

SÄKERHETSMEDVETENHET I HEMMET

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2012

Vyacheslav Lytvynenko

Handledare: Helen Pehrsson
Examinator: Rose-Mharie Åhlfeldt

Sammanfattning

Arbetet undersöker och kartlägger säkerhetsmedvetenhet gällande IT-användning samt säkerhetsnivån hos hemanvändare. Undersökningen grundas i påståendet att en legitim användare ofta utgör en säkerhetsrisk för systemet genom brist på kunskap. Anledningen till att fokus läggs på hemanvändaren är syftet att få fram data kring användarens säkerhetsmedvetenhet i en miljö där denne inte blir påverkad av utomstående faktorer såsom säkerhetsregler som ofta förekommer på arbetsplatser. Datainsamlingen sker genom enkätundersökning samt experiment. Arbetet använder sig också av en litteraturstudie som syftar till att tillhandahålla bakgrund, fördjupa kunskapen inom ämnet samt sätta arbetet i ett större sammanhang. Studien pekar också på ett samband och en påverkan som informationssäkerheten hemma kan ha på informationssäkerheten på en arbetsplats. Resultaten visar på en säkerhetsnivå som är i olika grader bristande beroende på område. I många fall visar det även att denna brist härstammar från låg säkerhetsmedvetenhet.

Nyckelord: [IT, Säkerhet, Informationssäkerhet, Användare, Säkerhetsmedvetenhet]

Innehållsförteckning

1	Introduktion	1
1.1	Motivering	1
1.2	Förväntat resultat	2
2	Bakgrund	4
2.1	Skadlig kod	4
2.2	Trådlösa nätverk	4
2.3	Lösenord	5
2.4	Tidigare arbeten.....	6
3	Problem	7
3.1	Problemprecisering	8
3.2	Delfrågor.....	8
3.2.1	Skadlig kod	8
3.2.2	Backups	8
3.2.3	Lösenord	9
3.2.4	Trådlösa nätverk	9
3.2.5	Säkert beteende.....	9
3.3	Avgränsning.....	9
4	Metod	11
4.1	Enkätundersökning	11
4.2	Experiment	12
4.3	Litteraturstudie	13
5	Genomförande	14
5.1	Enkätundersökning	14
5.2	Experiment	15
5.3	Litteraturstudie	16
6	Resultat och analys	17
6.1	Skadlig kod	17
6.2	Backups.....	21
6.3	Lösenord	24
6.4	Trådlösa nätverk.....	28
6.5	Säkert beteende	31
6.6	Sammanfattning.....	34
6.7	Slutsats	36
7	Diskussion	38
7.1	Metod.....	38
7.2	Resultat	38
7.3	Etisk aspekt.....	38
7.4	Samhällelig aspekt	39
7.5	Vetenskaplig aspekt	39
8	Framtida arbete	41

1 Introduktion

Den tekniska utvecklingen har gått allt snabbare och snabbare, speciellt under de senaste åren. Det kan ses som positivt ur de flesta aspekter men när det gäller informationssäkerheten har den snabba utvecklingen fört med sig även en negativ sida. Den negativa sidan är den ökande tendensen att förlita sig enbart på tekniken för att säkra sin IT-infrastruktur. I och med detta ökar även risken att förbise användarens delaktighet i säkerhetsarbetet. Dessutom, om tekniken inte presenteras på rätt sätt, kan det förvirra och fjärma användaren vilket i sin tur leder till att de avancerade säkerhetsmekanismerna inte används eller missbrukas på ett eller annat sätt. Ett exempel är de olika internetjänster som kräver ett lösenord, många av vilka även har krav på lösenordskomplexitet för att höja säkerhetsnivån. Gehringer (2008) beskriver hur en användare med ett stort antal olika konton inte längre klarar av att hålla alla lösenord i minnet och tvingas att skriva ner eller återanvända lösenord vilket ökar risken för intrång. När det gäller företag finns det oftast en IT-ansvarig som är kunnig inom området samt att företaget har en viss säkerhetspolicy vars syfte är att inkludera även vanliga användare i säkerhetsarbetet. Men hur ser informationssäkerheten ut hemma hos en användare där det inte finns några sådana policies? Hur mycket vet en användare, som inte är utbildad inom IT, om vilken säkerhet som är nödvändig och är det tillräckligt för att undvika de risker som är associerade med datoranvändningen i hemmet? Många studier, främst inom *social engineering*, pekar ut just användaren som den svagaste länken som till exempel Applegates (2009) eller Nohlbergs (2008) arbeten.

Syftet med det här arbetet är att samla in information kring säkerhetsmedvetenheten hos en vanlig användare i en situation då användaren själv är fullt ansvarig för det, det vill säga i hemmamiljön. Denna frågeställning gör det möjligt att dra paralleller mellan användarens IT-vanor hemma och på en arbetsplats. Informationen kommer därefter att sammanställas för att få en bild över situationen kring informationssäkerheten i hemmet. Med vanliga användare menas användare utan specialutbildning inom IT. Eftersom studien handlar om datoranvändningen i hemmet kommer dessa användare härnäst att refereras till som hemanvändare, användare i en bredare kontext kommer fortfarande att refereras till som användare. Säkerhetsmedvetenhet handlar här om hemanvändarens kunskapsnivå inom området, det vill säga om hemanvändaren har tillräckligt med kunskaper för att kunna utnyttja befintliga säkerhetsmekanismer fullt ut.

1.1 Motivering

Anledningen till att en studie kring säkerhetsmedvetenhet hemma hos hemanvändare är viktig är att det ofta poängteras att en användare utan någon större kunskap inom IT kan innebära en säkerhetsrisk (Nohlberg, 2008). Han beskriver problemet utifrån *social engineering* aspekten, det vill säga att vid en attack är det lättast att angripa människan. Arbete ämnar att bygga vidare på detta och inkludera även andra aspekter, nämligen situationer som inte initieras av angripare utan snarare fokuserar på säkerhetsluckor som lämnas av hemanvändaren själv, utan någon påverkan utifrån. Det är viktigt eftersom i många fall kan risken för en säkerhetsincident minimeras med hjälp av grundläggande kunskap inom ämnet som i fall med starka lösenord (Burnett, 2005) eller pålitlig krypteringsalgoritm (Beck, 2008). Tekniken som finns idag erbjuder adekvat skydd men det

är upp till individen att använda sig av den. Därför är det viktigt att identifiera om användare känner till de olika säkerhetsmekanismerna samt använder sig av dessa för att minimera de olika risker som finns i samband med datoranvändning. Det finns en del studier som handlar om säkerhetsmedvetenhet som till exempel Isakssons (2011) examensarbete om lösenordhantering. Där jämför han lösenordhanteringen i tre olika sammanhang - på ett företag, en bank och en kommun. Det är ett intressant arbete då det tar upp temat om säkerhetsmedvetenhet. Dock är det bara lösenordsaspekten som behandlas. Studien ämnar att utforska de aspekter som hemanvändaren kommer i kontakt med och som kan påverkas av denne (se 3.1 Avgränsning). Dessutom kommer mer fokus att läggas på just hemanvändaren själv genom att eliminera faktorer som påverkar användare i allmänhet såsom policys som finns på olika arbetsplatser. Genom att undersöka hemanvändarnas IT-vanor kan detta arbete ta fram informationen som kan hjälpa att bilda en uppfattning kring hemanvändarens säkerhetsmedvetenhet gällande IT.

Det som gör studien viktig för just hemanvändare är tre olika aspekter. Den ekonomiska aspekten är en av dessa eftersom dataintrång kan äventyra bankkontoinformationen vilket i sin tur kan resultera i pengaförlust. Därefter finns även en juridisk aspekt som hemanvändare kan bli påverkade utav om de blir utsatta för "malware" och deras dator används i en kriminell handling som en del av en "botnet". Som det finns beskrivet längre fram under "2. Bakgrund" kan detta leda till att datorns ägare kan åtalas för brottet, även om den begicks utan ägarens vetskap. Den slutliga aspekten är hemanvändarens integritet som kan utsättas för risk vid ett dataintrång. Viktig information lagrad lokalt, alternativt känsliga e-post kan lätt komma i fel händer om förövaren kommer över lösenordet.

Även om fokusen ligger på hemanvändaren så berör denna fråga även arbetsplatser. En användare som har dålig viruskydd hemma kan innebära en ökad risk även för företaget då hemanvändaren kan ovetande sprida viruset vidare till företaget genom ett infekterat USB-minne. Det gäller även hanteringen av e-post från okända avsändare som kan innehålla skadlig kod. En redovisning från Securelist (2011) visar att 3,23% av alla e-post innehåller virus. En användare som inte känner till denna risk utgör ett hot för informationssäkerheten på en arbetsplats precis som i hemmet. Samma sak gäller för hanteringen av lösenord. Även om ett företag kan framtvinga en viss lösenordskomplexitet genom policys kan en användare med låg säkerhetsmedvetenhet fortfarande innebära en ökad risk genom att till exempel skriva ner sina lösenord eller avslöja dessa som ett resultat av en *phishing* attack.

1.2 Förväntat resultat

Det förväntade resultatet är att få en uppfattning om kunskapen om informationssäkerhet hos hemanvändare samt säkerhetsnivå i hemmet genom att sammanställa information från de olika delfrågor presenterade längre ner. Undersökningen kommer att utformas så att information från ett större antal användare kan samlas in och på så sätt öka resultatens precision (se 4. Metod). De flesta studier kring denna fråga riktar in sig på olika arbetsplatser. Resultat av arbetet kommer att kunna användas för att rikta mer uppmärksamhet på hemanvändare. Ett annat syfte med detta kan knytas närmare till systemadministrationsämnet. Det handlar om användarnas delaktighet i säkerhetsarbetet på arbetsplatser. IT-administratörer säkrar upp nätverken genom att implementera olika säkerhetsmekanismer men det är inte alltid tillräckligt. Zhou (2008) skriver hur spam kan skickas ut med hjälp av "botnets" på ett sätt som kan komma förbi många implementerade säkerhetsåtgärder. Eftersom spam ofta kan innehålla eller länka till skadlig kod kan en

användare som öppnar sådan e-post orsaka en del skada. Om användaren å andra sidan har den kunskapen från datoranvändningen hemma kan detta problem undvikas och därmed underlätta arbetet för systemadministratörer. På så sätt kan ett arbete som riktar in sig på hemanvändare även gynna olika arbetsplatser.

2 Bakgrund

Detta kapitel innehåller övergripande information om de aspekter som är relevanta för en hemanvändare och som har att göra med informationssäkerhet. Syftet med denna information är att sätta de olika koncepten i ett sammanhang som kan relatera till just hemanvändare. De olika aspekterna är framtagna baserat på "Datorstödd informationssäkerhetsutbildning för användare" framtagna av MSB (2012) samt "Internetsäkerhet för hemmet" av Post- och telestyrelsen (2012). De ursprungliga aspekter presenterade på ovanstående sidor är omstrukturerade och anpassade för att bättre passa till den här undersökningen. Till exempel aspekten kring sociala medier samt e-post är grupperade tillsammans med säkert beteende. De aspekter som hamnar utanför undersökningens avgränsning tas inte med. Ett exempel på en sådan aspekt är loggningen som är mindre relevant för hemanvändningen då dator oftast används endast av ägaren eller också en familjemedlem.

2.1 Skadlig kod

Al-Dossary (1990) skriver: "*The only known method of **completely** securing a computer system against viruses is total isolation.*". Det innebär i sin tur att alla som har tillgång till internet har antingen medvetet eller omedvetet kommit i kontakt med datavirus. Al-Dossary (1990) definierar virus som en mjukvara som kan replikera och sprida sig själv och vars kod består av två viktiga delar. Den första delen är replikeringsmekanismen som gör det möjligt för viruset att spridas vidare. Den andra delen av koden utför själva syftet med virus som kan vara allt från att stjäla information till att ta över hela datorn. Virus finns i många olika variationer som till exempel trojaner eller maskar men det gemensamma för alla virus är att de antingen ger sig ut för att vara någon legitim mjukvara eller gömmer sig inbäddade i en mjukvara som annars är fullständigt legitim.

Beroende på vilken virus det handlar om kan de skapa olika problem för berörda användare. Effekten av vissa är fullt synlig och uttrycker sig i ett hinder för vanlig datoranvändning. Andra virus, som oftast har större konsekvenser, är de som förblir obemärkta. Ett sådant virus kan användas för att stjäla kontoinformation genom så kallade *keyloggers*. Harley (2006) beskriver hur en sådan *keylogger* kan spara alla inmatningar som användaren gör från både tangentbordet och musen. I andra fall kan virus helt obemärkt för användaren ta över datorn. Den tillsammans med ett stort antal andra datorer som har blivit övertagna på samma sätt bildar tillsammans en "botnet". Den kombinerade styrkan av en "botnet" kan användas för att utföra DDoS attacker som beskrivs i Puris (2003) artikel. Svårigheter med att avgöra användarens faktiska delaktighet i attacken kan ofta leda till att användaren som har varit fullständigt ovetande om brottet fortfarande kan åtalas för det. Det är användarens ansvar att installera en antivirus mjukvara samt hålla den uppdaterad för att kunna skydda sig mot både nya och gamla virus. Om användaren inte känner till konsekvenser som de olika virus har (som i exemplen ovan) kan det vara svårt att inse vikten med en antivirus mjukvara.

2.2 Trådlösa nätverk

Det växande antalet enheter som stödjer trådlös kommunikation ger fler och fler anledningar att gå över till denna lösning. Nackdelen med att gå över till trådlös kommunikation är att en del av kontrollen över vem som har tillgång till ett nätverk går förlorad i och med att det inte längre krävs någon fysisk kontakt. Graziani (2005) skriver att inomhusräckvidden för de

vanligaste antennerna är mellan 30 och 40 meter. Det innebär ofta att nätverket sträcker sig utanför lägenheten. Det är inte helt ovanligt att kunna se ett flertal trådlösa nätverk, speciellt i lägenheter. För att åtgärda detta problem och för att kunna begränsa åtkomsten till sitt nätverk till de som är behöriga finns det inbyggda säkerhetsmekanismer för åtkomstkontroll och kryptering. Nackdelen här är att de mekanismer är oftast inte förinställda och kräver en viss inblandning från användarens sida och de som inte känner till det kan hamna i en situation där de har ett helt öppet nätverk. Det kan i sin tur leda till allt från att obehöriga använder internetåtkomsten till en fullständig övervakning av allt som händer på nätverket samt en ökad risk för virus. Även om lösenordskyddet aktiveras finns det tre olika standarder som för en nybörjare kan till synes vara väldigt lika men i själva fallet kan vara skillnaden mellan ett skyddat och ett oskyddat nätverk. De olika standarderna är WEP, WPA och WPA2. Alla tre brukar finnas på de flesta routern för bakåtkompatibilitet och oftast saknar en beskrivning för vilken som ger bästa skyddet. Det kan leda till att användaren väljer mer eller mindre slumpmässigt och kan mycket väl välja WEP som idag är väldigt utdaterad och sårbar för attacker. I Bittaus (2006) artikel kan man läsa om WEPs svagheter. Där beskriver hon hur enkelt och snabbt det är möjligt att ta sig förbi WEP och få full tillgång till nätverket. WPA ger bättre skydd än WEP men även den är sårbar för attacker som visas i Becks (2008) artikel. Det lämnar endast WPA2 som en pålitlig mekanism för skydd av nätverket och visar på hur viktigt det är att känna till denna information för att kunna säkra sitt nätverk.

