Bilaga 1:4

8. [*] Skyddar ditt antivirusprogram mot Spyware?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

9. [*] Är din hemdator skyddad av någon brandvägg?

Ange om du är skyddad av någon brandvägg

- ☐ Ja, jag är skyddad av en eller flera brandväggar
- ☐ Nej, jag är inte skyddad av någon brandvägg
- ☐ Vet ej om jag är skyddad av någon brandvägg

10. [*] Använder du dig av fildelningsprogram?

- ☐ Ja
- ☐ Nej
- ☐ Vet ej

11. [*] Vilket fildelningsprogram använder du?

Använder du flera fildelningsprogram, så välj det du använder mest.

- ☐ Direct Connect
- ☐ eMule (eller liknande eDonkey variant)
- ☐ Gnutella-variant (LimeWire, BearShare, Swapper etc)
- ☐ iMesh
- ☐ Kazaa / Kazaa lite
- ☐ Morpheus
- ☐ Soulseek
- ☐ WinMX
- ☐ Bit Torrent
- ☐ Annat
- ☐ Vet ej

Bilaga 1:5

12. [*] Använder du något antispyware-program?

Ange om du använder ett eller flera renodlade antispyware-program, räkna ej med eventuellt antivirusprogram.

- ☐ Ja, jag använder ett
- ☐ Ja, jag använder flera
- ☐ Nej, jag använder inget
- ☐ Vet ej

13. [*] Vilket eller vilka antispywareprogram använder du?

Ange vilket eller vilka antispywareprogram du använder.

- ☐ AdAware
- ☐ CounterSpy
- ☐ Cyberpartol
- ☐ Giant
- ☐ McAfee
- ☐ Pest Patrol
- ☐ Punk Buster
- ☐ Spybot Search & Destroy
- ☐ Spy Sweeper
- ☐ Spyware Eliminator
- ☐ Annat
- ☐ Vet ej

14. [*] Brukar du aktivt söka igenom din dator efter spyware?

Ange hur ofta du söker igenom din dator, gäller ej genomsökningar som utförs automatiskt av ditt program

- ☐ Dagligen
- ☐ Flera gånger per vecka
- ☐ Varje vecka
- ☐ En till två gånger per månad
- ☐ En gång i månaden eller mer sällan
- ☐ Aldrig

Bilaga 1:6

15. [*] Har du, eller har du haft, spyware på din dator?

Ange om du tror att du har någon slags Spyware-infektion på din dator:

- ☐ Ja, helt säkert
- ☐ Ja, det tror jag
- ☐ Vet ej
- ☐ Nej, det tror jag inte
- ☐ Nej, helt säkert inte

För följande påståenden, ange på en skala från ett till fem hur väl du tycker de stämmer in på dig

16. [*] Jag vet vilka hot och säkerhetsrisker Spyware utgör

- ☐ Instämmer helt
- ☐ Instämmer delvis
- ☐ Varken eller
- ☐ Instämmer till viss del
- ☐ Instämmer inte alls

17. [*] Jag känner att min personliga integritet kan kränkas av Spyware

- ☐ Instämmer helt
- ☐ Instämmer delvis
- ☐ Varken eller
- ☐ Instämmer till viss del
- ☐ Instämmer inte alls

Bilaga 1:7

18. [*] Spyware är mer ett irritationsmoment än en säkerhetsrisk

- ☐ Instämmer helt
- ☐ Instämmer delvis
- ☐ Varken eller
- ☐ Instämmer till viss del
- ☐ Instämmer inte alls

19. [*] Jag läser alltid igenom hela EULA (end-user license agreement) innan jag installerar ett nytt program.

- ☐ Instämmer helt
- ☐ Instämmer delvis
- ☐ Varken eller
- ☐ Instämmer till viss del
- ☐ Instämmer inte alls

20. [*] Mitt förtroende för e-handel och onlinetransaktioner har minskat på grund av att jag tror att spyware kan förekomma på min dator.

- ☐ Instämmer helt
- ☐ Instämmer delvis
- ☐ Varken eller
- ☐ Instämmer till viss del
- ☐ Instämmer inte alls

Bilaga 1:8

Lunds Universitet

Institutionen för Informatik

Färdigt
Vi har nu mottagit dina svar, tack så mycket för din medverkan! Ditt deltagande hjälper oss få PC-användarens inställning till Spyware.

