LUNDS UNIVERSITET
Ekonomihögskolan

Internetanvändande privatpersoners IT-säkerhetstänkande kontra experters: likheter, skillnader och orsaker

Kandidatuppsats, 15 högskolepoäng, SYSK01 i informatik

Framlagd: 02/06/2010

Författare: André Boysen
Dan Gunnarsson
Thomas Holm

Handledare: Anders Svensson
Examinatorer: Lars Fernebro
Claus Persson

Abstrakt

Titel: Internetanvändande privatpersoners IT-säkerhetstänkande kontra experters: likheter, skillnader och orsaker

Författare: André Boysen
Dan Gunnarsson
Thomas Holm

Utgivare: Institutionen för Informatik

Handledare: Anders Svensson

Examinatorer: Lars Fernebro
Claus Persson

Publiceringsår: 2010

Uppsatstyp: Kandidatuppsats

Språk: Svenska

Nyckelord: IT säkerhet, Internet, skadlig kod, säkerhetsmedvetenhet

Abstrakt
Eftersom Internetanvändandet blir allt mer vanligt i privatpersoners vardagliga sysslor och att hoten på Internet expanderar allt mer, så har vi här jämfört vad två experter från de ledande antivirusföretagen har för åsikter gentemot privatpersoners erfarenheter.

De empiriska data vi samlat in är hämtade via en webbenkät som är utskickad till ett femtiotal privatpersoner, i vilken vi kartlagt deras erfarenhet utav skadlig kod. Därefter har vi även ställt frågor till experter inom området för att sedan jämföra svaren med varandra och därefter dragit slutsatser utifrån det.

I vår undersökning fann vi att privatpersonerna hade mer erfarenhet av skadlig kod än vad vi antog. Det visade sig att kunskapsnivån var varierande, men ändå på en hög medelnivå.

Det visade sig att privatpersoner och experterna hade liknande synsätt på IT-säkerhet.

Innehållsförteckning

1. Introduktion

1.1 Bakgrund

Vi skulle kunna påstå att man har kontroll över sin egen dator och vilka program som ska utföra en koppling mellan varandra och hur denna ska gå till, men detta gäller bara tills första gången vi blir uppkopplade mot Internet (Gollmann, 2006). Om ett program ska vara säkert så krävs det pålitlighet. Ett program som innehåller många säkerhetshål, vilka är närmast omöjliga att aktivera för en vanlig användare är mer säkert än ett program som innehåller färre buggar, eftersom de i det senare programmet aktiveras under vanligt användande (Gollmann, 2006). Gollmann menar här att man inte är säker när man är uppkopplad mot Internet eftersom webbläsare och andra uppkopplade program ofta har säkerhetsbrister som är vanliga att utnyttjas av brottslingar.

Något som Pfleeger och Pfleeger (2003) specifikt nämner är att man måste utföra tydliga och genomgående test av programmen när de utvecklas, för att de ska bli så säkra som möjligt. Programmerarna kan ofta få kontroll över de flesta av de säkerhetsrisker som kan uppstå, men ytterligare kompetens från utomstående programmerare kan öka säkerheten. Speciellt om det finns många mindre delar som behöver kontrolleras. (Pfleeger och Pfleeger, 2003)

De två vanligaste formerna av skadlig kod är maskar och virus. De flesta vet inte skillnaden på maskar och virus, som helt olika typer av hot. Masken sprids genom att kod aktiveras och virus infekterar genom att användaren aktiverar det (Gollmann, 2006). Andra vanliga och oftast mer omfattande typer av skadlig kod är, trojanska hästar och logiska bomber.

Skadlig kod har en stor inverkan på världen

Microsoft (2010) har skrivit en rapport som beskriver bland annat hur skadlig kod ter sig världen över. Undersökningen är genomförd med bland annat verktyget *Windows Defender,* som är Microsofts egna antivirusprogram. Det är detta program som adderat ihop hur många olika datorer det har rensat ifrån skadlig kod.

Med 239.711 infekterade datorer ligger Sverige på tjugonde plats. Detta kan man jämföra med Kina som med totalt 3.333.368 infekterade datorer ligger på en andra plats. Dock är det viktigt att komma ihåg att det finns betydligt fler datorer i Kina än i Sverige.