2.3 Lösenord

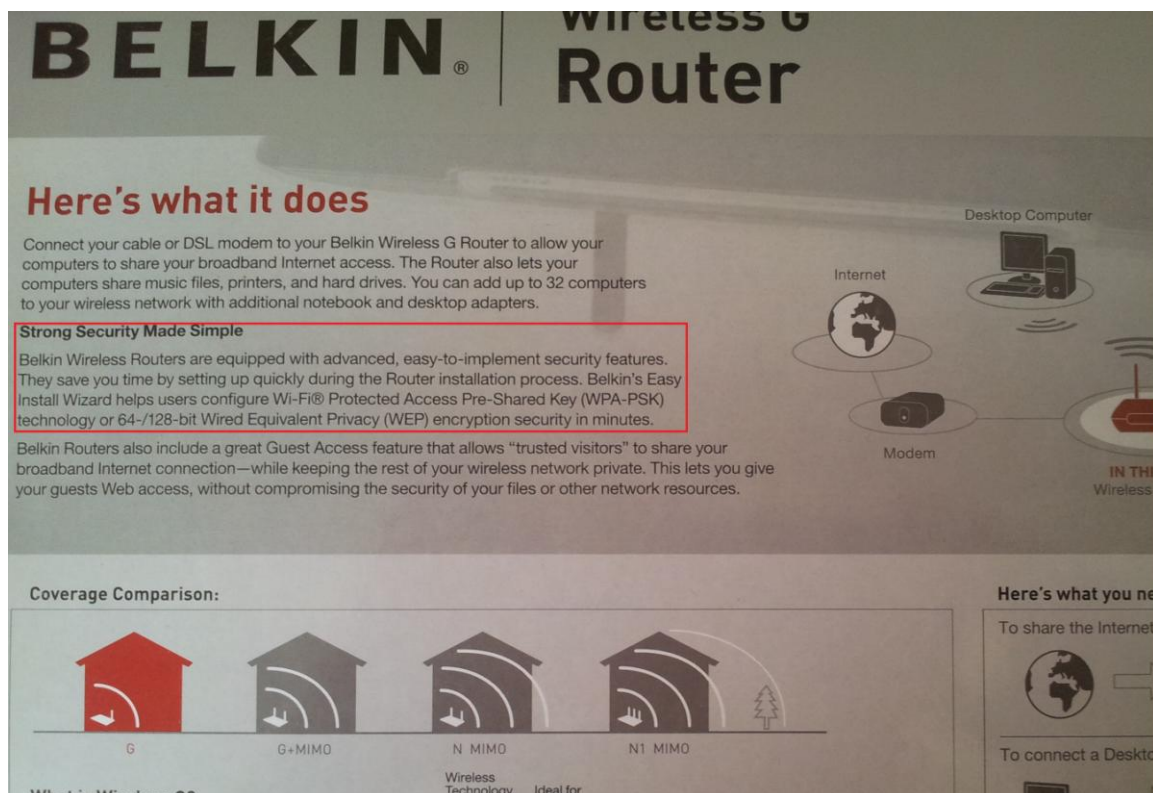
Lösenord har länge varit ett allmänt känt och accepterat sätt att kontrollera åtkomsten. Därför har tekniken för att styrka denna mekanism ständigt förbättrats. Det är även därför som det minst resurskrävande sättet att ta reda på ett lösenord att bara fråga om den. Mitnick (2002) skriver: "*Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.*". Det stora problemet idag är alltså just användare och deras tendens att minska det tänkta skyddet genom felaktig användning av lösenord. Den felaktiga användningen kan innebära allt från användningen av väldigt enkla lösenord till en felaktig lagring av dem. Det skapar en intressant situation, å ena sidan så finns det en teknik som är framtagen speciellt för att på bästa sättet skydda användaren men å andra sidan så är det användaren själv som väljer att inte ta del av den. Detta kan jämföras med en bepansrad dörr som erbjuder ett väldigt bra skydd men som användaren väljer att inte låsa eller är bara rentav slarvig med nyckeln. Många vanliga användare känner inte till attacker som till exempel *brute force* som är baserat på ordlistor och därför känner sig säkra när de använder sitt mellannamn eller favoritkaraktär från en bok som lösenord vilket minskar skyddet drastiskt. I sin bok beskriver Burnet (s.7-10 och s.107-109, 2005) hur vanlig förekomsten av osäkra lösenord är och hur sårbara de blir för just *brute force* attacker. I och med detta ger han exempel på top 500 sämsta lösenord och påpekar att en av tio användare har ett lösenord från den listan vilket innebär att på grund av deras okunskap har de själva ökat risken för dataintrång. Problemet förvärras ytterligare i och med mängden av olika lösenord som en vanlig användare behöver hålla koll på. Det kan vara allt från inloggningen till datorn till e-post och olika former av sociala hemsidor som är vanliga på internet idag. Detta, enligt Gehringer (2008) ökar användarens tendens att skriva ner eller återanvända lösenord.

2.4 Tidigare arbeten

Det finns ett flertal arbeten som handlar om informationssäkerhet. Deras gemensamma nämnare är dock att de flesta av dem handlar om säkerheten samt säkerhetsmedvetenhet på olika arbetsplatser, det vill säga platser där säkerheten är styrd av både policy och ansvariga personer. Ett exempel på ett sådant arbete är Isakssons (2011) arbete som handlar om lösenordshantering på olika arbetsplatser. Det finns även andra arbeten som har vissa saker gemensamt med denna studie, som till exempel arbeten som handlar om *social engineering*. Skillnaden är dock den att de angriper frågan från ett annat perspektiv, nämligen från angriparens håll och handlar oftast om hur angriparen kan manipulera offret till att öppna upp säkerhetsluckor. Ett exempel på ett sådant arbete är Mitnicks (2002) bok. Det här arbetet vänder lite på frågan och fokuserar istället på säkerhetsluckor som hemanvändarna lämnar utan något tryck utifrån och oftast på grund av brist på kunskap. Som en av aspekter i sitt arbete tar Stone-Gross (2009) upp hur allvarligt situationen är gällande lösenord. Studien visade att 28% procent av deltagare återanvände sina lösenord på flera hemsidor och nästan 40% av de testade lösenord kunde gissas, med hjälp av anpassad mjukvara, på mindre än 75 minuter. Det finns inga kommentarer på vilken typ av användare det handlade om men det visar tydligt att det finns bra anledningar att genomföra vidare studier kring säkerhetsmedvetenheten. Richardsons (2008) artikel kan användas som ett annat argument då han tar upp i den de olika skador och dess kostnader som IT-brott orsakar. Det som är allra mest relevant för det här arbetet är en artikel av Besnard (2003) där han beskriver hur en legitim användare ofta kan minska systemets säkerhet genom att bland annat byta säkerhet mot bekvämlighet. Även Furnell (2005) tar upp frågan om användare som inte använder sig av säkerhetsmekanismer samt möjliga anledningar bakom det. Furnell (2005 & 2008) genomförde även två liknande studier som undersöker användarnas säkerhetsmedvetenhet. Den ena studie riktar in sig på internetanvändning i allmänhet medan den andra fokuserar mer på specifika applikationer. Ingen av studierna ämnar dock att skapa en mer fullständig bild över informationssäkerheten som en hemanvändare kan komma i kontakt med.

3 Problem

Ett av problemen som finns inom informationssäkerhet är att människor ofta förbises i ett säkerhetssammanhang. Fokus ligger på tekniken och tekniken idag är avancerad och anpassad till olika situationer. Det som utgör ett problem här är dock att denna teknik ofta kräver en viss ansträngning från användarens sida. Användaren kan då i sin tur, på grund av okunskap eller andra orsaker, agera felaktigt och därmed minska skyddet som tekniken ämnar att erbjuda. Ett exempel är en hemanvändare som köper och kopplar in en trådlös router. I de flesta fall behöver den konfigureras innan användningen för att bland annat erbjuda bästa möjliga säkerhet. För en hemanvändare kan det dock vara svårt att se skillnaden mellan WEP, WPA och WPA2 när i själva verket det är en skillnad på ett skyddat och ett oskyddat nätverk. Detta problem förvärras ytterligare i och med att vissa tillverkare, som till exempel Belkin, fortfarande anger WEP och WPA som säkra krypteringsmetoder och ibland även utan att ange WPA2 alls (se Figur 1). Ett annat exempel är lösenord. I de flesta fall är det en säker mekanism men den förlitar sig starkt på att användaren själv tar ansvaret att använda ett starkt lösenord samt kunna hantera sina lösenord på ett säkert sätt (för mer information om båda exemplen se respektive underkapitel under "2.Bakgrund"). Det stöds av olika *social engineering* studier som pekar ut just användaren som den svagaste länken. I sin artikel beskriver Applegate (2009) hur mycket enklare det är att angripa användaren direkt och illustrerar bland annat *phishing* och trojan attacker.



Figur 1 Belkin Wireless G Router förpackning (baksidan).

Studien kommer att rikta in sig på hemanvändaren för att ta reda på hur situationen kring informationssäkerhet ser ut idag. Studien kommer att omfatta aspekter av datoranvändning i hemmet där hemanvändarens agerande är direkt avgörande för den resulterande säkerhetsnivån. Medan största fokuset kommer att ligga på säkerhetshål som lämnas av hemanvändaren utan något påtryck utifrån kommer även vissa undantag att finnas. De undantag är frågor som härstammar ifrån *social engineering* och som handlar om attacker som i grunden är initierade av angripare men vars succé beror på hemanvändarens kunskap inom ämnet. Därför blir även de frågor relevanta i denna studie då de kommer att behandlas

ur hemanvändarens perspektiv. Till de frågor hör först och främst olika *phishing* attacker samt e-post som innehåller virus.

3.1 Problemprecisering

Hur säkerhetsmedveten är en hemanvändare samt hur ser säkerheten ut hemma i dagsläget?

Anledningen till att säkerhetsmedvetenheten är så viktig är de olika säkerhetsaspekter som kräver hemanvändarnas delaktighet. Exempel på sådana aspekter är krypteringsskyddet för det trådlösa nätverket och antivirusmjukvaror. Kunskapen spelar en stor roll här då användaren behöver känna till både hur de olika säkerhetsaspekterna ska implementeras för att tillhandahålla bästa möjliga säkerhet och de möjliga konsekvenserna med bristen på adekvat skydd. Kännedom kring konsekvenser kan då tjäna som en motivation till att implementera de olika skyddsmetoderna. Huvudfrågan kommer att besvaras genom att sammanställa och analysera informationen från delfrågorna. Nedan, under "3.2.Delfrågor" finns en lista på alla de punkter som kommer att behandlas för att besvara frågan.

3.2 Delfrågor

Hela studien delas upp i ett antal delfrågor, både för att ge ett tydligare resultat och för att underlätta bearbetandet av ämnet. Framtagningen av de olika delfrågor bygger på "Datorstödd informationssäkerhetsutbildning för användare" framtagen av MSB (2012) samt "Internetsäkerhet för hemmet" av Post- och telestyrelsen (2012). Den gemensamma nämnaren för de olika aspekterna som behandlas inom varje delfråga är att de är olika säkerhetsrelaterade mekanismer som finns implementerade inom IT-infrastrukturen men som inte kan fungera utan att användaren känner till och använder de korrekt. Syftet med delfrågorna är att täcka aspekter av informationssäkerheten som kräver att hemanvändaren är aktivt delaktig. Med hjälp av de här delfrågorna ämnar arbetet att bygga upp en bild över hemanvändarens IT-vanor.

3.2.1 Skadlig kod

Hur mycket kan hemanvändaren om användningen av antivirusmjukvaror?

Antivirus mjukvaran är till en stor utsträckning hemanvändarens ansvar. Det är en viktig aspekt av informationssäkerheten i hemmet som kräver en viss kunskap och framför allt engagemang från hemanvändarens sida. En dator utan antivirus mjukvara eller med mjukvaran som inte uppdateras regelbundet löper en stor risk att bli utsatta för samt sprida vidare olika virus. Tekniken finns tillgänglig men den kräver hemanvändarens delaktighet vilket gör det viktigt att kartlägga hemanvändarens antivirus preferenser. Datainsamlingen kommer att ske genom enkätundersökningen.

3.2.2 Backups

I vilken utsträckning säkerhetskopierar hemanvändare sina filer?

Även backups berör säkerheten, dock handlar det inte om att förhindra en incident utan snarare att kunna återhämta sig från dessa. Även om datorn har bra skydd kan andra aspekter orsaka dataförlust, som till exempel tekniska fel eller stöld. Frågan blir ännu viktigare i de fall då de implementerade säkerhetsmekanismer är otillräckliga. Genom att ta backups kan hemanvändaren minimera konsekvenser av en eventuell säkerhetsincident. Datainsamlingen kommer att ske genom enkätundersökningen.

3.2.3 Lösenord

Hur hanterar hemanvändaren sina lösenord?

Alla som använder dator och internet kommer dagligen i kontakt med lösenord. Allt från inloggningen på datorn till de olika tjänster på internet som erbjuder hemanvändaren egna konton kräver lösenord. Här har hemanvändaren ett väldigt stort ansvar eftersom lösenordskomplexiteten är avgörande för hur hög den resulterande säkerhetsnivån blir. Förutom komplexiteten är det även intressant att undersöka andra aspekter som kan sänka säkerhetsnivån såsom återanvändning eller osäker lagring av lösenord. Datainsamlingen kommer att ske genom enkätundersökningen och en litteraturstudie.

3.2.4 Trådlösa nätverk

Hur skyddas det trådlösa nätverket hos hemanvändaren?

En stor del av hemanvändare som har tillgång till internet hemma har även trådlösa nätverk. För alla de som bor i en lägenhet är chansen stor att de kan se ett flertal olika trådlösa nätverk inom deras räckvidd. Det är dock inte alltid självklart att detta nätverk är skyddat eftersom många av de trådlösa routern som säljs idag för hemmabruk kommer utan någon förinställt skydd. Det krävs inte mer än grundläggande kunskaper inom IT för att kunna aktivera detta skydd men om den inte aktiveras eller om felaktig standard används så löper hemanvändaren en stor risk för intrång på sitt nätverk. Data kommer att samlas in genom en enkätundersökning samt olika experiment. Experimenten kommer att innefatta *wardriving* med syftet att få en bild över procenten av oskyddade nätverk och en övervakad installation av en trådlös router för att se hur en hemanvändare kan hantera det.

3.2.5 Säkert beteende

Hur påverkar hemanvändarens IT-vanor risken för diverse angrepp samt deras succé?

Antivirus mjukvaran är ett steg till att skydda sig mot virus men det finns alltid en sannolikhet att vissa virus inte upptäcks, som till exempel så kallade "*zero day threats*" som antivirus mjukvaror inte har hunnit lära känna. Därför är det viktigt att undersöka hur försiktiga hemanvändarna är i sitt beteende på internet och om de agerar på ett sätt som ökar risken för att bli utsatta för virus eller bedrägeri. Datainsamlingen kommer att ske genom enkätundersökningen.

3.3 Avgränsning

Ämnesområdet som det här arbetet kommer att täcka är säkerhetsmedvetenhet kring informationssäkerheten hos hemanvändare samt den nuvarande säkerhetssituationen. Avgränsningen för ämnet är säkerhetsrelaterade aspekter av datoranvändning hemma som kräver aktivt delaktighet från hemanvändarens sida. Därför kommer inte aspekter som hör till en arbetsplats tas med i undersökning. Undersökningen omfattar inte heller situationer där användarens säkerhetsbeslut påverkas av andra personer som ansvarar för säkerheten.

Studien riktar in sig på användare som dagligen använder sin dator hemma och som inte har en utbildning inom IT. Alla som inte stämmer in på dessa kriterier ingår inte i undersökningen. Undantaget är *wardriving*-experimentet eftersom den saknar möjligheten att kontrollera om deltagarna stämmer in på avgränsningen. I övrigt kontrolleras att rätt målgrupp deltar i undersökningen genom att inkludera frågor i enkäten som handlar om just

IT-utbildningen och datoranvändningen. Det stämmer även för installationsexperimentet då deltagare till det väljs ut från personer som deltog i enkätundersökningen.

4 Metod

Metoden som används för att genomföra arbetet består av ett antal olika delar som främst kommer att följa det kvantitativa paradigmet. En enkätundersökning kommer att genomföras för att samla in information från olika användargrupper gällande deras säkerhetsmedvetenhet. Enkäten kommer att vara utformad så att relevant information till de olika delfrågorna kan samlas in. Liksom framtagningen av delfrågorna, bygger även framtagningen av enkätfrågor på informationen hämtad från "Datorstött informationssäkerhetsutbildning för användare" framtagen av MSB (2012) samt "Internetsäkerhet för hemmet" av Post- och telestyrelsen (2012). Data, insamlad med hjälp av enkätundersökningen, kommer att sammanställas och analyseras med syftet att besvara delfrågorna. Det kommer även att genomföras en del praktiska experiment, även de av en kvantitativ karaktär. *Wardriving*-stickprov kommer att genomföras på ett antal platser runt om i Skövde för att upptäcka antalet osäkra nätverk. Andra experimentet kommer att gå ut på att få en grupp av hemanvändare att genomföra en installation av en trådlös router för att se hur mycket vikt de kommer att lägga på säkerheten. All information från diverse undersökningar kommer att sammanställas för att besvara delfrågor och därmed få en bild över säkerhetsmedvetenheten hos hemanvändare samt nivån av deras informationssäkerhet. Parallellt med de olika undersökningarna kommer även en litteraturstudie att genomföras. Syftet med den är att få mer information inom området och därmed kunna förstå sakfrågan bättre, samt att kunna relatera arbetet till tidigare studier inom säkerhet. Resultatet av studien kommer att vara en kartläggning av säkerhetsnivån samt säkerhetsmedvetenheten hos hemanvändare.