Har du några kommentarer, någon fråga eller tycker du att vi missat något? Vi tar gärna emot feedback! Maila oss på websurvey@isen.se

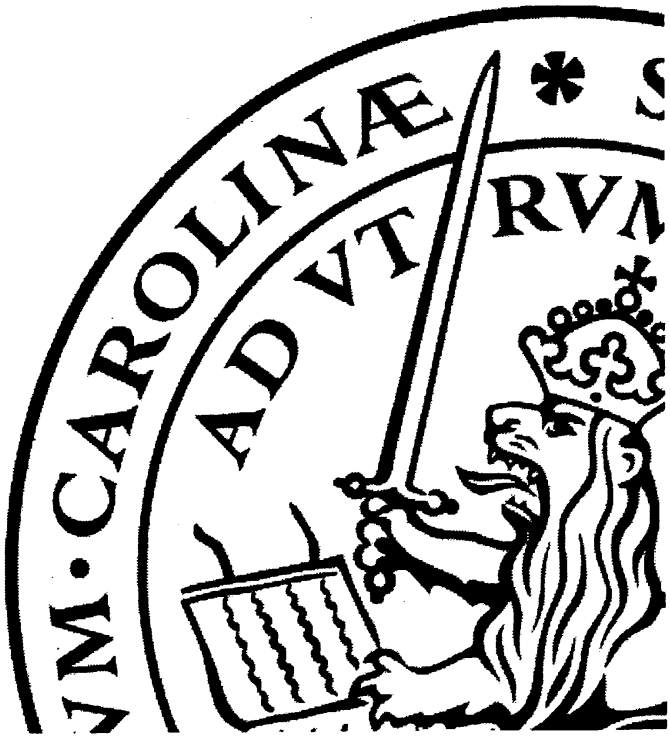
Väl mött!

Kristofer Nordin och Henrik Isaksson

Verktyget som används för webenkäten är nedladdat gratis från open source communityt Sourceforge och heter UCCASS v.1.8.0

För att hålla reda på vem som redan svarat på enkäten eller inte använder vi oss av en enkel cookie

Serverplatsen är utlånad av den idéella spelföreningen ISEN.



Bilaga 2:1

Tabell 1. Fråga 1 och 2, Ålder och Kön.

Ålder	Kvinna	Man	Totalt
10-24	8	36	44
25-34	7	28	35
35-44	3	1	4
45-54	4	5	9
55-74	1	5	6
76+	0	0	0
Totalt	23	75	98

Tabell 2. Fråga 3, Hur länge har du haft en PC i hemmet?

	Man	Kvinna	Totalt
0-6 månader	0	0	0
6 månader - 2 år	2	1	3
2 - 4 år	2	1	3
4 - 8 år	21	4	25
8 - 15 år	34	13	47
Över 15 år	15	4	19
Har inte tillgång till PC hemma	1	0	1

Tabell 3. Fråga 3, Hur länge har du haft en PC i hemmet? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
0-6 månader	0	0	0	0	0	0
6 månader - 2 år	2	0	0	0	0	2
2 - 4 år	1	1	0	0	0	2
4 - 8 år	12	6	1	1	1	21
8 - 15 år	15	13	0	2	4	34
Över 15 år	6	8	0	1	0	15
Har inte tillgång till PC hemma	0	0	0	1	0	1

Tabell 4. Fråga 3, Hur länge har du haft en PC i hemmet? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
0-6 månader	0	0	0	0	0	0
6 månader - 2 år	0	0	0	1	0	1
2 - 4 år	0	0	1	0	0	1
4 - 8 år	1	3	0	0	0	4
8 - 15 år	6	3	1	2	1	13
Över 15 år	1	1	1	1	0	4
Har inte tillgång till PC hemma	0	0	0	0	0	0

Bilaga 2:2

Tabell 5. Fråga 4, Vilket operativsystem använder du?