Enligt Microsoft (2010) så har det skett en 21.5% ökning i antalet infekterade datorer i Sverige om man jämför första halvåret av 2009 med andra halvåret 2009 (197.242 till 239.711). En bidragande orsak till att skillnaden på antalet infekterade datorer är så stort är masken *Conficker*, detta intygar även Gustaf, en av de experter vi intervjuat.

Vilken skadlig kod är det som har störst spridning världen över?

Microsoft (2010) har även skapat en tabell där de listat vilka olika typer av skadlig kod som infekterat mest datorer. Denna tabell är grundad på Microsofts egna antivirusprogram som rensat infekterade datorer.

Datorvirus toppar listan och spridningen har bara på ett halvår ökat med 14,5%. På andra plats kommer olika sorter av trojanska hästar som ökat med 14-45,7% beroende på vilken typ av trojan det är. Den typ av skadlig kod som ökat mest det senaste halvåret är spionprogram (engelska spyware), som har ökat med 151,6%. Värt att nämna, är att tangentregistreringsprogram (engelska keyloggers) och andra kartläggningsprogram minskat med 68,7% det senaste halvåret.

Figur 1: Antal infekteringar av vanligaste hoten 1H09/2H09

Category	2H09	1H09	Difference
Viruses	71,991,221	68,008,496	5.9% ▲
Miscellaneous Trojans	26,881,574	23,474,539	14.5% ▲
Trojan Downloaders & Droppers	9,107,556	6,251,286	45.7% ▲
Misc. Potentially Unwanted Software	4,674,336	2,753,008	69.8% ▲
Adware	3,492,743	3,402,224	2.7% ▲
Exploits	3,341,427	1,311,250	154.8% ▲
Worms	3,006,966	2,707,560	11.1% ▲
Password Stealers & Monitoring Tools	2,217,902	7,087,141	-68.7% ▼
Backdoors	812,256	589,747	37.7% ▲
Spyware	678,273	269,556	151.6% ▲
Total	**126,204,254**	**115,854,807**	**8.9%**

(Microsoft: Security Intelligence Report Volume 8)

Diagrammet ovan beskriver dessa och ytterligare andra typer av skadlig kod och antalet infekteringar de orsakat över tid, uppdelad i första/andra halvåret 2009.

I detta arbete tar vi upp några av de vanligaste hoten och gör en jämförelse av hur privatpersoner och experter ser på dessa, samt hur de kan motverkas eller förhindras. För att tillföra ytterligare perspektiv, har vi valt att även jämföra med en teoretisk modell över hur människor tänker när det kommer till säkerhet i allmänhet och hotande situationer i synnerhet, samt hur dessa kan förhindras och lösas. Tidigare undersökningar som tillämpat denna modell visar på att människor av andra anledningar än okunskap väljer att inte skydda sig. (Enbody et al, 2008; Clarke et al, 2010; Postin & Stafford, 2010; Chenoweth et al, 2009; Rogers, 1975)

1.2 Problem

Internet kan vara farligt om man inte är säkerhetsmedveten. Om nu lösningar på säkerhetsproblemen finns tillgängliga, varför väljer man att inte att använda dem? Användare som inte skyddar sig utsätter inte bara sig själva för risker utan även

andra användare, då deras dator kan bli ett medium för spridning av skadlig programvara. Hur och var lär sig de internetanvändande privatpersonerna om farorna och är det något datasäkerhetsleverantörerna missar när de marknadsför sina produkter?

1.3 Frågeställning

Frågan vi valt belysa berör såväl Internetanvändande privatpersoner och datasäkerhetsleverantörer som organisationer där privatpersonerna utövar sin profession.

Vår huvudsakliga frågeställning är följande:

Hur säkerhetsmedvetna är Internetanvändande privatpersoner i jämförelse med vad experter inom området anser önskvärt, samt finns det några bakomliggande orsaker till privatpersonens omedvetet/medvetet valda säkerhetsnivå?

Delas upp i följande delfrågor:

- *Hur ser säkerhetsläget ut just nu?*
- *Hur skiljer sig experternas syn på säkerhet från användarnas?*
- *Kan man se några mönster som funnits i andra undersökningar som använt sig av Protection motivation theory i vår undersökning också?*

1.4 Syfte

Syftet med studien är dels att undersöka hur IT-säkerhetsmedvetna Internetanvändande privatpersoner är , samt utröna deras attityd inför farorna vid användning av Internet.