4.1 Enkätundersökning

En av de stora fördelarna med enkätundersökningen enligt Berndtsson (s.63, 2008) är att med hjälp av den kan undersökningen nå ett stort antal individer. På så sätt kan resultatets precision ökas då fler deltagare ökar chansen för deltagarnas mångfald. I sina två studier undersöker Furnell (2005 & 2008) väldigt olika antal användare - 20 i den ena och över 300 i den andra. Utifrån det är målet för undersökningen satt till cirka 100 till 150 individer. Antalet deltagare påverkas även av tidsbegränsningar som undersökningen har på sig. Det gör detta angreppssätt passande för att samla in data som kommer att användas för behandlingen av delfrågorna 1-3 samt 5. Den kommer även att utgöra en del av datainsamlingen för delfrågan 4, dock kommer andra metoder att krävas för att få tillräcklig data för att kunna besvara den (se de andra metoder). Biemer (s.196-197, 2003) listar som en nackdel av en sådan undersökning att den är enkelriktad. Det gör att själva frågeformuläret måste vara noggrant utformat med tydliga frågor och förbestämda svarsalternativ. Det kommer att underlätta både för besvarandet av frågor och för sammanställningen av resultat. Framtagningen av frågorna bygger på informationen kring olika säkerhetsaspekter hämtad från "Datorstött informationssäkerhetsutbildning för användare" framtagen av MSB (2012) samt "Internetsäkerhet för hemmet" av Post- och telestyrelsen (2012). Enkäten kommer att distribueras ut genom sociala medier såsom Facebook. För att kontrollera att undersökningen når rätt målgrupp inkluderas två frågor i enkäten som ska kontrollera om deltagare har en utbildning inom IT samt om de dagligen använder en dator i hemmet. Nackdelen med Facebook som en distributionskanal är svårigheten för att få mångfald hos deltagare. Det innebär en viss risk att få en majoritet av deltagare som representerar en specifik grupp och därmed påverka undersökningens resultat. Målet för antalet deltagare är

därför satt till minst 100 för att öka chansen att få med representanter från så många olika grupper som möjligt. Det ger dock inga garantier. Därför är ett annat sätt att hantera det är att tydligt definiera avgränsningen för undersökningen som i detta fall visar att ända kravet på deltagare är att de inte har en utbildning inom IT samt att de använder dator hemma dagligen. Dessa två egenskaper kontrolleras med hjälp av de två ovannämnda frågor i enkäten. Det finns dock en viss reservation för möjligheten att resultaten kan påverkas beroende på vilka individer som kommer att delta i den. En nackdel med själva metoden å andra sidan är att enkätundersökningen är en enkelriktad kommunikation vilket innebär att frågor måste ha fördefinierade svar som dessutom omfattar alla de möjliga svarsalternativen. Tiden som en sådan undersökning kan ta att slutföra gör det väldigt viktigt att ta med alla punkter som kan behövas för att besvara undersökningens huvudfråga. Slutligen finns det en annan nackdel i samband med ett mörkertal i undersökningen. Mörkertalet förekommer i två olika frågor. Anledningen är att de båda behandlar ämnen som kan anses vara känsliga för vissa deltagare och därför tillhandahålls ett svarsalternativ för de som väljer att inte svara. Endast det aggregerade resultatet som ska presenteras i detta arbete kommer att sparas.

4.2 Experiment

För att kunna besvara delfråga 4 kommer enkätundersökningen att kompletteras med några experiment. Detta är nödvändigt eftersom noggrannheten vid endast enkätundersökningen kan variera. Eftersom den undersökta gruppen är hemanvändare måste hänsyn tas till faktumet att vissa hemanvändare kommer att ha svårigheter att besvara frågor gällande till exempel krypteringsstandarden som används på det trådlösa nätverket. Det är dock en väldigt viktig punkt som direkt berör säkerheten. Därför kommer två separata experiment att genomföras. Med hjälp av de experimenten kan data kring ett genomsnittligt antal oskyddade nätverk samlas in. Det första experimentet kommer att vara installation av en trådlös router. Berndtsson (s.65, 2008) skriver att vid experiment som involverar människor är det viktigt att vara noga vid valet av deltagare. Det kan vara en nackdel då precis som i fallet med enkätundersökningen kan överrepresentation av en specifik grupp påverka resultaten. Det hanteras på två olika sätt. Det ena sättet är densamma som med enkäten, dvs. att valet av deltagare utgår endast från avgränsningen. Därför väljs deltagare ut från personer som deltog i enkätundersökningen eftersom enkäten innehåller frågor kring både datoranvändningen och IT-utbildningen. Det andra sättet är att utvärdera experimentets resultat tillsammans med motsvarande resultaten från både enkätundersökningen och det andra experimentet. Deltagare till experimentet kommer att sökas genom att skicka ut en förfrågan via e-post och Facebook. Kravet för att delta i experimentet är densamma som för enkätundersökningen. Experimentet genomförs tillsammans med 10 hemanvändare. Varje deltagare kommer att få tillgång till en trådlös router (i förpackning, med alla inkluderade instruktioner) samt en bärbar dator med operativsystemet Windows 7. Målet för deltagare kommer att vara att installera den och kunna koppla in sig till den via en bärbar dator. Routern kommer att återställas till ursprungsläget efter varje deltagare. Aspekter så som lösenord och valet av krypteringsalgoritm kommer att observeras.

Det andra experimentet kommer att handla om att ta "wardriving"-stickprov på olika platser i Skövde. Syftet är att se hur stor andel av tillgängliga trådlösa nätverk som är oskyddade. Det kommer att tas mellan 10 och 20 stickprov, beroende på antal trådlösa nätverk som finns tillgängliga. Nackdelen med sådana experiment enligt Berndtsson (2008) är att de endast ger en indikation på att något är på ett visst sätt och kan inte tolkas som en absolut fakta. För att

få ett mer noggrant svar kommer data från experimenten utvärderas tillsammans med data från enkäten för att besvara delfrågan.

4.3 Litteraturstudie

Litteraturstudiets roll är tjäna som grund för hela studien. Med hjälp av den kommer en djupare förståelse inom ämnet eftersökas. Den kommer även att underlätta förklaringen samt motiveringen av de olika delarna av arbetet. Litteraturstudien kommer även att behövas för att sätta arbetet i ett större sammanhang. Den stora utmaningen här som Berndtsson (s.58-60, 2008) beskriver den är att kunna välja relevant information. Förutom relevansen behöver informationen även ha valida källor. Ett sätt att försäkra informationens validitet är att kontrollera att den kommer från "peer-reviewed" artiklar.

5 Genomförande

Här beskrivs det praktiska tillvägagångssättet för detta arbete. Beskrivningen innehåller även information kring hur de olika delarna har tagits fram, vad de innehåller och hur undersökningen har genomförts.

5.1 Enkätundersökning

Enkätundersökningen är ämnad till att samla in den största delen av informationen för studien. Den implementerar den kvantitativa forskningsmetoden genom att låta ett flertal individer besvara samma frågor med ett antal förbestämda svarsalternativ.

Frågorna till enkäten har tagits fram genom att analysera de olika delfrågorna inom studien och identifiera vilken information som krävs för att kunna besvara dessa. Enkäten består av 26 frågor totalt som är uppdelade i 5 olika kategorier. För att göra det enklare för undersökningens deltagare och för att underlätta sammanställningen av resultaten, finns det förbestämda svarsalternativ till alla frågor i enkäten. Svarsalternativet "Vet inte" är inkluderad i de frågorna där deltagaren inte förväntas veta svaret. Ett annat svarsalternativ som är värt att nämna är "Svarar helst inte" som förekommer i frågor där deltagaren kan tänkas vilja undvika svara direkt såsom med frågan om nedladdning av piratkopierad material. Slutligen så finns det även två frågor i enkäten som skiljer sig väldigt mycket från de andra eftersom själva formuleringen i de frågorna är felaktig. De frågorna handlar om utlämningen av personlig information över telefon, respektive internet, till personer som legitimt identifierar sig. Denna formulering är felaktig då legitim identifiering över de två medier som skulle kunna rättfärdiga överlämningen av personlig information är väldigt problematisk. Formuleringen är dock medveten och är ämnad till att undersöka hur många av deltagare som inte känner till det och som därför är mottagliga för *phishing* attacker.

För att distribuera ut enkäten har den laddats upp på ett DropBox konto, därefter har en länk lagts upp på Facebook med en förklarande text som beskrev vad undersökningen går ut på, ungefärlig tid för genomförandet samt en försäkran att undersökningen är anonym och att inga individuella enkäter kommer att sparas efter att resultaten har blivit sammanställda. Länken tillsammans med den förklarande texten distribuerades ut till alla på vänner-listan (omkring 134 personer). I och med den förklarande texten uppmanades även alla att sprida vidare länken till sina egna vänner-listor för att på så sätt nå ut till så många som möjligt och även komma utanför egna vänner-listan. Ett e-post konto har skapats för att samla in svaren och själva enkäten innehöll adressen dit svaren skulle skickas.

Slutligen när antalet inkomna svar uppnådde hundra stycken, som var den önskade mängden, har resultat från alla individuella enkäter sammanfattats för att kunna analysera och presentera det kompletta resultatet från undersökningen. Det som är viktigt att poängtera här är att anonymiteten i enkätundersökningen gör det möjligt för en och samma person att skicka in fler än ett svar och på så sätt påverka resultatet. Enkätundersökningen ger inte heller några garantier att deltagare svarar ärligt på frågor som ställs. Förutom det påverkas även resultatet av faktumet att enkäten distribuerades bland personer på vänner-listan på Facebook. Det kan resultera i en smalare målgrupp då majoriteten deltagare kan tillhöra en specifik typ av användare. Många olika användartyper kan passa in på avgränsningen och om en specifik typ är överrepresenterad kan det påverka resultatet. Alla deltagare uppmanades dock att sprida enkäten vidare för att komma utanför den egna

vänner-listan och för att bredda målgruppen. Undersökningsdata kring trådlösa nätverk valideras ytterligare av två experiment som bekräftar den erhållna resultatet. Utifrån det kan ett antagande göras att även de andra enkätfrågorna besvarades ärligt av undersökningens deltagare.

5.2 Experiment

Syftet med de två experimenten som genomfördes inom ramar av studien var att införskaffa mer information kring säkerheten av trådlösa nätverk hos hemanvändare. Enkätundersökningen gav en del information om det men eftersom trådlösa nätverk är en av de mer tekniska punkterna som behandlas och som kan kräva en viss kunskap från användarens sida ansågs data från experimenten vara nödvändig för att komplettera resultaten. Detta kunde även ses i och med antalet deltagare som svarade "Vet inte" på frågor relaterade till trådlösa nätverk.

Det första experimentet gick ut på att låta deltagare installera en trådlös router för att kunna observera hur de går tillväga samt vilken säkerhet deras installation kommer att ha. Till detta användes en laptop med Windows 7 samt en trådlös router av märket Belkin (Belkin Wireless G router). Denna router valdes för att den hörde till medelprisklassen bland trådlösa routers för hemmabruk, baserat på jämförelsen av de olika routers som erbjöds av de olika elektronikkedjorna. Den hade även en adekvat prestanda och täckning som gjorde den till ett bra val för en hemmarouter. Dessutom erbjöd den de vanliga säkerhetsmekanismer för skyddet av nätverket såsom WEP/WPA/WPA2-krypteringar och MAC-filtrering som var nödvändiga för undersökningen. Deltagare för experimentet valdes i samband med enkätundersökningen där enkätdeltagare kunde visa sitt intresse för att delta i experimentet. Kraven för experimentets deltagare var samma som för enkätdeltagare.

Innan experimentet fick alla deltagare information om experimentet. Deras uppgift var installera routern såsom de skulle ha gjort det hemma. När de var klara med detta skulle de ansluta laptoppen till det nya nätverket och gå ut på Google för att bekräfta internetåtkomsten och även visa att de var klara med uppgiften. Varje deltagare skulle utföra detta enskilt för att försäkra att deltagare inte påverkar varandra. Eftersom endast en router användes för experimentet var det nödvändigt att återställa den till fabriksinställningar (resett-knappen) samt packa in den i förpackningen. Förutom routern och tillhörande sladdar innehöll förpackningen en kortare manual i pappersform samt en CD-skiva med en mer utförlig manual för installation och konfiguration.

Internetåtkomsten kunde enkelt uppnås genom att bara koppla in routern, de olika säkerhetsmekanismerna däremot kunde endast aktiveras från det webbaserade gränssnittet (liksom de flesta andra trådlösa routers för hemmabruk). Det innebar att routern skulle kunna kopplas in och användas utan att någonsin behöva konfigurera den, men det skulle också innebära att nätverket skulle vara helt öppet. Målet för deltagare var att få en anslutning mot internet men samtidigt så uppmanades de tydligt att installera routern så som de skulle ha gjort hemma. Denna förutsättning användes för att visa vilken kunskap deltagare har om hur de ska skydda sitt trådlösa nätverk. Deltagare observerades under själva experimentet för att se hur och om de använder sig av de olika skyddsmekanismerna.

Det andra experimentet handlade om att försöka uppskatta hur vanligt det är med trådlösa nätverk som är oskyddade eller som är skyddade med en svag krypteringsalgoritm. En mätning genomfördes vid tio olika flervåningshus i centrala Skövde. Anledningen bakom

valet av just flervåningshus var att flera lägenheter i samma hus ger en större chans att kunna se fler trådlösa nätverk samtidigt. Denna anledning gör det också viktigt att undersöka just de platser eftersom lägenheternas närhet till varandra innebär att ett oskyddat nätverk kan komma åt av flera grannar, ett problem som till exempel privathus som ligger längre ifrån varandra inte har i samma utsträckning. För att se de olika nätverken användes en laptop av märket Zepto med ett trådlöst nätverkskort Intel(R) WiFi Link 5300 AGN. Den gav möjligheten att se de olika nätverk samt vilken krypteringsalgoritm som de använde. Detta experiment var menad att ge data endast om krypteringen eftersom MAC-filtreringen inte kunde kontrolleras med denna metod.

5.3 Litteraturstudie

Litteraturstudie pågick under hela undersökningen. Den användes för att både ta fram ett bakgrund, sätta undersökningen i ett större sammanhang genom att relatera till andra områden och undersökningar samt för att tolka de olika resultaten. Syftet var att se till att majoriteten av källor kom från "peer-reviewed" tidsskrifter men det förekommer även en del annat material såsom "white papers".

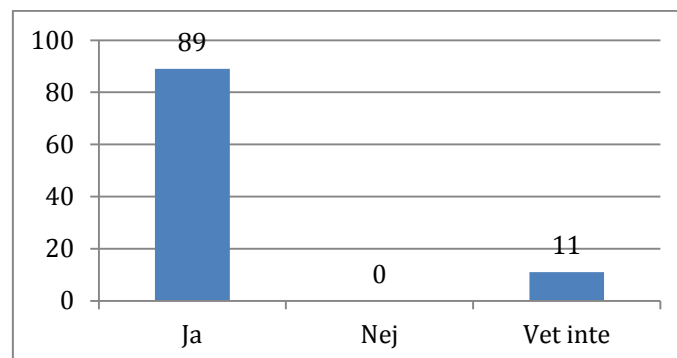
6 Resultat och analys

I detta kapitel kommer de olika delfrågorna samt huvudfrågan att besvaras. De olika svaren kommer att tas fram genom att analysera data från ovanstående undersökningar. I varje delfråga kommer det att presenteras de delar av resultat från ovanstående undersökningar som är relevanta för respektive delfråga. Denna data kommer att analyseras och användas för att besvara frågan. Slutligen kommer huvudfrågan att behandlas. Eftersom delfrågorna som har tagits fram är biståndsdelar av huvudfrågan, kommer svaret på huvudfrågan baseras på svaren på delfrågor och vara en summering av dessa. Resultat från enkätundersökningen består av svar från 100 deltagare. Därför motsvarar de olika siffror, som presenteras här, antalet deltagare som har svarat på ett eller annat sätt. I vissa svar överskrider det sammanlagda siffran från de olika alternativ antalet deltagare. Det beror på att fler än en alternativ kunde väljas som svar på frågan.

6.1 Skadlig kod

Syftet med denna delfråga är att ta reda på hur mycket som hemanvändare kan om antivirusmjukvaror samt om dessa används på ett optimalt sätt för att skydda mot diverse virus. Enkäten innehåller 5 frågor som hör till delen som handlar om skadlig kod.

1. Använder du antivirusmjukvaror?

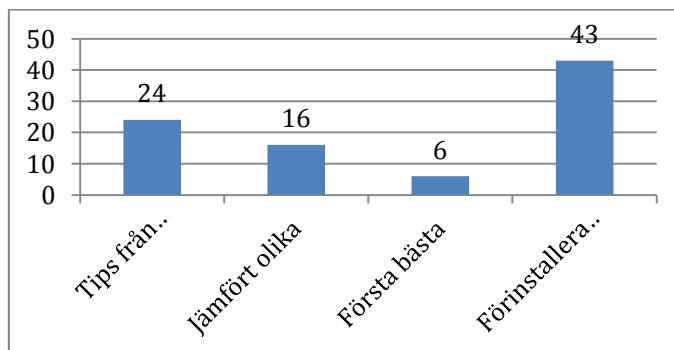


Majoriteten (89 personer) svarade att de använder antivirusmjukvaror. Dessutom hade ingen svarat att de inte använder någon antivirusmjukvara alls. Det som kan härledas från de två punkterna tillsammans är att de flesta verkar känna till att antivirusmjukvaran är en viktig del av säker datoranvändning. Det är dock endast första steget som inte säger något om hur antivirusmjukvaran används men den visar på en viss medvetenhet gällande vikten av antivirusmjukvaror. Vad gäller de 11 personer som svarade "Vet inte" kan det tolkas på olika sätt, dels så skulle det kunna bero på att de delar en dator med en annan person som sköter administreringen men det skulle även kunna innebära att de antingen saknar antivirusmjukvaran eller helt enkelt inte använder den. Det första antagandet har mindre allvarliga konsekvenser då datorn kan i själva verket vara fullt skyddad då det sköts av någon annan. Det kan dock ha vissa långsiktiga konsekvenser i och med att personen som inte är insatt i hur en dator ska skyddas kommer att få svårigheter om denne hamnar i en situation där han eller hon själv får ansvaret för det.