	Man	Kvinna	Totalt
Windows 95 / 98 / ME	5	2	7
Windows XP	63	18	81
Windows NT / 2000	3	3	6
Använder Windows, vet ej vilken version	1	0	1
Använder ej Windows	2	0	2

Tabell 6. Fråga 4, Vilket operativsystem använder du? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Windows 95 / 98 / ME	2	1	1	1	0	5
Windows XP	31	25	0	2	5	63
Windows NT / 2000	2	1	0	0	0	3
Använder Windows, vet ej vilken version	0	0	0	1	0	1
Använder ej Windows	1	1	0	0	0	2

Tabell 7. Fråga 4, Vilket operativsystem använder du? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Windows 95 / 98 / ME	1	0	0	1	0	2
Windows XP	7	5	3	2	1	18
Windows NT / 2000	0	2	0	1	0	3
Använder Windows, vet ej vilken version	0	0	0	0	0	0
Använder ej Windows	0	0	0	0	0	0

Bilaga 2:3

Tabell 8. Fråga 5, Vilken webbläsare använder du?

	Man	Kvinna	Totalt
Internet Explorer	40	22	62
Netscape Navigator	1	0	1
Mozilla / Mozilla Firefox	26	1	27
Opera	2	0	2
Annan	3	0	3
Vet ej	0	0	0

Tabell 9. Fråga 5, Vilken webbläsare använder du? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Internet Explorer	18	13	1	3	5	40
Netscape Navigator	1	0	0	0	0	1
Mozilla / Mozilla Firefox	12	13	0	1	0	26
Opera	2	0	0	0	0	2
Annan	2	1	0	0	0	3
Vet ej	0	0	0	0	0	0

Tabell 10. Fråga 5, Vilken webbläsare använder du? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Internet Explorer	8	6	3	4	1	22
Netscape Navigator	0	0	0	0	0	0
Mozilla / Mozilla Firefox	0	1	0	0	0	1
Opera	0	0	0	0	0	0
Annan	0	0	0	0	0	0
Vet ej	0	0	0	0	0	0

Bilaga 2:4

Tabell 11. Fråga 6, Ungefär hur lång tid är du uppkopplad mot Internet dagligen?

	Man	Kvinna	Totalt
0 - 30 minuter	4	5	9
30 minuter - 1 timme	4	3	7
1 - 2 timmar	6	0	6
2 - 3 timmar	10	0	10
3 - 5 timmar	10	3	13
Mer än fem timmar	38	12	50

Tabell 12. Fråga 6, Ungefär hur lång tid är du uppkopplad mot Internet dagligen? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
0 - 30 minuter	0	0	1	1	2	4
30 minuter - 1 timme	2	1	0	1	0	4
1 - 2 timmar	2	1	0	0	3	6
2 - 3 timmar	5	5	0	0	0	10
3 - 5 timmar	5	5	0	0	0	10
Mer än fem timmar	21	15	0	2	0	38

Tabell 13. Fråga 6, Ungefär hur lång tid är du uppkopplad mot Internet dagligen? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
0 - 30 minuter	1	0	1	3	0	5
30 minuter - 1 timme	0	1	1	0	1	3
1 - 2 timmar	0	0	0	0	0	0
2 - 3 timmar	0	0	0	0	0	0
3 - 5 timmar	2	0	0	1	0	3
Mer än fem timmar	5	6	1	0	0	12

Bilaga 2:5

Tabell 14. Fråga 7, Har du något antivirusprogram installerat på din hemdator?

	Man	Kvinna	Totalt
Ja	57	20	77
Nej	13	2	15
Vet ej	2	1	3

Tabell 15. Fråga 7, Har du något antivirusprogram installerat på din hemdator? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja	25	22	1	4	5	57
Nej	9	4	0	0	0	13
Vet ej	1	1	0	0	0	2

Tabell 16. Fråga 7, Har du något antivirusprogram installerat på din hemdator? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja	8	7	2	2	1	20
Nej	0	0	1	1	0	2
Vet ej	0	0	0	1	0	1

Tabell 17. Fråga 8, Skyddar ditt antivirusprogram mot Spyware?

	Man	Kvinna	Totalt
Ja	23	6	29
Nej	19	3	22
Vet ej	15	11	26

Tabell 18. Fråga 8, Skyddar ditt antivirusprogram mot Spyware? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja	11	10	0	0	2	23
Nej	10	7	0	2	0	19
Vet ej	4	5	1	2	3	15

Tabell 19. Fråga 8, Skyddar ditt antivirusprogram mot Spyware? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja	2	2	1	1	0	6
Nej	2	1	0	0	0	3
Vet ej	4	4	1	1	1	11

Bilaga 2:6

Tabell 20. Fråga 9, Är din hemdator skyddad av någon brandvägg?