1.5 Avgränsningar

Vi har avgränsat oss till att undersöka de hot som finns vid Internetanvändning. Vårt intervjuformulär kommer besvaras av människor med tillgång till Internet och email, således lämnas de som inte har tillgång till detta utanför.

Vi har även valt att begränsa oss till hotet skadlig kod, med skadlig kod reserverar vi oss för de hot som byggs upp av någon form av kodad logik som orsakar skada ekonomiskt eller på hårdvaran. Social ingenjörskonst tas också upp för att det är ett utbrett hot för framförallt Internetanvändare.

Den psykologiska teori vi valt att tillämpa för att tolka den data vi samlar in är Rogers protection motivation theory, PMT (1975). Denna modell består av 4 variabler, vilka stimulerar de kognitiva processerna som leder till hur en person agerar när denne utsätts för fara.

De experter som vi intervjuat är experter anställda av de större datasäkerhetsföretagen.

Fokus ligger på hur säkerhetsmedvetna privatpersoner är gentemot vad som enligt experter är önskvärt. Kan vi se några mönster eller samband med vad man kommit fram till tidigare med PMT hos dem som *inte* valt att tillämpa säkerhetslösningen.

2. Teoretiska utgångspunkter

Nedan kommer vi gå igenom de vanligaste formerna av skadlig kod som finns på Internet idag. En kort beskrivning av hur dessa former av skadlig kod fungerar kommer även att ges. Vi har även valt att inkludera social ingenjörskonst (engelska social engineering), trots att detta inte är baserat på skadlig kod, då detta blivit alltmer vanligt idag. Hur ESET's Threatsense.NET fungerar kommer även behandlas. Till sist presenteras den teori vi valt att applicera på vår data för att kunna jämföra vår data med tidigare undersökningar inom IT-säkerhetsområdet.

2.1 Vilka är de vanligaste hoten på Internet?

Detta kapitel behandlar vad skadlig kod är och i korta drag hur det fungerar. Skadlig kod är det svenska ordet för malware, men även i vissa sammanhang kallat malicious software. De vanligaste formerna av skadlig kod kommer att tas upp. Det är viktigt för läsaren att förstå de olika begreppen som avhandlas löpande genom uppsatsen.

Idag har betydelsen av begreppet skadlig kod breddats och kan definieras olika, beroende på sammanhanget. Skadlig kod är väsentligen ett program med avsikt att samla information eller orsaka skada. Skadlig kod installeras på datorn utan användarens tillåtelse. Ursprungligen var det virus man syftade på när man talade om skadlig kod. Med tiden har det utvecklats en rad olika former av skadlig kod som opererar på olika sätt och därför har man fått inkludera fler begrepp som faller under skadlig kod. (Pfleeger & Pfleeger, 2003)

Den skadliga kod som bland annat återfinns på Internet kan sedan delas upp i underkategorierna virus, trojanska hästar och maskar. Dessa tre begrepp kan man i sin tur kan dela in i ytterligare mindre delar. (Pfleeger & Pfleeger, 2003)

2.1.1 Datorvirus

Datorvirus påminner mycket om hur ett biologiskt virus fungerar. Likt ett biologiskt virus kan inte ett datorvirus reproducera sig utan att ha tillgång till en värdkropp. Datorvirus reproducerar sig genom att sprida sig själv vidare till andra datorer eller program. Hur ett virus opererar är helt upp till det syfte skaparen hade i åtanke. De vanligaste syftena virus har är, borttagning av filer, lösenordskopiering samt stölder av filer. Virus är ofta gömda i andra program, ibland till och med i operativsystemet. Avancerade virus kan ibland även ta kontroll över datorn, vilket medför att skaparen kan göra vad denne vill med infekterade datorn.

Kännetecknande för datorvirus är följande:

- Det sprider sig själv: Datorviruset tillverkar kopior av sig själv och sprider sig

vidare till nästa värd.