Det andra antagandet innebär i sin tur att användaren saknar ett effektivt skydd mot virus. Även om det finns en antivirusmjukvara installerad på datorn kan användarens ovetskap innebära att den inte uppdateras regelbundet samt att datorn inte skannas efter virus (mer

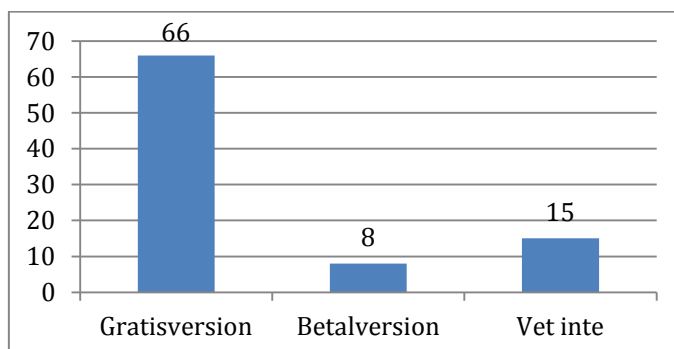
om detta längre fram). Båda alternativen innebär en brist på ett optimalt viruskydd. Det leder till att användaren kan lätt bli utsatt för diverse virus med de olika konsekvenserna som följer, såsom stöld av personlig data. I en sådan situation kan fler personer än själva användaren drabbas eftersom viruset kan då spridas vidare. Spridningen behöver inte nödvändigtvis begränsa sig till användarens hemmanätverk heller. Eftersom många idag har tillgång till bärbara datorer samt bärbara minnen kan dessa utnyttjas av viruset för att spridas vidare till andra nätverk där användaren kopplar in sig.

2. Hur har du valt antivirusmjukvaran som du använder (svara endast om du svarade ja på första frågan)?



Här handlar det om hur användaren går tillväga för att välja en antivirusmjukvara. Det används för att se var användaren lägger fokus vid detta val. Syftet är att få en inblick i hur mycket användaren tänker på att uppnå en optimal säkerhet. Majoriteten, som utgjordes av 43 personer, svarade att de väljer att använda antivirusmjukvaran som var förinstallerad på datorn. Utan att säga något om själva mjukvaran i frågan så är det möjligt att anta att de användare som valde detta alternativ har ett mindre fokus på säkerhet och känner sig nöjda av att veta att det finns något skydd installerad. Det säger inte något om hur bra dator är skyddad i slutändan men det visar att användaren har en tendens att fokusera mer på om dator är skyddad eller inte än på hur bra den är skyddad. Samma sak gäller för de 6 som har valt att ta första bästa antivirusmjukvaran som de hittar. Däremot de 24 som gick efter tips från sina bekanta samt de 16 som jämförde olika tar det ett steg vidare och utgår från att alla antivirusmjukvaror är inte likvärdiga. Det visar på en mer säkerhetsinriktad inställning och visar att även de som inte har någon erfarenhet vad gäller informations säkerheten väljer att söka kunskap genom att rådfråga andra. Det kan i sin tur ge blandade slutresultat som beror på den andra personens kriterier för valet av antivirusmjukvara men det visar på ett intresse för att få en optimal antiviruskydd.

3. Använder du gratis- eller betalversionen (svara endast om du svarade ja på första frågan)?



Denna fråga syftar till att undersöka hur många hemanvändare är villiga att betala för viruskydd. Många företag erbjuder en gratisversion av sin antivirusmjukvara som har de grundläggande funktioner. Det brukar finnas många andra funktioner utöver detta som är menade att förhöja säkerheten ytterligare och som är en del av en betalversion av mjukvaran (se Figur 2).

Download new avast! version 7
and get the world's most popular antivirus
(150 107 324 active users and growing)

Or, learn more about our most powerful security:
[avast! Pro Antivirus](#) & [avast! Internet Security](#)

	Free Antivirus	Pro Antivirus	Internet Security
Engine: Blocks viruses & spyware	✓	✓	✓
Remote: Allows assistance from a geek friend	✓	✓	✓
SafeZone: Secures shopping & banking		✓	✓
Sandbox: Lets you surf the web virtually		✓	✓
Sandbox: Runs risky programs virtually		✓	✓
Firewall: Blocks hacker attacks			✓
Firewall: Secures personal data			✓
Firewall: Secures your identity			✓
Anti-spam: Stops annoying SPAM			✓
Anti-spam: Blocks phishing scams			✓

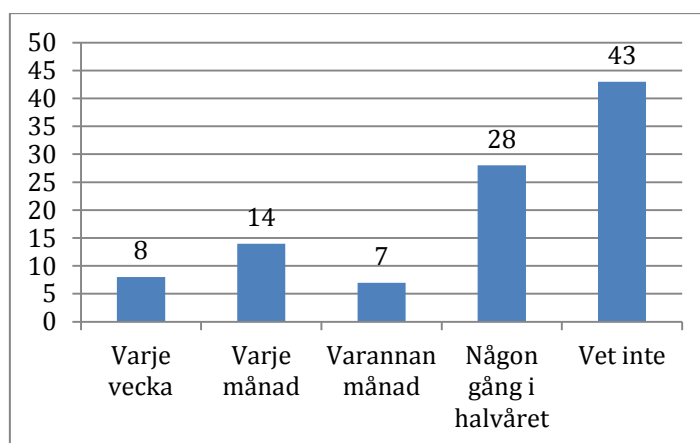
*avast! Free Antivirus is only for personal and non-commercial use

DOWNLOAD * DOWNLOAD DOWNLOAD

Figur 2 Olika versioner av antivirusmjukvaran Avast (www.avast.com, 2012)

En stor majoritet på 66 personer svarade att de väljer att använda en gratisversion. Det visar på att trots många hemanvändare tar hänsyn till informationssäkerheten så anser de inte att det är något som är värt att lägga extrapengar på. De flesta verkar nöja sig med grundskyddet som gratisversioner erbjuder. Det kan tolkas som att antivirusmjukvaran blir nedprioriterad på grund av diverse andra utgifter alternativt att hemanvändare ser det grundläggande skyddet som fullt tillräcklig. Vad gäller andelen som svarade "Vet inte" kan det, tillsammans med tidigare data om hur många väljer att använda den förinstallerade antivirusmjukvaran, tolkas som många verkar vara osäkra på om mjukvaran som följer med en ny dator är gratis eller ingår i dess pris.

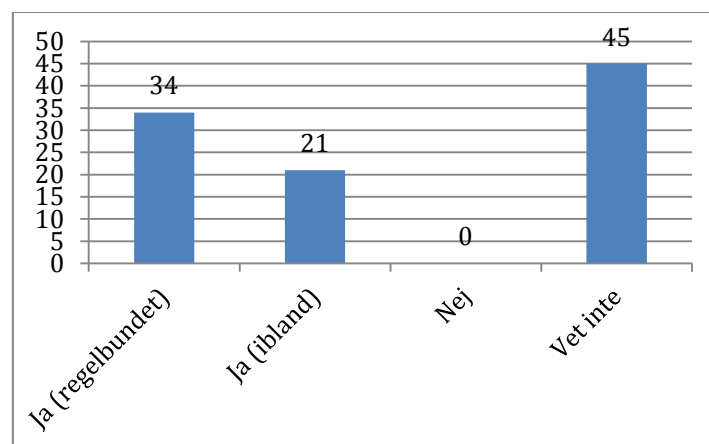
4. Hur ofta skannar du din dator efter virus?



Genom att analysera resultat från denna fråga kan informationen om hur antivirusmjukvaran används tas fram. Därmed kan ytterligare data samlas kring frågan om vare sig användare

nöjer sig med en närvaro av en antivirusmjukvara eller om de aktivt använder den för att skydda sig mot virus. En mindre procent av deltagare svarade här att de skannar sin dator regelbundet, dvs. varje vecka eller månad. Den regelbundna virusskanningen skulle då kunna vara antingen manuell eller en inställning i mjukvaran som gör att skanningen utförs regelbundet. I båda fallen har användare gjort ett medvetet val att utföra virusskanningen vilket visar på en viss säkerhetstänkande. De som väljer att utföra skanningen någon gång i halvåret kan ses som en mer passiv grupp. Motiveringen här är att de verkar känna till behovet att utföra regelbundna skanningar men av en eller annan anledning utför det väldigt sällan. Det visar på en tendens att nedprioritera säkerheten så länge ett akut behov saknas. Personer som var osäkra på skanningsfrekvensen kan tolkas som de som har minst intresse för informationssäkerhet och blir också en del av gruppen som väljer att nöja sig med en vetskap att de har en antivirusmjukvara installerad.

5. Uppdaterar du din antivirusmjukvara?



Denna fråga har en liknande syfte till den föregående, dvs. att ta reda på om användare aktivt använder sig av antivirusmjukvaran. Frågan är viktig på grund av faktumet att antivirusmjukvaror letar efter virus utifrån diverse kännetecken som mjukvaran känner till. Den nya uppdateringen innehåller ofta kännetecken på nya virus som tidigare varit okända. Detta är nödvändigt för att antivirusmjukvaran ska kunna upptäcka de och bristen på dessa uppdateringar kan innebära att nya virus inte upptäcks. Cohen (1987) skriver att det är omöjligt att ta fram en algoritm som kan upptäcka alla möjliga virus. Därför minskas skyddet från en antivirusmjukvara som inte regelbundet uppdateras med nya virusdefinitioner

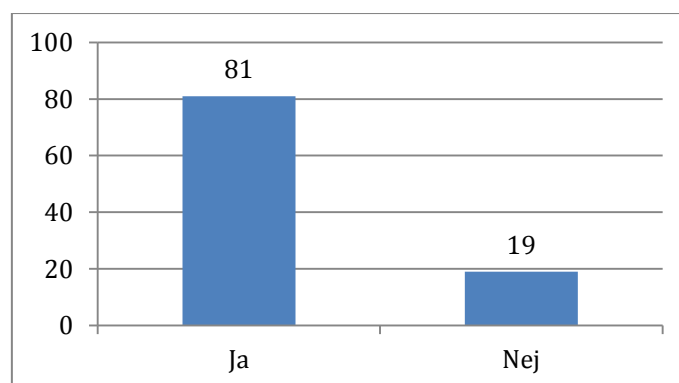
34 deltagare har svarat att de regelbundet uppdaterar sin antivirusmjukvara och ytterligare 21 väljer att göra samma sak, dock mindre regelbundet. Det, tillsammans med faktumet att ingen av deltagare aktivt avfärdar uppdateringar, visar på att över hälften av deltagare ser uppdateringar som något positivt och nödvändigt. 45 deltagare svarade på att de är osäkra på om antivirusmjukvaran uppdateras. Faktumet att de valde att svara "Vet inte" istället för "Nej" visar att även de känner till att uppdateringar är inget som ska avfärdas. Däremot visar det på att de inte gör något aktivt själva för att försäkra att deras antivirusmjukvara håller sig uppdaterad. Det kan råda om bristen på kunskap samt, även här, peka på att många användare ser antivirusmjukvaran som något som behöver finnas på en dator men som i stort inte behöver någon tillsyn från användarens sida. Vissa antivirusmjukvaror kan utföra automatiska uppdateringar som inte är initierade av användaren. Det påverkar dock inte denna undersökning eftersom den handlar inte bara om aktivt deltagande men även om användarens kännedom kring det.

Delfrågan här handlar om att ta reda på hur mycket kan en hemanvändare om antivirusmjukvaror samt användningen av dessa. Den samlade bilden utifrån deltagarnas svar på de olika frågorna visar att majoriteten känner till att en antivirusmjukvara är nödvändig. Siffran börjar dock sjunka när det kommer till den praktiska användningen. Runt 40% av deltagare väljer att lägga ner tid på att välja en antivirusmjukvara, vare sig om det handlar om att rådfråga en bekant eller jämföra olika mjukvaror själv. Dock är det lika många som väljer att använda den förinstallerade antivirusmjukvaran som kommer med datorn. En överväldigande majoritet väljer att använda gratisversionen trots att många tillverkare försöker vara väldigt tydliga med vilka funktioner som saknas ifrån den jämfört med betalversionen (se Figur 2). När det gäller användningen av antivirusmjukvaran är det runt hälften av deltagare som inte kunde svara på hur ofta deras dator skannas efter virus eller om själva antivirusmjukvaran hålls uppdaterad. Det som kan härledas från allt detta är att trots faktumet att majoriteten känner till behovet av en antivirusmjukvara verkar minst hälften av deltagare nöja sig med en vetskap att den finns installerad samt litar på att den ska sköta sig själv. Denna data kan vidare användas av olika företag då en användare med en infekterad dator kan potentiellt sprida vidare viruset till företaget genom att ta med sin infekterade bärbara dator eller USB-minne. Kondakci (2009) beskriver skadekostnaden som ett virus kan potentiellt orsaka på ett företag.

6.2 Backups

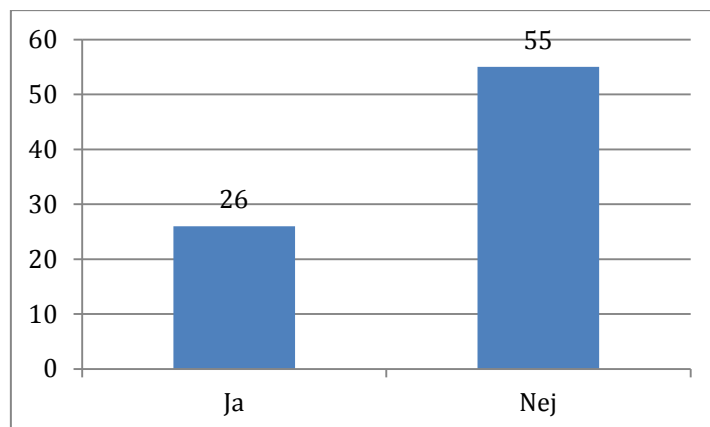
Denna delfråga undersöker situationen kring säkerhetskopieringen. Antalet deltagare som skulle potentiellt dra nytta av säkerhetskopiering tas fram och ställs emot antalet som utför säkerhetskopiering. Här granskas även vilka metoder som används för lagring av backups samt antalet deltagare som har råkat ut för en dataförlust. Enkätdelen som handlar om backups består av 5 frågor.

1. Har du filer, som du är rädd för att bli av med (semesterbilder, diverse dokument osv.), lagrade på din dator/USB/extern hårddisk/CD?



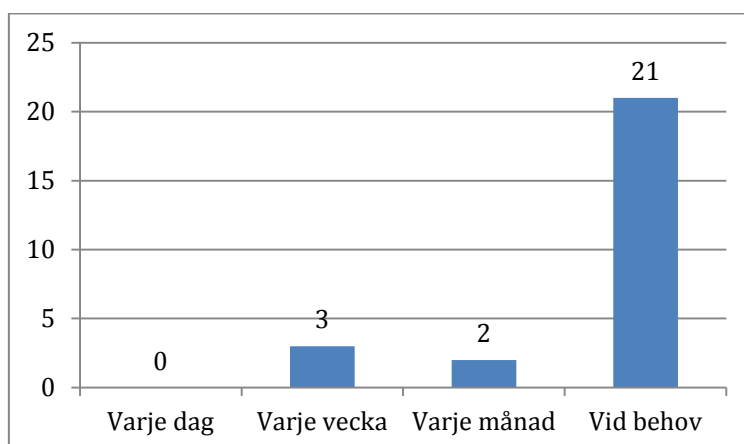
För att ta reda på hur hemanvändare sköter backups är det först viktigt att ta reda på antalet hemanvändare som skulle dra nytta av att säkerhetskopiera sin filer. I och med dagens digitalisering kan det antas att många användare har filer som för de är oersättliga, lagrade på sina datorer, som till exempel semesterbilder. Undersökningen visar att 81 deltagare har filer som de är rädda för att bli av med. Den data kan användas i följande steg för att se hur många hemanvändare som skulle kunna dra nytta av backups faktiskt säkerhetskopierar sina filer.

2. Brukar du ta backups (svara endast om du svarade ja på första frågan)?



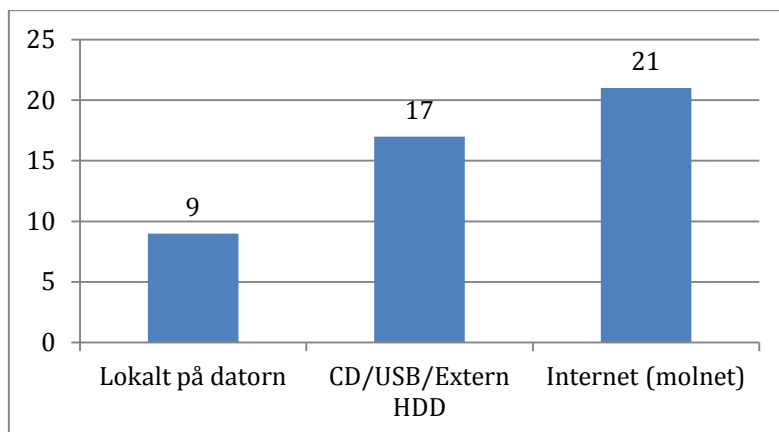
Endast en tredjedel av de som teoretiskt sätt skulle dra nytta av att ta backups faktiskt gör det. Det innebär att två tredjedelar skulle kunna bli av med filer som de anser som väldigt viktiga utan att kunna återställa dessa filer ifall användare i frågan råkade ut för en säkerhetsincident. Sådana siffror kan tyda på en bristande säkerhetsmedvetenhet hos en stor del hemanvändare när det gäller att bevara sina filer.