	Man	Kvinna	Totalt
Ja, jag är skyddad av en eller flera brandväggar	60	17	77
Nej, jag är inte skyddad av någon brandvägg	10	4	14
Vet ej om jag är skyddad av någon brandvägg	2	2	4

Tabell 21. Fråga 9, Är din hemdator skyddad av någon brandvägg? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja, jag är skyddad av en eller flera brandväggar	27	25	0	3	5	60
Nej, jag är inte skyddad av någon brandvägg	7	1	1	1	0	10
Vet ej om jag är skyddad av någon brandvägg	1	1	0	0	0	2

Tabell 22. Fråga 9, Är din hemdator skyddad av någon brandvägg? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja, jag är skyddad av en eller flera brandväggar	6	6	3	1	1	17
Nej, jag är inte skyddad av någon brandvägg	1	1	0	2	0	4
Vet ej om jag är skyddad av någon brandvägg	1	0	0	1	0	2

Tabell 23. Fråga 10, Använder du dig av fildelningsprogram?

	Man	Kvinna	Totalt
Ja	57	10	67
Nej	13	9	22
Vet ej	2	4	6

Tabell 24. Fråga 10, Använder du dig av fildelningsprogram? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja	30	24	0	1	2	57
Nej	4	3	0	3	3	13
Vet ej	1	0	1	0	0	2

Tabell 25. Fråga 10, Använder du dig av fildelningsprogram? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja	4	5	1	0	0	10
Nej	3	2	2	2	0	9
Vet ej	1	0	0	2	1	4

Bilaga 2:7

Tabell 26. Fråga 11, Vilket fildelningsprogram använder du? (noll-svar uteslutna i följande tabeller)

	Man	Kvinna	Totalt
Bit Torrent	12	1	13
Direct Connect	42	8	50
Kazaa / Kazaa lite	1	0	1
Morpheus	1	0	1
Annat	1	1	2
Vet ej	0	0	0

Tabell 27. Fråga 11, Vilket fildelningsprogram använder du? (noll-svar uteslutna i följande tabeller) Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Bit Torrent	5	7	0	0	0	12
Direct Connect	25	16	0	0	1	42
Kazaa / Kazaa lite	0	0	0	1	0	1
Morpheus	0	0	0	0	1	1
Annat	0	1	0	0	0	1
Vet ej	0	0	0	0	0	0

Tabell 28. Fråga 11, Vilket fildelningsprogram använder du? (noll-svar uteslutna i följande tabeller) Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Direct Connect	3	4	1	0	0	8
Kazaa / Kazaa lite	0	0	0	0	0	0
Morpheus	0	0	0	0	0	0
Bit Torrent	0	1	0	0	0	1
Annat	1	0	0	0	0	1
Vet ej	0	0	0	0	0	0

Bilaga 2:8

Tabell 29. Fråga 12: Använder du något antispyware-program?

	Man	Kvinna	Totalt
Ja, jag använder ett	39	4	43
Ja, jag använder flera	15	3	18
Nej, jag använder inget	10	7	17
Vet ej	8	9	17

Tabell 30. Fråga 12, Använder du något antispyware-program? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja, jag använder ett	22	15	0	1	1	39
Ja, jag använder flera	7	5	1	1	1	15
Nej, jag använder inget	3	6	0	1	0	10
Vet ej	3	1	0	1	3	8

Tabell 31. Fråga 12, Använder du något antispyware-program? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja, jag använder ett	2	2	0	0	0	4
Ja, jag använder flera	1	1	1	0	0	3
Nej, jag använder inget	2	1	0	4	0	7
Vet ej	3	3	2	0	1	9

Bilaga 2:9

Tabell 32. Fråga 13, Vilket eller vilka antispywareprogram använder du?