• Måste köras: Ett datorvirus måste bli startad av någon eller något för att fungera. Det är därför viruset oftast använder sig av operativsystemet som startmotor och på så vis startas datorviruset varje gång operativsystemet startas. Virus kan aktiveras på två sätt, första typen exekveras efter en satt tid. Den andra logiska typen exekveras efter att ett visst tillstånd hos den attackerade har uppnåtts.

• Effekter: Ett datorvirus innehåller kod för att förstöra eller att förändra data.

• Osynligt för ögat: Ett datorvirus vill inte bli upptäckt eftersom risken då är stor att man tar bort det/ det blir borttaget. Viruset har därför två möjligheter att undvika att bli upptäckt, genom kryptering eller smygteknik.

(Pfleeger & Pfleeger, 2003; Dubrawsky, 2007)

2.1.2 Trojanska hästar

En trojansk häst fungerar på ett liknande sätt som ett virus. Den största skillnaden är att trojanska hästar inte kan duplicera sig själva, och därför endast skadar den dator där den har blivit installerad. (Dubrawsky, 2006). Den ursprungliga trojanska hästen finner man i Iliaden och i Virgil's Latinska episka poesi ”The Aeneid”. Där beskrivs en konflikt mellan Troja och Grekland. Det grekiska folket bygger en trähäst som några soldater gömmer sig i och ger denna sedan som en fredsgåva till trojanerna. Det visar sig dock att grekerna är ute efter att plundra Troja. Efter att trojanerna tagit in hästen i staden så lämnar de grekiska soldaterna hästen under natten och släpper in resten av den grekiska truppen till Troja(Stanford: The Trojan War; Symantec: Trojan Horse, 2010). Detta fenomen som datorhot uppträder på ett liknande sätt, det kan t.ex. vara ett till synes ofarligt program eller en fil som användaren får skickat till sig som i själva verket har en trojan inkluderad. (Pfleeger och Pfleeger, 2003)

Trojaner utför sin aktivitet i bakgrunden och likt virus försöker de undgå att upptäckas. Trojaner har ofta inte syftet att skada datorn, utan de fungerar som spionprogram. De kan t.ex. ge falska notifikationer om uppdateringar med länkar till add-ons. Detta tillvägagångssätt kallas för en ”Driveby-download”. (Symantec: Trojan Horse, 2010). Dessa pop-ups meddelar ofta användaren om att denne fått ett virus eller att datorn behöver kontrolleras. Om användaren sedan aktiverar länken så installeras troligen ett virus då istället.

Trojaner innefattar ett brett begrepp då de kan fungera på en rad olika sätt. Några av de specifikt kategoriserade är dock:

- Bakdörrs trojanen som installerar en bakdörr på den drabbade användarens dator.

- ”Downloader” trojanen som utger sig för att vara en av användaren känd fil, men som i själva verket installerar en uppdatering till en tidigare installerad

trojan eller annan skadlig kod.

- Informationsstjälande/ dataskickande trojaner stjäl information som är konfidentiell och utnyttjar ofta användarens personliga information för ett vinstdrivande syfte. Det kan även vara en typ av tangentregistreringsprogram som registrerar tangenttryckningar utförda av den som använder den infekterade datorn.

(Symantec: Trojan Horse, 2010)

- Remote access trojans (Rats) är en trojan-variant som har för avsikt att låta brottslingen ta kontroll och fjärrstyra datorn. Denna trojan finns oftast gömd i ett spel eller andra mindre program. (Microsoft: Danger: Remote Access Trojans, 2002)

2.1.3 Maskar

En datormask har många likheter med ett datorvirus. En mask använder sig också av datorer för att reproducera och sprida sig. Masken behöver dock varken infektera ett program, eller ingen eller inget som aktiverar den. Masken är självständig och letar upp och sprider sig till friska värdar i nätverket. (Pfleeger & Pfleeger, 2003) Spridningen är effektiv och tusentals datorer kan bli infekterade inom loppet av några sekunder. Masken utnyttjar ofta säkerhetshål bl.a. i operativsystemet. Chatprogram, P2P-program (Peer-2-Peer) och andra fildelnings- och kommunikationsprogram underlättar spridningen av maskar. (”Symantec: Datavirus allt svårare att upptäcka”, 2004).