3. Hur ofta tar du backups (svara endast om du brukar ta backups)?



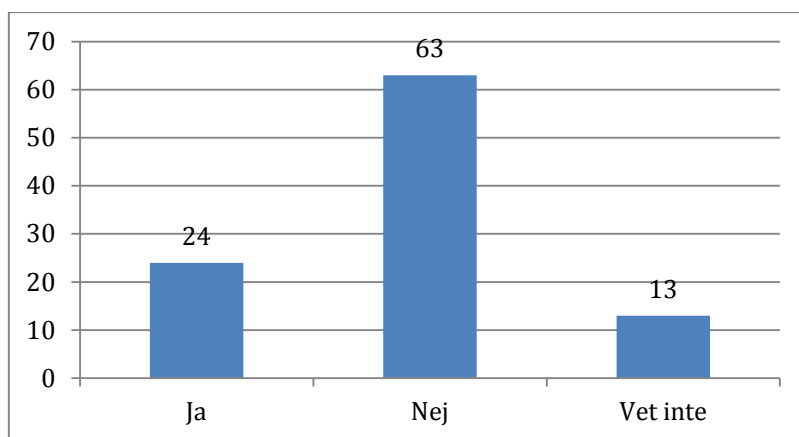
Den här frågan visar på hur hemanvändare går tillväga när de tar backups. Det verkar som att få har en rutin när det gäller backups utan de flesta tar backups manuellt när det sker en förändring som kräver en backup. Bristen på automatisering medför en viss ansvar eftersom användaren själv måste avgöra när en ny backup behövs och aktivt göra den. Dessutom kräver det en nivå av organisering när det kommer till lagringen av backups för att hålla koll på senaste versionen samt undvika dubbellagring.

4. Var lagrar du dina backups (svara endast om du brukar ta backups)? (kan välja flera alternativ)



För att backups ska tjäna sitt syfte, dvs. minimera konsekvensen av dataförlust, måste de lagras på ett säkert sätt. Det innebär lagringen av backup separat från originalfilen för att inte bli påverkade av datorhaveri. 9 deltagare, hälften av de som använder sig av backups, har svarat att de lagrar sina backups lokalt på datorn. Denna lösning kan fungera i vissa fall som till exempel om dator har två fysiska hårddiskar. Skyddet som denna metod erbjuder är dock mer begränsad än alternativet där backups lagras separat. De flesta deltagare väljer också att använda flera olika lagringsalternativ med Internet och bärbara medier som vanligast. Undersökningen visar även på en tydlig trend i samband med lagring av backups på Internet. Tjänster som DropBox och SkyDrive erbjuder både gratis och betalalternativ för olika lagringskapaciteter och undersökningen visar det vara ett populärt alternativ.

5. Har du någonsin varit med om dataförlust?



Denna fråga visar hur vanligt det är med dataförlust hos hemanvändare. Nästan en fjärdedel har svarat att de faktiskt har varit med om en dataförlust. Den siffran skulle kunna tjäna som en motivation för fler hemanvändare att använda sig av backups. Antalet deltagare som har varit med om en dataförlust sammanfaller grovt med antalet deltagare som väljer att ta backups. Det kan innebära en initial brist på säkerhetsmedvetenheten samt kännedomen av risker. Det verkar som att det påverkas mycket av själva säkerhetsincidenten som förtydligar behovet av att effektivt skydda sig mot dataförlust. Den höga siffran gällande dataförlust kan i denna undersökning hänvisas till att dataförlust här kan bero på allt från virus och datahaveri till förlusten av ett USB-minne.

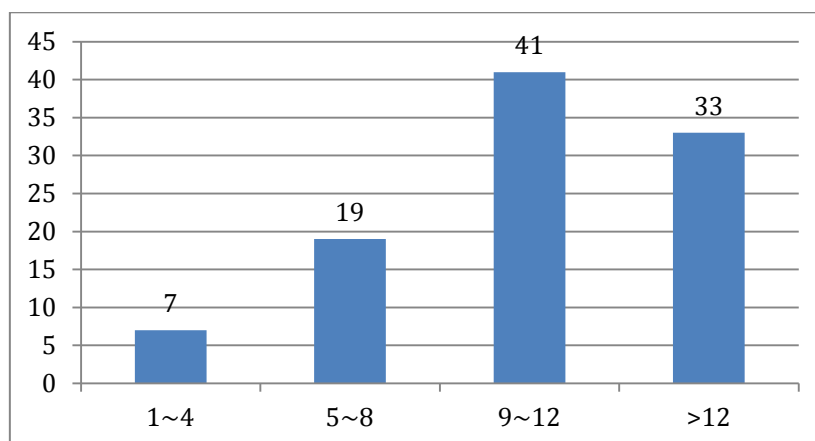
De sammanfattade resultaten visar att majoriteten av deltagare har många filer som de är rädda att bli av med. Trots det är det bara en tredjedel av de som faktiskt använder sig av

backups. Dessutom sammanfaller detta antal med antalet som har vid ett eller annat tillfälle varit med om en dataförlust. Det innebär att själva dataförlusten kan vara det som tydligt illustrerar för användare konsekvenser med bristen på backups och därmed motiverar de att använda sig av dem framöver. Utifrån detta kan det göras en slutsats att både behovet och intresset för att skydda sina filer finns hos majoriteten av användare. Problemet är dock just bristen på kännedom om hur stor risken är för att bli av med data, utifrån resultat av fråga 5, samt uppskattningen av personliga konsekvenser som det kan medföra. När det gäller själva backups så väljer de flesta hemanvändare att göra de manuellt och vid behov. Endast ett fåtal svarade att de hade någon rutin gällande backup. Som medier för lagring av dessa verkar de flesta välja att kombinera flera olika sätt och majoriteten använder sig av både bärbara medier och Internet. Drygt hälften dock lagrade sina backups lokalt vilket inte kan skydda filerna mot incident som total datorhaveri eller datorstöld.

6.3 Lösenord

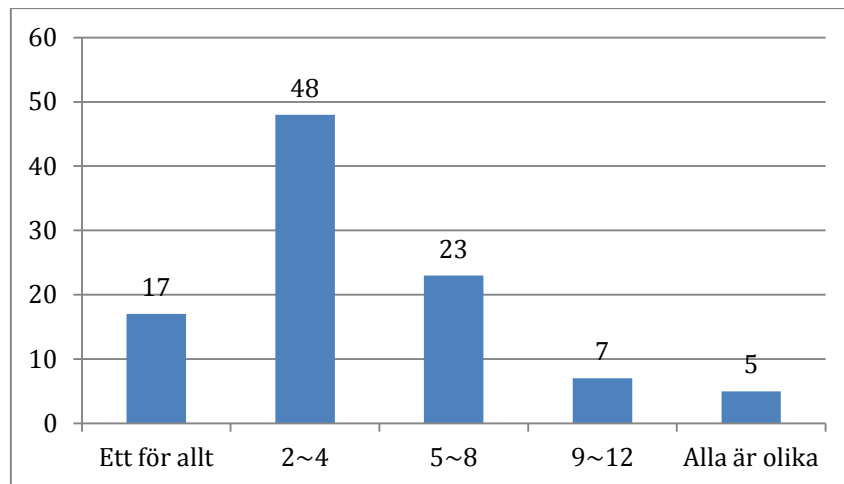
Delfrågan behandlar hanteringen av lösenord och sambandet mellan antalet lösenord och tendensen att återanvända dessa. Hanteringen av lösenord omfattar förvaringen samt lösenordskomplexitet och frekvensen för byte av lösenord. Enkät delen som handlar om lösenord består av 6 frågor.

1. Hur många sidor/tjänster/program använder du som kräver lösenord?



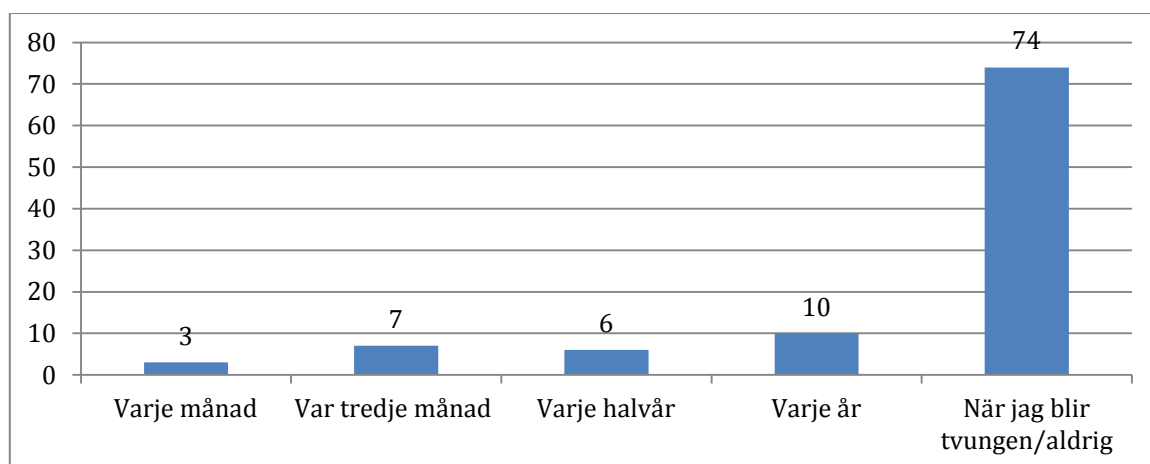
Syftet med att fråga efter antalet tjänster som kräver lösenord är att ta reda på hur många lösenord totalt som en hemanvändare behöver hålla koll på. Ett stort antal lösenord kan resultera i att användaren börjar återanvända samma lösenord för flera tjänster eller skriva ner de (Gehring, 2008). I båda fallen minskar säkerheten som lösenord ämnar att tillhandahålla. Dessutom ju fler tjänster som kräver lösenord som används desto mer tidskrävande blir det att byta lösenord regelbundet. Data från denna fråga kommer i följande frågor att utvärderas genom att ställas emot data om lösenordsbyte, lagringen av lösenord samt återanvändningen.

2. Hur många OLIKA lösenord använder du, dvs. hur många lösenord har du som skiljer sig från varandra?



När samma lösenord används för ett flertal olika tjänster innebär det större konsekvenser om lösenordet skulle komma ut. Angriparen får genast tillgång till ett flertal tjänster istället för en. Gehringer (2008) beskriver sambandet mellan antalet lösenord som användaren behöver hålla reda på och tendensen att återanvända samma lösenord. Resultatet från denna fråga stödjer detta. Nästan tre fjärdedelar använde sig av 9 eller fler tjänster som kräver lösenord och den här frågan visar att 17 personer använder samma lösenord för alla tjänster och nästan hälften använder mellan 2 och 4 lösenord som skiljer sig från varandra. Antalet sjunker mer och mer ju fler olika lösenord det handlar om. Anledningen till att majoriteten har valt mellan 2 och 4 lösenord skulle kunna tolkas med att det finns olika krav vad gäller lösenordskomplexiteten bland olika tjänster vilket tvingar även de som försöker använda ett lösenord för allt att anpassa sig. Samma teori kan vara en förklaring till att inte mer än 17 har valt alternativet med ett lösenord för alla tjänster. Resultat från denna fråga kan jämföras med en undersökning av Stone-Gross (2009) som visade att 28% av deltagare återanvänder sina lösenord. Studien specificerar dock inte i vilken grad som lösenord återanvänds.

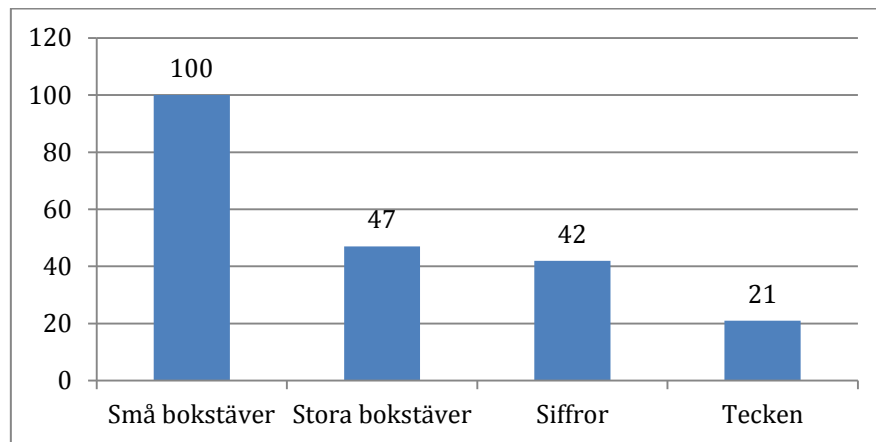
3. Hur ofta byter du lösenord?



Här visas det väldigt tydligt tendensen som hemanvändare har när det kommer till lösenordshantering. Nästan tre fjärdedelar har svarat att de byter sina lösenord antingen aldrig eller när de blir tvungna (till exempel återställning av ett glömt lösenord). Resten av svaren var spridda över de andra alternativen och var mindre signifikanta jämfört med majoriteten. Detta stödjer påståendet om att regelbundet byte av lösenord försvåras i och med användningen av ett flertal olika tjänster som kräver lösenord. Antalet sådana tjänster,

tillsammans med data kring återanvändningen samt byte av lösenord, visar på en ökad säkerhetsrisk för alla berörda användare.

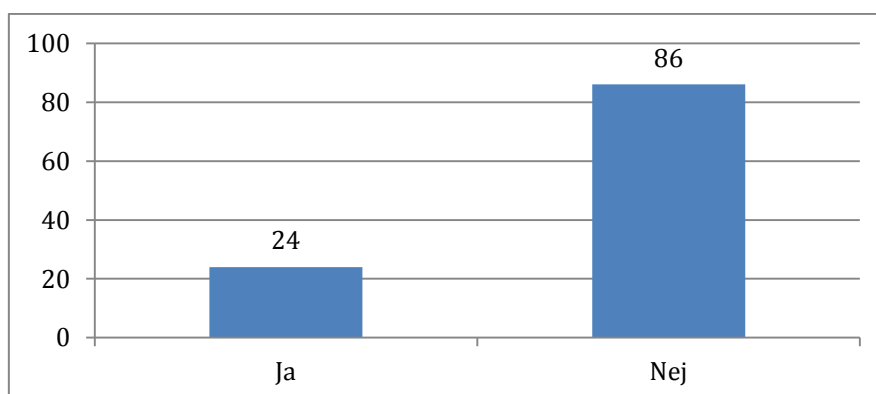
4. Vad består dina lösenord av (kan välja flera alternativ)?



Här undersöks komplexiteten som de olika deltagarnas lösenord har. Komplexiteten av ett lösenord spelar en stor roll när det gäller att skydda sig mot attacker såsom *brute force* (Burnet , 2005). Det illustrerades ytterligare i en undersökning genomförd av Stone-Gross (2009) där 40% av lösenord kunde gissas med *brute force* tekniken på mindre än 75 minuter.

Resultatet av enkätundersökningen visar att alla deltagare använde små bokstäver i sina lösenord. Lite mindre än hälften använde också antingen stora bokstäver, siffror eller båda. Endast en femtedel hade svarat att de använder även tecken i sina lösenord. Denna fråga säger inget om användarnas egna säkerhetsmedvetenhet gällande lösenordskomplexitet då komplexiteten kan dikteras av diverse krav som de olika tjänsterna har. Det som visas här är nuvarande fördelning bland deltagare gällande sammansättningen av ett lösenord.

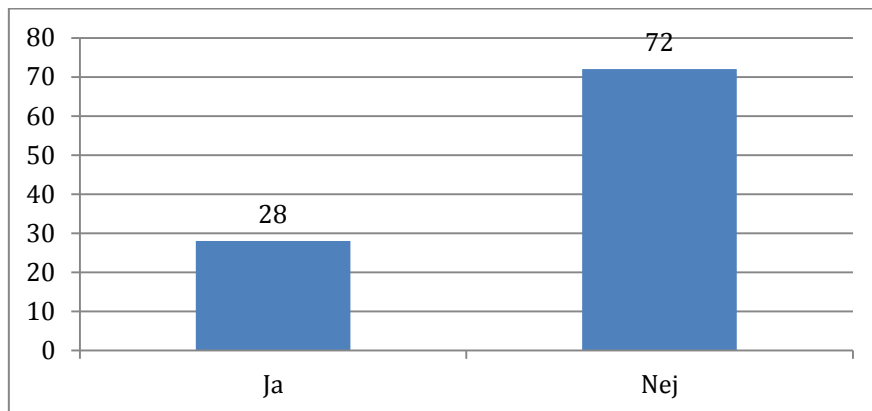
5. Finns ett eller fler av dina lösenord nedskrivna någonstans (papper, textfil, e-post, mobilen osv.)?



Som tidigare nämnts ökas chansen att användaren skriver ner sina lösenord med antalet av dessa. Undersökningen visar att nästan en fjärdedel väljer att skriva ner sina lösenord på ett eller annat sätt. Det minskar säkerheten eftersom angriparen får ytterligare ett sätt att ta reda på användarens lösenord. Det finns en del program som samlar in alla lösenord på ett ställe och användaren behöver endast hålla reda på ett lösenord för att komma åt dem. Det underlättar för själva användaren med medför också ett problem eftersom även angriparen

behöver endast få reda på ett lösenord för att kunna komma åt allt. Ett annat syfte med denna fråga är att komplettera data till följande fråga.