	Man	Kvinna	Totalt
AdAware	45	5	50
McAfee	3	0	3
Pest Patrol	3	0	3
Punk Buster	1	0	1
Spybot Search & Destroy	17	3	20
Spy Sweeper	1	0	1
Annat	6	2	8
Vet ej	1	0	1

Tabell 33. Fråga 13, Vilket eller vilka antispywareprogram använder du? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
AdAware	22	19	1	2	2	46
McAfee	1	2	0	0	0	3
Pest Patrol	1	1	0	0	1	3
Punk Buster	1	0	0	0	0	1
Spybot Search & Destroy	9	5	1	1	1	17
Spy Sweeper	1	0	0	0	0	1
Annat	4	2	0	0	0	6
Vet ej	1	0	0	0	0	1

Tabell 34. Fråga 13, Vilket eller vilka antispywareprogram använder du? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
AdAware	2	2	1	0	0	5
McAfee	0	0	0	0	0	0
Pest Patrol	0	0	0	0	0	0
Punk Buster	0	0	0	0	0	0
Spybot Search & Destroy	1	2	0	0	0	3
Spy Sweeper	0	0	0	0	0	0
Annat	1	0	1	0	0	2
Vet ej	0	0	0	0	0	0

Bilaga 2:10

Tabell 35. Fråga 14: Brukar du aktivt söka igenom din dator efter spyware?

	Man	Kvinna	Totalt
Dagligen	3	0	3
Flera gånger per vecka	4	1	5
Varje vecka	11	1	12
En till två gånger per månad	21	4	25
En gång i månaden eller mer sällan	13	1	14
Aldrig	2	0	2

Tabell 36. Fråga 14, Vilket eller vilka antispywareprogram använder du? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Dagligen	2	1	0	0	0	3
Flera gånger per vecka	2	0	1	1	0	4
Varje vecka	5	6	0	0	0	11
En till två gånger per månad	9	10	0	1	1	21
En gång i månaden eller mer sällan	10	3	0	0	0	13
Aldrig	1	0	0	0	1	2

Tabell 37. Fråga 14: Brukar du aktivt söka igenom din dator efter spyware? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Dagligen	0	0	0	0	0	0
Flera gånger per vecka	1	0	0	0	0	1
Varje vecka	1	0	0	0	0	1
En till två gånger per månad	1	2	1	0	0	4
En gång i månaden eller mer sällan	0	1	0	0	0	1
Aldrig	0	0	0	0	0	0

Bilaga 2:11

Tabell 38. Fråga 15: Har du, eller har du haft, spyware på din dator?

	Man	Kvinna	Totalt
Ja, helt säkert	53	5	58
Ja, det tror jag	8	3	11
Vet ej	3	9	12
Nej, det tror jag inte	5	3	8
Nej, helt säkert inte	3	3	6

Tabell 39. Fråga 15: Har du, eller har du haft, spyware på din dator? Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Ja, helt säkert	30	18	1	2	2	53
Ja, det tror jag	2	5	0	0	1	8
Vet ej	2	0	0	1	0	3
Nej, det tror jag inte	1	1	0	1	2	5
Nej, helt säkert inte	0	3	0	0	0	3

Tabell 40. Fråga 15: Har du, eller har du haft, spyware på din dator? Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Ja, helt säkert	3	2	0	0	0	5
Ja, det tror jag	1	2	0	0	0	3
Vet ej	4	1	1	3	0	9
Nej, det tror jag inte	0	1	1	0	1	3
Nej, helt säkert inte	0	1	1	1	0	3

Bilaga 2:12

Tabell 41. Fråga 16: Jag vet vilka hot och säkerhetsrisker Spyware utgör

	Man	Kvinna	Totalt
Instämmer helt	22	3	25
Instämmer delvis	27	5	32
Varken eller	10	2	12
Instämmer till viss del	6	5	11
Instämmer inte alls	7	8	15

Tabell 42. Fråga 16: Jag vet vilka hot och säkerhetsrisker Spyware utgör. Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Instämmer helt	9	12	0	1	0	22
Instämmer delvis	19	6	0	0	2	27
Varken eller	2	5	0	1	2	10
Instämmer till viss del	2	3	0	0	1	6
Instämmer inte alls	3	1	1	2	0	7

Tabell 43. Fråga 16: Jag vet vilka hot och säkerhetsrisker Spyware utgör. Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Instämmer helt	2	0	1	0	0	3
Instämmer delvis	3	2	0	0	0	5
Varken eller	0	1	0	1	0	2
Instämmer till viss del	1	3	1	0	0	5
Instämmer inte alls	2	1	1	3	1	8

Bilaga 2:13

Tabell 44. Fråga 17: Jag känner att min personliga integritet kan kränkas av Spyware

	Man	Kvinna	Totalt
Instämmer helt	28	6	34
Instämmer delvis	24	7	31
Varken eller	11	7	18
Instämmer till viss del	5	0	5
Instämmer inte alls	4	3	7