6. Finns det någon förutom dig som känner till en eller flera av dina lösenord?



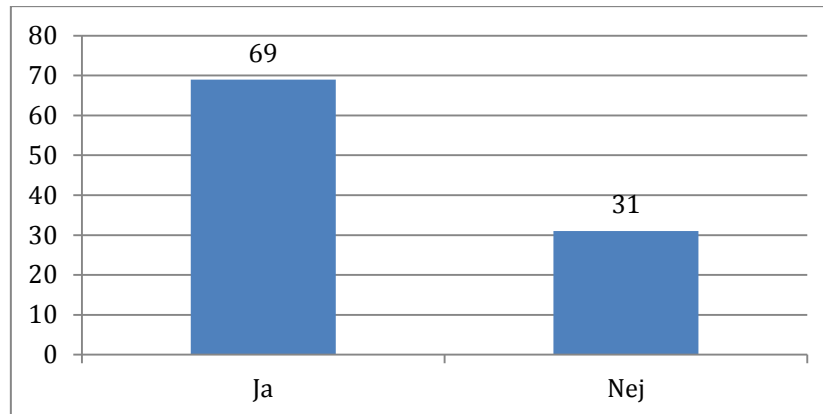
Mer än en fjärdedel av alla användare har svarat att de litar på andra med sina lösenord. Denna tillit i sig behöver inte innebära en drastisk riskökning då användaren förutsätter att den som får lösenordet inte kommer att missbruka den. Däremot kan data från denna fråga kombineras med den föregående. Den visar då att även om personen i frågan inte avsiktligt missburkar eller avslöjar lösenordet så har vissa användare en tendens att skriva ner lösenord och därmed negativt påverka säkerhetsnivån.

Sammanfattningen av de ovanstående frågorna ger en bild över nuvarande säkerhetssituationen samt hemanvändares tendenser gällande lösenordshantering. Majoriteten, nästan tre fjärdedelar, använder 9 eller fler tjänster som kräver lösenord. Samtidigt använder majoriteten fyra eller färre lösenord som skiljer sig ifrån varandra. Det innebär en ökad negativ konsekvens om en angripare skulle få reda på lösenordet. Risken för det ökas i och med att runt en fjärdedel av deltagare har sagt att de antingen skriver ner ett eller flera av sina lösenord eller har andra personer förutom de som känner till ett eller fler av dessa. Det intressanta här är att trots att majoriteten använder sig av ett fåtal olika lösenord väljer en fjärdedel ändå att skriva ner de. En teori kring det är att medans lösenorden kan återanvändas fritt mellan olika tjänster så kan användarnamnet skilja sig åt på fler ställen då det önskade användarnamnet behöver inte nödvändigtvis vara tillgänglig. Oavsett anledningen är det ett faktum att en fjärdedel av användare aktivt ökar risken för dataintrång genom att hantera sina lösenord på det ovannämnda sättet. Faktumet att majoriteten väljer att inte byta sina lösenord dessutom ökar risken ytterligare. Ett teoretiskt exempel är att om lösenordet ändras varje vecka får angriparen betydligt mindre tid på sig att få reda på det än om lösenordet bytts en gång i månaden. Även om användaren väljer att skriva ner eller dela med sig av sitt lösenord till andra så kan en regelbunden rutin för byte av lösenord höja säkerheten. Även om angriparen kommer över ett lösenord är chansen större att den är redan ogiltig. Lösenordsbyte påverkar även en annan aspekt, nämligen *brute force* attacker. Lösenordskomplexiteten påverkar tiden som en *brute force* attack kräver (Stone-Gross, 2009) vilket gör byte av lösenord relevant även här. Hälften av deltagare har svarat att de använder antingen stora bokstäver, siffror eller båda i sina lösenord vilket höjer deras resistans mot *brute force* attacker. Däremot faktumet att lösenordet inte ändras gör att en sådan attack kan pågå under en längre tid och därmed ha större chans att lyckas.

6.4 Trådlösa nätverk

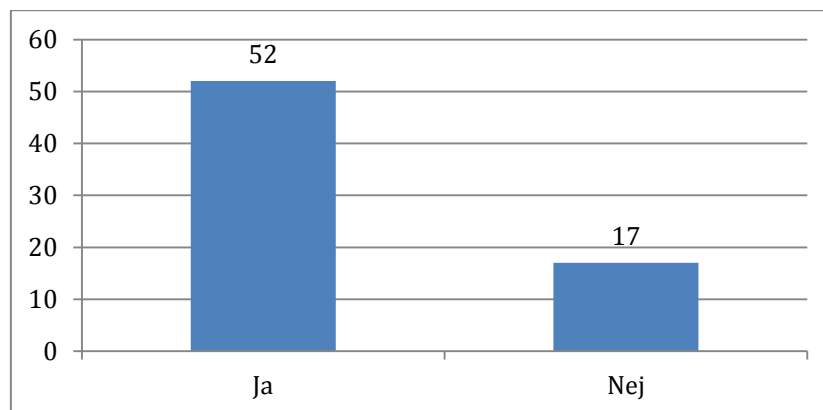
Delfrågan behandlar de olika metoder som används av hemanvändare för att skydda sina trådlösa nätverk samt i vilken utsträckning dessa metoder används. Data som används för att besvara delfrågan kommer från enkäten och från två olika experiment. Enkät delen som handlar om trådlösa nätverk består av 5 frågor.

1. Har du ett trådlöst nätverk hemma?



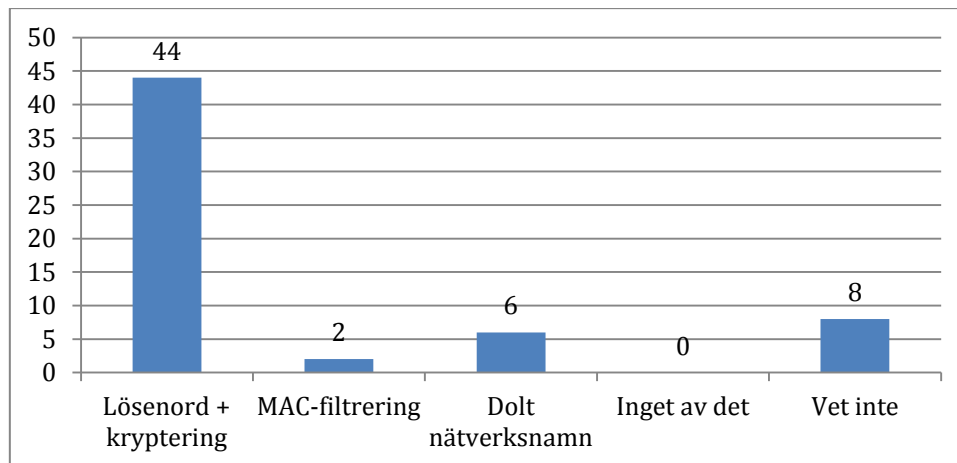
För denna delfråga är det viktigt att först identifiera de deltagare som har ett trådlöst nätverk hemma. Det görs för att se hur vanligt det är med trådlösa nätverk i hemmet. Följande 3 frågor kommer att handla om installation och skydd av det trådlösa nätverket och kommer därför endast att besvaras av de som har ett trådlöst nätverk hemma.

2. Var det du som installerade den trådlösa routern (svara endast om du svarade ja på föregående fråga)?



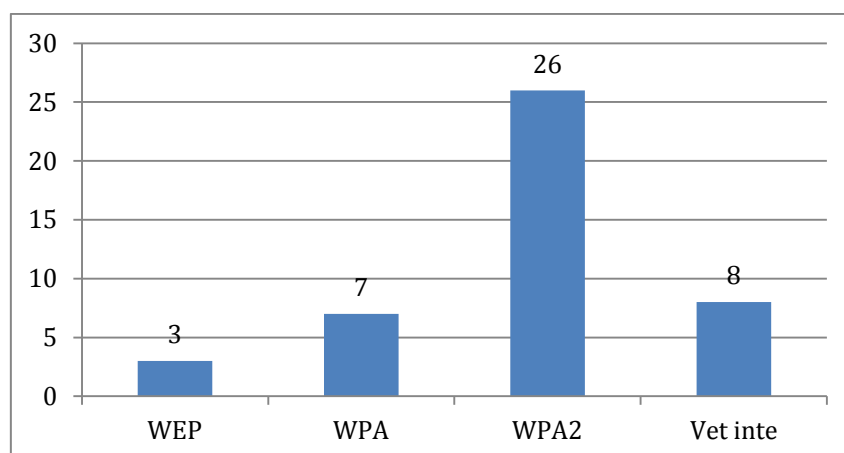
Syftet med denna fråga är att få fram de hemanvändare som har själva installerat det trådlösa routern. Hänsyn behöver tas till att deltagaren som svarar på enkäten behöver inte vara den som har installerat routern. Därför är det viktigt att identifiera just de personer som har installerat det eftersom det är just deras perspektiv som undersökningen eftersöker.

3. Hur skyddas ditt trådlösa nätverk (svara endast om du svarade ja på föregående fråga)? (kan välja flera alternativ)



Här undersöks vilken skydd som de olika hemanvändares trådlösa nätverk har. Alternativet med lösenord samt kryptering är den mest populära och används av majoriteten av deltagare. Eftersom krypteringen kan vara WEP, WPA eller WPA2 säger inte just denna fråga något om hur säker skyddet är men det visar på att deltagare känner till att det trådlösa nätverket behöver skyddas. Det styrkes ytterligare med faktumet att ingen valde alternativet där nätverket är helt oskyddat. Detta resultat kan då jämföras med tidigare resultat gällande antivirusmjukvaran. Även där var det ingen som svarade att de inte hade något skydd alls. Våldigt få använder sig av något mer utöver krypteringen, endast två deltagare använde MAC-filtrering och sex deltagare dolde nätverksnamnet. Däremot har åtta personer svarat att de inte visste hur deras nätverk var skyddat. Eftersom det var just de deltagare som hade hand om installationen samt att all skydd behöver konfigureras specifikt kan ett antagande göras att de åtta personer saknar ett skydd för sitt trådlösa nätverk. Eftersom många routers ämnade för hemmabruk fungerar direkt så fort de blir inkopplade (till exempel Belkin Wireless G Router), utan något skydd och med en förinställt nätverksnamn, kan användare som inte känner till det få en illusion att installationen är fullbordad eftersom de får tillgång till Internet. I själva verket är nätverket fullt öppet (se längre ner för praktiskt experimentdata om öppna nätverk). Det lämnar de sårbara för angripare som kan då lätt ta sig in i nätverket.

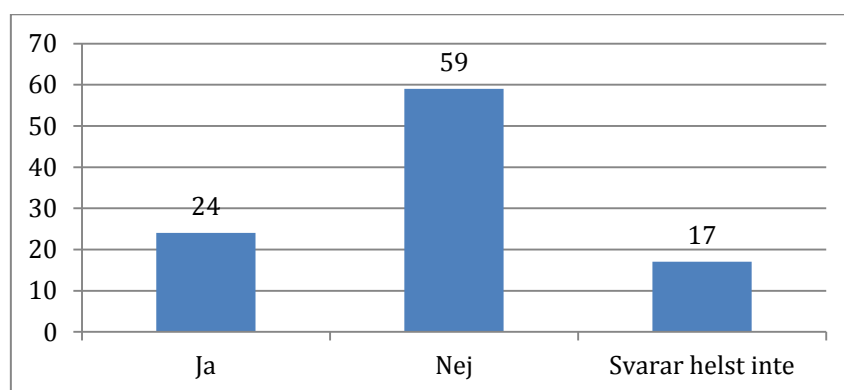
4. Vilken kryptering använder du (svara endast om du använder kryptering)?



Den här frågan ämnar att ta reda på vilken krypteringsalgoritm används bland de som använder kryptering. 26 personer har svarat att de använder WPA2 som är också den starkaste krypteringen (Lashkari, 2009). I denna grupp kan dock ingå två typer av

hemanvändare - de som valde WPA2 på grund av att den är starkast bland de tre och de som inte kände till skillnaden och valde det på ren slump. Undersökning ger ingen information gällande den detaljen, däremot visar den att över hälften av deltagare har valt den bästa krypteringsalgoritmen för skyddet av sitt trådlösa nätverk. Kvarstående 18 personer har valt antingen WEP, WPA eller har svarat "Vet inte". Alla de tre fall innebär när de ställdes inför valet så har de antingen valt slumpmässigt eller blivit felaktigt informerade. Den felaktiga informationen kan i vissa fall även komma från tillverkaren (se 3. Problem). Det innebär att anledningen bakom deras val har varit brist på kunskap eftersom de aktivt försökte säkra upp sitt nätverk men som, undersökningen visar, inte visste vilken krypteringsalgoritm är starkast.

5. Har du någonsin använt någon annans trådlösa nätverk (utan tillåtelse) för att surfa?



Här visas data på hur vanligt det är att hemanvändare använder sig av andras nätverk utan tillåtelse. Det visar även hur vanligt det är med nätverk som har dålig skydd eller saknar den helt och hållet. Eftersom denna fråga kan anses vara känslig finns det ett alternativ för de som väljer att inte svara. Det skapar ett visst mörkertal vilket innebär att en fjärdedel eller mer av deltagare har vid något tillfälle använt någon annans trådlösa nätverk utan tillåtelse. Det verkar dessutom vara väldigt vanligt med oskyddade trådlösa nätverk då en på fyra har haft tillgång till minst en. Sådana siffror utgör en bra motivering för hemanvändare att säkra upp sitt trådlösa nätverk.

Experimentet användes för att styrka data från enkätundersökningen gällande användningen av kryptering för skydd av trådlösa nätverk. Tabellen nedan visar resultat från olika mätställen samt en sammanfattning av dessa från det första experimentet.

	Hus 1	Hus 2	Hus 3	Hus 4	Hus 5	Hus 6	Hus 7	Hus 8	Hus 9	Hus 10	Sammanfattning
WEP	1	2	0	0	1	0	0	0	1	0	5
WPA	1	0	2	1	1	2	1	0	1	0	9
WPA2	6	7	7	5	8	7	6	9	7	7	69
Öppet	0	1	2	0	0	0	1	0	0	0	4
Totalt	8	10	11	6	10	9	8	9	9	7	87

Det andra experimentet gick ut på att låta 10 deltagare installera en trådlös router för att se vilken skydd de använder för det trådlösa nätverket. Liksom förra experimentet var syftet att införskaffa data som skulle användas för att backa upp delen av undersökningen som handlade om skyddet av det trådlösa nätverket. Följande tabell visar resultaten från detta experiment.

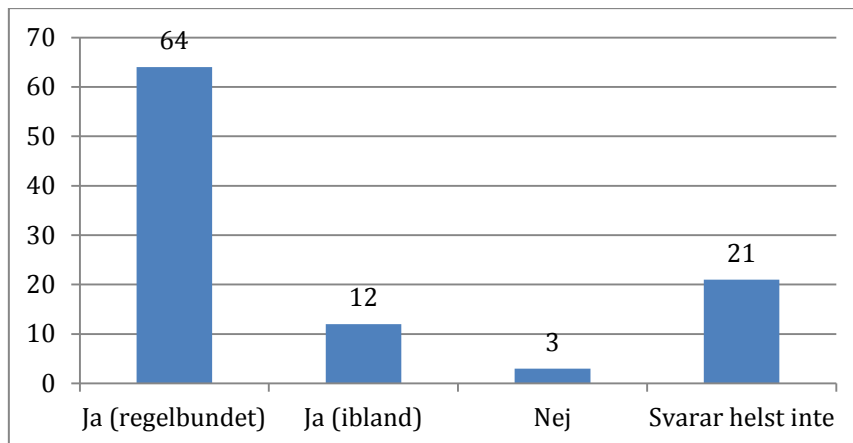
	Deltagare 1	Del. 2	Del. 3	Del. 4	Del. 5	Del. 6	Del. 7	Del. 8	Del. 9	Del. 10	Sammanfattning
WEP											0
WPA					X						1
WPA2	X	X	X	X		X	X	X		X	8
Öppet									X		1

Den ackumulerade data från enkäten samt experimentet visar att majoriteten av deltagare, som har ett trådlöst nätverk hemma som de själva har installerat, känner till att det finns ett behov att skydda den. Det framgår av att majoriteten har svarat att de använder något slags skydd för sitt trådlösa nätverk. Det stöds ytterligare med data från experimenten som visar att över 90% av testade trådlösa nätverk (från både mätningen och installationsexperimentet) har något slags skydd. Däremot är det inte alla som känner till hur nätverket ska skyddas på bästa sättet som visas av användningen av andra krypteringsalgoritmer än WPA2 samt andelen deltagare som inte visste vilken krypteringsalgoritm som användes. 24 personer har svarat att de har vid något tillfälle använt någon annans trådlösa nätverk utan tillåtelse, ett antal som skulle kunna vara ännu högre på grund av mörkertalet som utgjordes av 17 personer. Det är ett högt tal jämfört med antalet som faktiskt har ett bra skydd på sitt nätverk. Det kan dock förklaras med flera faktorer. Runt två tredjedelar har sagt att de har ett trådlöst nätverk hemma. Mätningsexperimentet har visat bland annat att det inte är helt ovanligt att kunna se 8-9 trådlösa nätverk för de som bor i ett höghus. Allt detta kombinerat med antalet som har bristande eller inget skydd på sitt trådlösa nätverk förklarar det höga antalet deltagare som har använt andras trådlösa nätverk. Detta antal visar dessutom hur vanligt det är med att trådlösa nätverk med dålig skydd utnyttjas av andra och kan användas som en motivering att säkra upp sitt nätverk.

6.5 Säkert beteende

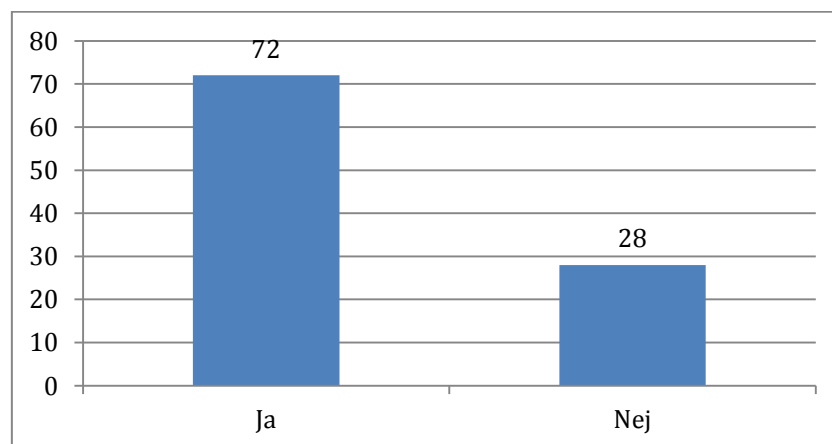
Delfrågan behandlar olika aspekter av hemanvändares beteende som kan påverka säkerhetsnivån. Det handlar om olika aktiviteter som kan öka risken för virussmittan samt faktorer som ökar risken för att bli av med personlig information såsom lösenord. Enkät delen som handlar om säkert beteende består av 5 frågor.

1. Laddar du ner piratkopierade filer?



Den frågan har en direkt relation till säker IT-användning. Som det har nämnts tidigare brukar virus utge sig för att vara en legitim mjukvara, alternativt vara inbäddade i mjukvaror som annars är fullständigt legitima och exekveras tillsammans med dem. När användaren laddar ner piratkopierad mjukvara finns det inga garantier att den inte innehåller virus. Denna mjukvara är oftast förändrad på ett sätt som låter användaren bruka den utan att behöva införskaffa en giltig licens. Den förändringen behöver då inte begränsa sig till att göra mjukvaran "öppen" utan kan lika väl inkludera ett virus. En annan aspekt som gör piratkopierade filer farliga ur virussympunkten är att det, till skillnad från legitima distributörer, är väldigt svårt att hitta de som är ytterst ansvariga. En person kan då ladda upp en fil som sedan delas vidare mellan ovetande användare medan den ansvarige har länge sedan slutat vara delaktig. Allt detta gör att de som laddar ner piratkopierade filer utsätter sig för en större risk att råka ut för ett virus. En överväldigande majoritet svarade här att de laddar ner piratkopierade filer regelbundet samt en mindre del (12 personer) som gör det ibland. Dessutom finns det även ett mörkertal på 21 personer som valde att inte svara då denna fråga kan i vissa fall vara känslig. Oavsett så är det tre fjärdedelar eller fler som laddar ner piratkopierad mjukvara. Denna siffra kan jämföras med resultatet från antivirusdelen där kring hälften av deltagare inte gjorde några regelbundna viruskanningar eller uppdateringar. Resultatet blir då att majoriteten av deltagare utsätter sig för en ökad risk för virusmitta och runt hälften av dem saknar en optimal skydd.

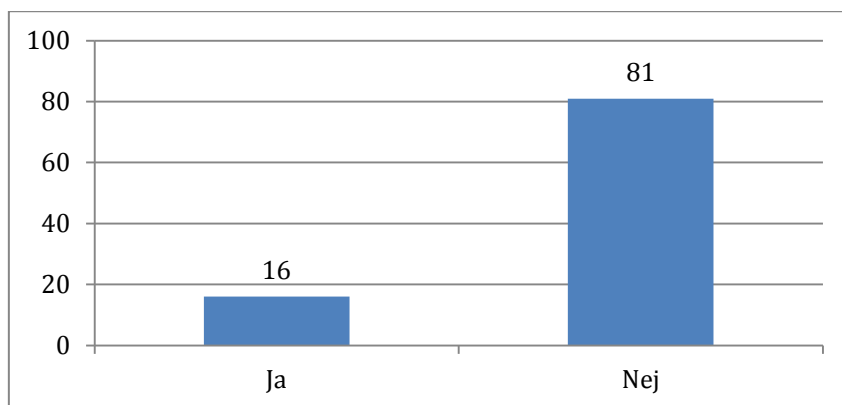
2. Öppnar du e-post från okända avsändare?



Den här punkten har mycket gemensamt med den föregående eftersom båda handlar om att minimera risken att bli utsatt för virus. E-post är en annan känd distributionsväg för diverse

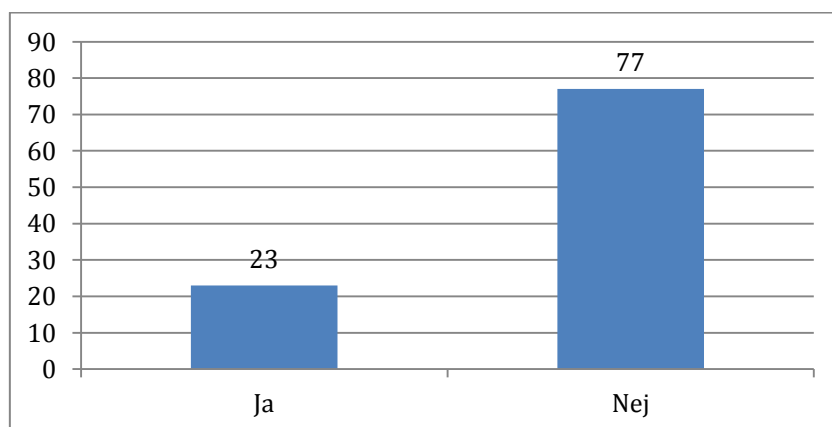
virus och risken att bli utsatt ökas om användaren väljer att öppna e-post från okända avsändare. Nästan tre fjärdedelar svarade här att de öppnar de e-post. Även här kan paralleller dras till antivirusdelen och dra samma slutsatser. Förutom virus kan e-post från okända avsändare vara en *phishing* attack (Applegate, 2009). Denna attack innebär att avsändaren ger sig ut för någon annan, helst en auktoritär person, och an en eller annan, till synes legitim, anledning frågar efter användarens personliga information.

3. Skulle du kunna tänka dig att överlämna personlig information över Internet om motparten skulle legitimt identifiera sig?



Denna fråga är avsiktligt felformulerad. Poängen är att det inte går att legitimt identifiera sig över Internet på ett sätt där det går att entydigt veta att personen i frågan är den som denne ger sig ut för att vara. Med hjälp av den formuleringen kan informationen tas fram om hur många deltagare är mottagliga för en typ av attack som brukar kallas *phishing* (Applegate, 2009). 16 deltagare svarade ja vilket tillsammans med data från föregående fråga om e-post från okända avsändare kan tolkas som att de löper en stor risk att bli utsatta för en lyckad *phishing* attack.

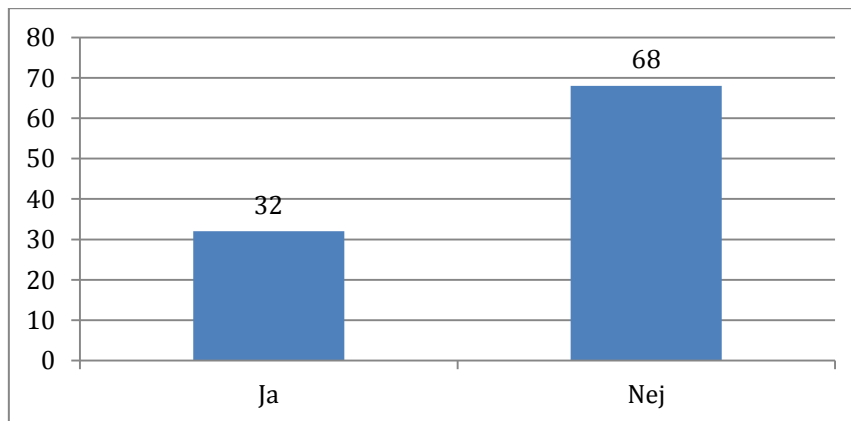
4. Skulle du kunna tänka dig att överlämna personlig information över telefon om motparten skulle legitimt identifiera sig?



Den här frågan följer samma tankegång som den föregående. Den går dock ut på att jämföra och identifiera om det finns någon skillnad mellan kontakten över Internet och kontakten över telefon. Attacker av samma natur som *phishing* kan på samma sätt utföras över telefon. I detta fall är det fler deltagare, nästan en fjärdedel, som svarade att de skulle överlämna personlig information över telefon. Det kan tolkas som att denna sorts kontakt upplevs som

mindre distanserad jämfört med Internet och verkar därför mer pålitlig men liksom med föregående fallet så finns det inga sätt att legitimera sig tillräckligt väl för att rättfärdiga överlämningen av personlig information som beskrivs av Mitnick (2002).

5. Har du bekanta som du kommunicerar med över Internet men som du aldrig har träffat ansikte mot ansikte?



Sidor som Facebook möjliggör kommunikation över Internet mellan personer som aldrig har träffats ansikte mot ansikte. Poängen är att eftersom kommunikationen sker endast över Internet så finns det inga garantier att personen är den som den ger sig ut för att vara. Det möjliggör en *social engineering* attack beskriven av Mitnick (2002) som går ut på att angriparen kommer i kontakt med offret och inleder en relation byggd på gemensamma intressen eller dylikt. Syftet är att med tiden få offrets tillit varpå angriparen kan försöka ta reda på offrets personliga information såsom lösenord eller annan information. En jämförelse mellan antalet som svarade ja på den här frågan och antalet som skulle kunna tänka sig att ge ut personlig information över Internet visar att drygt 15% har en ökad risk för att bli utsatta för denna sorts attack.

En sammanfattning från denna del visar att många hemanvändare ökar risken att bli utsatta för virus samt *social engineering* angrepp genom sina IT-vanor. Majoriteten av alla deltagare laddar ner piratkopierad programvara samtidigt som hälften av dem saknar en optimal viruskydd. Liknande situation råder kring hanteringen av e-post från okända avsändare där tre fjärdedelar av alla deltagare har svarat att de brukar öppna sådana e-post. Förutom virus kan e-post även innebära *phishing* attacker och 16 deltagare har svarat att de skulle kunna tänka sig att lämna ut personlig data över Internet. Detta svar innebär även faktumet att dessa personer skulle anse det som legitimt om motparten identifierade sig över Internet. Ännu fler, 23 personer, har sagt att de skulle lämna ut personlig information över telefon. Det tyder på att kommunikation över telefon uppfattas som mer förtroendeingivande. Slutligen har en tredjedel svarat att de håller kontakt med personer över Internet som de aldrig har träffat ansikte mot ansikte vilket gör dessa hemanvändare sårbara för *social engineering* attacker.

6.6 Sammanfattning

Delen av undersökningen som handlar om skadlig kod har visat att majoriteten av hemanvändare känner till behovet av antivirusmjukvaran, något som görs ännu tydligare på grund av att ingen av deltagare har svarat att de väljer att inte använda det. Däremot ser bilden lite annorlunda ut när det kommer till användningen av antivirusmjukvaran. Omkring

hälften av deltagare hade svårt för att svara på hur ofta deras dator skannas efter virus eller hur ofta antivirusmjukvaran uppdateras. Shabtai (2011) beskriver så kallade *zero-day threats*, virus som utnyttjar svagheter med en ny version av operativsystemet eller annan mjukvara. Det visar att det ständigt uppkommer nya virus som hittills har varit okända för antivirusmjukvaran. För att hantera nya virus fyller utvecklare på antivirusmjukvaror med nya definitioner för vad som utgör ett virus. Om antivirusmjukvaran inte uppdateras med dessa definitioner kommer den inte att kunna upptäcka nya virus vilket i det här fallet lämnar runt hälften av undersökningens deltagare utan ett adekvat virusskydd. Det backas upp vidare av Cohen (1987) som påstår att det inte kan finnas en algoritm som kan upptäcka alla virus vilket vidare illustrerar behovet av uppdateringar. Undersökningen har även visat att 40% procent av deltagare lägger ner tid på att välja antivirusmjukvaran genom att rådfråga andra och jämföra själv. Det är dock lika många som fortsätter använda den förinstallerade antivirusmjukvaran. Det i sig behöver inte innebära ett problem eftersom det kan röra sig om en mjukvara som de är nöjda med men kombinerat med data om uppdateringen och virusskanningen kan det tolkas på ett annat sätt. Det verkar nämligen som att runt hälften av deltagare nöjer sig med tanken att det finns en antivirusmjukvara installerad och därmed är deras dator skyddad. Undersökningen visade även att väldigt få väl av deltagande hemanvändare väljer att lägga pengar på antivirusmjukvaran. Även det, tolkat tillsammans med övrig data, kan ses som ett tecken på att säkerheten är något nedprioriterad.

Virusrisken som undersökningen har visat kan innebära bland annat dataförlust för användare vilket gör det viktigt att ha en återställningsplan i form av backup. Undersökningen visade även att majoriteten av deltagare har viktiga filer på sin dator som de är rädda att bli av med. Trots det så var det endast en femtedel som säkerhetskopierade sina filer. I och med det bristande virusskyddet kan detta innebära att andra deltagare löper en ökad risk att bli av med viktiga filer. Det intressanta här var att antalet som brukar ta backups sammanfaller grovt med de som har varit med om en dataförlust. Utifrån det kan ett antagande göras att bristen på säkerhetsmedvetenheten spelar en stor roll här. Dataförlusten var just det som ökade säkerhetsmedvetenheten genom att praktiskt demonstrera konsekvensen som bristen på backups kan innebära. Den informationen skulle kunna användas för att informera fler användare om fördelar med backups utan att de ska behöva gå miste om viktiga filer.

En annan aspekt av informationssäkerheten som undersökningen omfattar är lösenord. Resultaten har visat att nästan tre fjärdedelar av deltagare använder 9 eller fler tjänster som kräver lösenord. Här kan det röra sig om allt från inloggningen på dator till e-post eller bankkonto. Oavsett så handlar det i många fall om informationen som användaren vill skydda. Trots det visar det sig att många deltagare hanterar lösenord på ett sätt som kan utsätta dessa för en ökad risk. Majoriteten av deltagare återanvände sina lösenord på ett flertal platser. Praktiskt innebär det att en angripare som får reda på ett lösenord genast får tillgång till ett flertal platser. En teoretisk fördel med få lösenord skulle kunna vara att användaren har lätt för att komma ihåg de och därför inte behöver utsätta de för ytterligare risk genom att skriva ner sina lösenord. Undersökningen har dock visat att omkring en fjärdedel av deltagare väljer även att skriva ner sina lösenord. Det tillsammans med faktumet att lika många deltagare låter andra veta en eller flera av sina lösenord sänker den säkerhetsnivån som lösenord ska tillhandahålla. En annan sak, som också har en stor inverkan på säkerhet, som undersökningen visar är att majoritet på 74 deltagare har svarat att de byter sina lösenord endast när de blir tvungna eller aldrig. Allt detta tillsammans kan

resultera i att en angripare kan få tillgång till en eller flera av användarens konto samtidigt och kan en kontinuerlig tillgång till de utan användarens vetskap. Även här skulle de sammanställda fakta kring den sänkta lösenordssäkerheten användas för att uppmärksamma hemanvändare och höja deras säkerhetsmedvetenhet.

Frågan som behandlades med hjälp av både enkätundersökningen och experiment handlade och skyddet av trådlösa nätverk. Båda delarna har visat att över 90% deltagare försöker aktivt skydda sitt trådlösa nätverk. Även de fall där nätverket har ett mindre pålitlig skydd, som till exempel WEP kryptering, visar en viss förståelse för faktumet att nätverket behöver skyddas. Vissa paralleller kan dras till frågan kring antivirusmjukvaran. Även där kände majoriteten till behovet av ett skydd, dock saknades det i vissa fall djupare kunskap. Majoriteten av deltagare som skyddar sitt nätverk använder lösenord och kryptering i detta syfte. Majoriteten av de väljer även den starkaste algoritmen WPA2. Dock faktumet att både WEP och WPA också förekommer kan tyda på att vissa av de som väljer WPA2 väljer det av än slump snarare än grundat i kunskap. Slutligen kom det även fram att minst en fjärdedel av deltagare har vid något tillfälle använd någon annans trådlösa nätverk utan tillåtelse. Den höga siffran visar hur vanligt det är med dåligt skyddade trådlösa nätverk samt hur vanligt det är att dessa utnyttjas av andra.

Sista delen av undersökningen fokuserar sig på hemanvändares beteende, närmare bestämt beteende som kan potentiellt öka risken för diverse angrepp. Det visade sig att majoriteten av deltagare väljer att ladda ner piratkopierade filer och majoriteten av dessa gör det kontinuerligt. Det, kombinerat med antalet som saknar adekvat virussydd samt de som har viktiga filer på sin dator resulterar i en ökad risk för både virussmitta och dataförlust. Samma sak gäller hanteringen av e-post från okända avsändare. Förutom virusrisken innebär sådana e-post även risk för *phishing* attacker. Det blir ett ännu större hot då undersökningen visade att 16 deltagare skulle kunna vara villiga att lämna ut personlig data över Internet. Detta faktum blir ännu alvarligare när kombinerad med svaret att en tredjedel av deltagare håller kontakt över Internet med personer som de aldrig har träffat ansikte mot ansikte.