Tabell 45. Fråga 17: Jag känner att min personliga integritet kan kränkas av Spyware. Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Instämmer helt	17	9	0	1	1	28
Instämmer delvis	13	8	0	1	2	24
Varken eller	2	6	1	1	1	11
Instämmer till viss del	2	1	0	1	1	5
Instämmer inte alls	1	3	0	0	0	4

Tabell 46. Fråga 17: Jag känner att min personliga integritet kan kränkas av Spyware. Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Instämmer helt	3	2	1	0	0	6
Instämmer delvis	2	3	1	1	0	7
Varken eller	3	2	1	1	0	7
Instämmer till viss del	0	0	0	0	0	0
Instämmer inte alls	0	0	0	2	1	3

Bilaga 2:14

Tabell 47. Fråga 18: Spyware är mer ett irritationsmoment än en säkerhetsrisk

	Man	Kvinna	Totalt
Instämmer helt	12	1	13
Instämmer delvis	22	3	25
Varken eller	10	9	19
Instämmer till viss del	20	4	24
Instämmer inte alls	8	6	14

Tabell 48. Fråga 18: Spyware är mer ett irritationsmoment än en säkerhetsrisk. Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Instämmer helt	5	7	0	0	0	12
Instämmer delvis	11	8	0	2	1	22
Varken eller	5	0	1	1	3	10
Instämmer till viss del	9	9	0	1	1	20
Instämmer inte alls	5	3	0	0	0	8

Tabell 49. Fråga 18: Spyware är mer ett irritationsmoment än en säkerhetsrisk. Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Instämmer helt	0	0	0	1	0	1
Instämmer delvis	0	2	1	0	0	3
Varken eller	4	2	1	2	0	9
Instämmer till viss del	2	1	0	0	1	4
Instämmer inte alls	2	2	1	1	0	6

Bilaga 2:15

Tabell 50. Fråga 19: Jag läser alltid igenom hela EULA (end-user license agreement) innan jag installerar ett nytt program.

	Man	Kvinna	Totalt
Instämmer helt	0	1	1
Instämmer delvis	3	5	8
Varken eller	3	1	4
Instämmer till viss del	9	4	13
Instämmer inte alls	57	12	69

Tabell 51. Fråga 18: Spyware är mer ett irritationsmoment än en säkerhetsrisk. Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Instämmer helt	0	0	0	0	0	0
Instämmer delvis	1	2	0	0	0	3
Varken eller	1	2	0	0	0	3
Instämmer till viss del	5	1	0	2	1	9
Instämmer inte alls	28	22	1	2	4	57

Tabell 52. Fråga 18: Spyware är mer ett irritationsmoment än en säkerhetsrisk. Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Instämmer helt	0	0	0	1	0	1
Instämmer delvis	1	3	1	0	0	5
Varken eller	0	0	0	0	1	1
Instämmer till viss del	0	1	2	1	0	4
Instämmer inte alls	7	3	0	2	0	12

Bilaga 2:16

Tabell 53. Fråga 20: Mitt förtroende för e-handel och onlinetransaktioner har minskat på grund av att jag tror att spyware kan förekomma på min dator

	Man	Kvinna	Totalt
Instämmer helt	5	2	7
Instämmer delvis	11	3	14
Varken eller	18	4	22
Instämmer till viss del	11	5	16
Instämmer inte alls	27	9	36

Tabell 54. Fråga 20: Mitt förtroende för e-handel och onlinetransaktioner har minskat på grund av att jag tror att spyware kan förekomma på min dator. Man

Man	10-24	25-34	35-44	45-54	55-74	Tot Man
Instämmer helt	2	1	1	0	1	5
Instämmer delvis	8	2	0	1	0	11
Varken eller	7	9	0	1	1	18
Instämmer till viss del	4	4	0	1	2	11
Instämmer inte alls	14	11	0	1	1	27

Tabell 55. Fråga 20: Mitt förtroende för e-handel och onlinetransaktioner har minskat på grund av att jag tror att spyware kan förekomma på min dator. Kvinna

Kvinna	10-24	25-34	35-44	45-54	55-74	Tot Kvinna
Instämmer helt	1	0	0	1	0	2
Instämmer delvis	1	0	2	0	0	3
Varken eller	1	1	0	1	1	4
Instämmer till viss del	2	2	0	1	0	5
Instämmer inte alls	3	4	1	1	0	9