6.7 Slutsats

Huvudfrågan som studien ämnar att besvara handlar om att identifiera hemanvändarnas säkerhetsmedvetenhet samt den nuvarande säkerhetsnivån. De två delarna gå in i varandra då säkerhetsmedvetenheten påverkar säkerhetsnivån. Resultat från undersökningen har visat att många hemanvändare har en bristande säkerhetsmedvetenhet och därmed även bristande säkerhetsnivå. Det illustreras av de olika delfrågorna som behandlar diverse säkerhetsrelaterade områden och tillsammans skapar en bild över hemanvändarnas säkerhetsmedvetenhet samt säkerhetsnivå. Omkring hälften av deltagare har en bristande virussydd samtidigt som majoriteten utsätter sig för en ökad smittrisk genom att till exempel ladda ner piratkopierade filer. Det ökar risken för virusmittan även för olika arbetsplatser då spridningen kan ske genom infekterade USB-minnen. Risken ökas också för dataförlust vilket kan ha stora konsekvenser för individen som undersökningen visar då 80% av deltagare har en potentiell behov för säkerhetskopiering men endast en fjärdedel använder sig av den. Även det kan påverka arbetsplatsen då diverse arbetsrelaterade filer kan finnas lagrade på en hemdator. Det ser lite bättre ut när det kommer till skyddet av trådlösa nätverk där majoriteten är skyddade. Det råder dock en viss kunskapsbrist vilket leder till att det finns en del nätverk som saknar en adekvat skydd. Lösenordshanteringen bland hemanvändare har däremot en hel del brister då majoriteten väljer att återanvända sina

lösenord på flera platser och aldrig ändra de. Det och en svaghet för olika *phishing* attacker som drygt hälften av deltagare uppvisade innebär betydligt lägre säkerhet än vad lösenord kan tillhandahålla.

Allt detta visar på att säkerheten behöver höjas vilken kan åstadkommas genom att öka hemanvändares säkerhetsmedvetenhet. I de flesta fall har den bristande säkerheten visat sig bero på hemanvändarnas kunskapsbrist inom området. Denna kunskapsbrist varierar inom olika områden men oftast handlar om kunskaper som är grundläggande. Det ger ett underlag för vidare studier och indikerar en potentiell anledning för den bristande säkerheten. Fler studier behövs dock för att säkerställa både orsaken och åtgärder.

7 Diskussion

Detta kapitel innehåller diskussioner kring de etiska, samhällliga och vetenskapliga aspekter av studien. Här tas även upp diskussionen kring de valda metoder och erhållna resultat.

7.1 Metod

Metoden som valdes för undersökningen, först och främst enkätundersökningen, grundade sig i syftet att nå ut till så många som möjligt. Initialt övervägdes det en annan metod för detta, nämligen intervju. Fördelen där skulle vara en bättre kvalitet på data som samlades in tack vara kommunikationen. Anledningen att det valdes bort var just syftet att nå ut till ett stort antal deltagare. En intervju skulle vara mycket mer tidskrävande för att uppnå samma antal deltagare. Berndtsson (s.63, 2008) påstår att enkätundersökningen är ett bra sätt att nå ut till flera deltagare och som inte kräver stora resurser vilket också var utgångspunkten för detta arbete. En av punkterna i enkätundersökningen (trådlösa nätverk) behövde dock kompletteras och därför valdes ytterligare en metod, nämligen experimentet. Syftet här var att införskaffa mer data för att backa upp resultaten från enkäten. Den sista delen var en litteraturstudie som användes för att få en djupare förståelse för ämnet samt för att sätta problemet i ett större sammanhang. Alternativet som valdes bort från undersökningen var en intervju med anställda på diverse IT-verkstäder. Syftet var att ta reda på mer om problemets omfattning samt få ett annat perspektiv. Detta alternativ valdes bort på grund av tidsbrist och även för dess syfte fylldes till en viss del med resultat från litteraturstudie.

7.2 Resultat

Huvudfrågan med arbetet är att identifiera nuvarande situationen kring informationssäkerhet i hemmet samt hemanvändares säkerhetsmedvetenhet. Problemet som arbetet stöter på härstammar från avgränsningen. Undersökningen fokuserar på individer som inte har en IT-utbildning och som dagligen använder dator i hemmet. För att se till att undersökningen når rätt målgrupp innehåller enkäten två frågor som kollar om deltagaren har en utbildning inom IT samt om denne dagligen använder en dator i hemmet. Endast svar från deltagare som passar in i avgränsningen behandlas vidare. Det som utgör ett problem är att avgränsning, tillsammans med den valda metoden innebär att resultaten beror väldigt mycket på vilka individer som kommer att delta eftersom ett brett spektrum av individer med olika graders IT-intresse kan passa in inom denna avgränsning. Därför finns det risk för ensidiga resultat om majoriteten av undersökningens deltagare skulle visa sig vara antingen över eller under snittet vad gäller vanliga hemanvändare. Det är en av anledningarna till att ytterligare två metoder används förutom enkätundersökningen.

7.3 Etisk aspekt

Arbetet behandlar några frågor som är intressanta ur en etisk synpunkt. Den första handlar om nedladdning av piratkopierad programvara. Det är förbjudet enligt lag men är fortfarande väldigt vanligt förekommande som även undersökningen hade visat. Denna fråga tas upp i samband med delen som handlar om skadlig kod. Anledningen, som beskrivet tidigare, är att de piratkopierade filer kan innehålla virus vilket gör det relevant att undersöka nedladdningen av dessa då det innebär en ökad risk för att bli utsatt för virus. Problemet här ur ren undersökningssynpunkt är att få fram informationen om detta. Faktumet att nedladdningen av piratkopierade filer är olaglig gör ämnet känslig för många användare.

Detta hanteras på två olika sätt. Den ena sättet är att göra undersökningen anonym. Den andra är att inkludera ett svarsalternativ för de deltagare som väljer att inte svara. Detta skapar ett visst mörkertal och därmed gör denna punkt av undersökningen mindre exakt men istället möjliggör denna frågeställning. Samma sak gäller frågan om användning av andras trådlösa nätverk. Även denna handling är olaglig vilket också gör den till en känslig fråga och därför hanteras den på samma sätt. Användningen av frågor som handlar om olagliga handlingar i en undersökning kan också ifrågasättas ur den etiska aspekten. Anledningen till att dessa frågor tas upp är att de är menade att tjäna ett högre syfte. I fallet med piratkopierade filer är syftet att visa på vikten av en effektiv antivirusmjukvara genom att presentera data på hur vanligt det är med nedladdningen av dessa filer. Möjligheterna för spridning i och med den stora andelen användare som är inblandade lockar många angripare. Fallet med användningen av andras trådlösa nätverk syftar till att illustrera hur vanligt det är och därmed rikta användarnas fokus till behovet av att effektivt säkra sitt trådlösa nätverk.

7.4 Samhällelig aspekt

Samhällsnyttan som arbetet syftar till att bidra med är att uppmärksamma hemanvändare på den nuvarande säkerhetssituationen samt risker i samband med den. Även företag kan dra nytta av detta arbete då ett antagande kan göras att undersökningens deltagare även jobbar eller kommer att jobba i framtiden. Informationssäkerheten hemma kan då även påverka informationssäkerheten på en arbetsplats. En individ som har ett virus på sin hemdator kan potentiellt föra över den till arbetsdator genom att ovetande använda ett smittat USB-minne. Det gäller även aspekter av ett säkert beteende som till exempel hantering av e-post från okända avsändare eller hantering av lösenord.

Rekommendationen med detta arbete är att ta del av resultaten och försöka dra egna slutsatser om sin informationssäkerhet hemma. Det kan också vara viktigt att ställa sig de olika frågorna som ingår i formuläret och kritiskt utvärdera sina svar. Det kan ge användarna ett underlag för utvärdering av sin egen informationssäkerhet och en motivering att förbättra det. Undersökningen gällande säkerhetskopiering visade till exempel att antalet personer som tar backups sammanfaller grovt med de som har varit med om en dataförlust. Därför kan detta arbete ge en liknande insikt och därmed höja motivationen för att genomföra förebyggande arbete.

7.5 Vetenskaplig aspekt

Som det nämnts tidigare brukar de flesta studier som fokuserar på användare behandla frågan i ett arbetsplatssammanhang. Det verkar inte finnas några studier som undersöker säkerhetsmedvetenheten hos hemanvändare, speciellt sådana som omfattar flera aspekter av informationssäkerheten. Det kan dock vara viktigt eftersom hemanvändarens säkerhetsmedvetenhet samt säkerhetsnivå påverkar även arbetsplatsen. Ett virus kan till exempel spridas från en infekterad hemdator till arbetsplatsen genom ett USB-minne. Ett annat exempel är ett nedskrivet lösenord som ökar risken för dataintrång på en arbetsplats precis på samma sätt som hemma. Den vetenskapliga bidraget från studien är att visa på den bristande säkerheten hos hemanvändare samt visa hur den kan påverka även arbetsplatsen. På så sätt uppmärksammas en annan aspekt av informationssäkerheten som kan behöva lyftas fram ytterligare, nämligen hemanvändare. Resultaten kan även användas som grund och motivation för genomförandet av ett arbete vars syfte är förbättringen av säkerhetsnivån.

Enkäten som har tagits fram för studien kan också ses som en vetenskaplig bidrag och användas i vidare forskning, bland annat de förslag som nämns längre fram.

8 Framtida arbete

Undersökning fokuserar på att kartlägga nuvarande situation kring informationssäkerheten samt säkerhetsmedvetenheten hos hemanvändare och visade på en del områden där säkerheten är bristande. Därför skulle det vara intressant att ta reda på varför situationen ser ut som den gör och vad dessa brister beror på. Följande steg skulle vara att ta fram en lista på rekommendationer på hur denna situation kan förbättras.

En annan intressant punkt är att utöka målgruppen. Målgruppen här är hemanvändare utan tidigare IT-utbildning. Det skulle vara intressant att genomföra en liknande studie på personer som har en IT-utbildning. En undersökning av deras IT-vanor i hemmet skulle kunna göras för att sedan jämföra med resultat från detta arbetet och se om det finns några skillnader och vilka de skillnaderna är.

Referenser

- Al-Dossary, G. 1990. *Computer virus prevention and containment on mainframes*. Computers & Security
- Applegate S., 2009. *Social Engineering: Hacking the Wetware*. Information Security Journal: A Global Perspective.
- Beck M., Tews E., 2008. *Practical attacks against WEP and WPA*. Packet Storm Security.
- Berndtsson, M. Hansson, J. Olsson, B. & Lundell, B. (2008) *Thesis Projects (2:a upplagan)*. London: Springer.
- Besnard D., Arief B., 2003. *Computer security impaired by legitimate users*. Computers & Security.
- Biemer P., Lyberg L., 2003. *Introduction to survey quality*. John Wiley and Sons Publication.
- Bittau A., Handley M., Lackey J., 2006. *The final nail in WEP's coffin*. Security and Privacy.
- Burnett M., 2005. *Perfect Password: Selection, Protection, Authentication* s.7-10 och s.107-109. Syngress.
- Cohen F., 1987. *Computer Viruses: Theory and Experiments*. Computers and Security 6.
- Furnell S., 2005. *Why users cannot use security*. Computers & Security.
- Furnell S., Jusoh A., Katsabas D., 2005. *The challenges of understanding and using security: A survey of end-users*. Computers & Security.
- Furnell S., Tsaganigi V., Phippen A., 2008. *Security beliefs and barriers for novice Internet users*. Computers & Security.
- Gehringer, E. (2008) *Choosing passwords: security and human factors*. Citeseer.
- Graziani R., 2005. *Cisco Fundamentals of Wireless LANs version 1.1*. Cabrillo College.
- Harley C., Florêncio D., 2006. *How to login from an internet café without worrying about keyloggers*. Symposium on Usable Privacy and Security.
- Isaksson S., 2011. *Säkerhetsmedvetenhet gällande lösenordshantering*. Examensarbete vid Högskolan i Skövde.
- Kondakci S., 2009. *A concise cost analysis of Internet malware*. Computers & Security.
- Lashkari H., 2009. *A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)*. Computer Science and Information Technology.
- Mitnick K., Simon W., 2002. *The Art of Deception*. Wiley.
- Myndigheten för samhällsskydd och beredskap. *Datastödd informationssäkerhetsutbildning för användare (DISA)*. Tillgänglig på Internet: <http://disa.msb.se> [Hämtad 24.03.2012]

Nohlberg M., 2008. *Why Humans Are The Weakest Link*, in Gupta, M. and Sharman, R. Social and Human Elements in Information Security: Emerging Trends and Countermeasures, Idea Group, Inc.

Post- och telestyrelsen. *Internetsäkerhet för hemmet*. Tillgänglig på Internet: <http://www.pts.se/sv/Internet/Internetsakerhet/For-hemmet/> [Hämtad 24.03.2012]

Puri R., 2003. *Bots and Botnet: An Overview*. SANS Institute.

Richardsson R., 2008. *CSI Computer crime and security survey*. Computer Security Institute.

Securelist, 2011. *Spam report: March 2011*. Tillgänglig på Internet: http://www.securelist.com/en/analysis/204792171/Spam_report_March_2011 [Hämtad 27.04.2012]

Shabtai A., 2011. *F-Sign: Automatic, Function-Based Signature Generation for Malware*. Systems, Man and Cybernetics.

Stone-Gross B., Cova M., Cavallaro L., Gilbert B., Szydlowski M., Kemmer R., Kruegel C., Vigna G., 2009. *Your botnet is my botnet: Analysis of a botnet takeover*. CCS '09 Proceedings of the 16th ACM conference on Computer and communications security.

Zhou C.V., Leckie C., Karunasekera S., 2009. *A survey of coordinated attacks and collaborative intrusion detection*. Computers & Security.

Appendix A - Enkätfrågor

1. Använder du dator hemma varje dag?

Ja

Nej

2. Har du någon utbildning inom IT (både program och enstaka kurser räknas)?

Ja

Nej

Skadlig kod

1. Använder du antivirusmjukvara?

Ja

Nej

Vet inte

2. Hur har du valt antivirusmjukvaran som du använder (svara endast om du svarade ja på första frågan)?

Tips från andra

Jämfört olika

Första bästa

Antivirusmjukvaran som var förinstallerad

3. Använder du gratis- eller betalversionen (svara endast om du svarade ja på första frågan)?

Gratisversion

Betalversion

Vet inte

4. Hur ofta skannar du din dator efter virus?

Varje vecka

Varje månad

Varannan månad

Någon gång i halvåret

Vet inte

5. Uppdaterar du din antivirusmjukvara?

Ja (regelbundet)

Ja (ibland)

Nej

Vet inte

Backup

1. Har du filer, som du är rädd för att bli av med (semesterbilder, diverse dokument osv.), lagrade på din dator/USB/extern hårddisk/CD?

Ja

Nej

2. Brukar du ta backups (svara endast om du svarade ja på första frågan)?

Ja

Nej

3. Hur ofta tar du backups (svara endast om du brukar ta backups)?

Varje dag

Varje vecka

Varje månad

Vid behov

4. Var lagrar du dina backups (svara endast om du brukar ta backups)? *kan välja flera alternativ*

Lokalt på dator

CD/USB/Extern hårddisk

Internet (molntjänst)

5. Har du någonsin varit med om dataförlust?

Ja

Nej

Vet inte

Lösenord

1. Hur många sidor/tjänster/program använder du som kräver lösenord?

1-4

5-8

9-12

>12

2. Hur många OLIKA lösenord använder du, dvs. hur många lösenord har du som skiljer sig från varandra?

Ett lösenord för allt

2-4

5-8

9-12

Alla lösenord är olika

3. Hur ofta byter du lösenord?

Varje månad

Var tredje månad

Varje halvår

Varje år

När jag blir tvungen

4. Vad består dina lösenord av (kan välja flera alternativ)?

Små bokstäver

Stora bokstäver

Siffror

Tecken

5. Finns ett eller fler av dina lösenord nedskrivna någonstans (papper, textfil, e-post, mobilen osv.)?

Ja

Nej

6. Finns det någon som känner till en eller flera av dina lösenord?

Ja

Nej

Trådlösa nätverk

1. Har du ett trådlöst nätverk hemma?

Ja

Nej

2. Var det du som installerade den trådlösa routern (svara endast om du svarade ja på föregående fråga)?

Ja

Nej

3. Hur skyddas ditt trådlösa nätverk (svara endast om du svarade ja på föregående fråga)? *kan välja flera alternativ*

Lösenord + kryptering

MAC-filtrering

Dolt nätverksnamn

Inget av det

Vet inte

4. Vilken kryptering använder du (svara endast om du använder kryptering)?

WEP

WPA

WPA2

Vet inte

5. Har du någonsin använt någon annans trådlösa nätverk (utan tillåtelse) för att surfa?

Ja

Nej

Svarar helst inte

Säker beteende

1. Laddar du ner piratkopierade filer?

Ja

Nej

Svarar helst inte

2. Öppnar du e-post från okända avsändare?

Ja

Nej

3. Skulle du kunna tänka dig att överlämna personlig information över Internet om motparten skulle legitimt identifiera sig?

Ja

Nej

4. Skulle du kunna tänka dig att överlämna personlig information över telefon om motparten skulle legitimt identifiera sig?

Ja

Nej

5. Har du bekanta som du kommunicerar med över Internet men som du aldrig har träffat ansikte mot ansikte?

Ja

Nej