Den första stora masken som, även kallas för ”the original computer worm” skapades av Robert Tappan Morris 1988. Morris hade studerat ämnet datateknik på Cornell. Han skrev koden till masken som ett experiment och exekverade den på Internet ifrån MIT. Masken använde sig utav svagheter i bl.a. sendmail. Masken tvingade flera tusen system att stängas ner helt eller bli frånkopplade ifrån Internet och orsakade en ekonomisk skada för upp emot 97 miljoner dollar (”The Robert Morris Internet Worm”, 1994, Pfleeger & Pfleeger, 2003).

En mask strävar efter att infektera så många datorer som möjligt, vilket gör maskarna mer farliga än datorvirusen då många datorer är uppkopplade mot Internet. Nuförtiden är maskarna ofta kombinerade med trojanska hästar, vilket ökar den potentiella skada de kan orsaka. (Pfleeger & Pfleeger, 2003)

2.1.4 Polymorfiska virus

Polymorfiska virus utmärker sig på grund av att de konstant förändrar sig. Detta gör det svårt för antivirusprogrammen att bekämpa dem. Gustaf berättade att ökningen av polymorfiska virus på webbaserade servrar har bidragit till att det har blivit mycket svårare för antivirusföretagen att analysera hur viruset har spridits och att spåra källan.

Moderna antivirusprogram använder sig av de signaturer som olika virus har i antivirusprogrammets databas för att söka upp dem på datorn. Problem uppstår ifall viruset har en förmåga att alternera sin signatur, vilket polymorfiska virus har. Viruset fungerar på samma sätt, men signaturen ändras och detta försvårar för antivirusprogrammen att upptäcka det. (Pfleeger & Pfleeger, 2003)

Polymorfiska virus kan även använda sig av krypterade nycklar för att dölja sig från antivirusprogrammen. De har även en inbyggd slumpgenerator som injicerar och kastar om kod i viruset, utan att ändra dess funktion. Därmed kan ett virus i praktiken kopieras flera gånger, så att det vid exekvering ser olika ut enligt signaturen, trots att det fortfarande är samma virus. (Pfleeger & Pfleeger, 2003)

2.1.5 Spionprogram

Det är vanlig förekommande att man är drabbad av spionprogram. Som namnet antyder så är det ett spionprogram. Däremot är syftet med programmet olika beroende på skapare. Ett spionprogram samlar ofta in personliga uppgifter om användaren, med eller utan dennes tillåtelse eller vetskap. (Symantec: Crimeware: Trojans & Spyware, 2010)

Fenomenet är såpass utbrett att till och med vissa spionprogram utger sig för att vara antispionprogram, detta för att även lura dem som försöker göra något åt problemet. De flesta spionprogram idag är ofarliga och inte ute efter att förstöra. Spionprogram har ofta en negativ inverkan på datorns prestanda. Risken finns att det spionprogram man drabbats av automatiskt laddar ner mer skadlig kod till datorn.

Spionprogram kan avslöja sig själv genom att skapa mycket pop-uprutor med diverse reklam (även kallat adware) eller nya ikoner på skrivbordet, som leder till hemsidor och program. Vissa förändrar sökningar ifrån tex Google och prioriterar sina egna produkter före andra, eller skickar vidare användaren till en hemsida den egentligen inte var ute efter att besöka. (Dubrawsky, 2007)

Tangentregistreringsprogram är en farligare form av spionprogram som sparar lösenord och uppgifter från sidor man brukar besöka, för att sedan skicka dessa vidare till någon med avsikt att missbruka informationen. (Symantec: “Crimeware: Trojans & Spyware”, 2010)

Den oerfarna Internetanvändaren kan lätt drabbas av spionprogram. Många gånger är det användaren själv som installerar spionprogram utan att han eller hon riktigt förstått det t.ex. genom att det medföljer en annan programvara när man laddat ner ifrån Internet. Vilseledande information som berättar att man har virus på datorn och därför behöver installera ett specifikt program är också vanligt, detta kallas Scam.

Spionprogram får ofta operera ostört då de vanligtvis inte är klassade som virushot och därmed inte hittas av antivirusprogrammen. (Dubrawsky, 2007; Symantec: ”Spyware: Vad innebär det för dig?”, 2010). Detta är för att vissa spionprogram inte är ämnade för kriminell verksamhet, utan krävs för att vissa program skall fungera.

Cookies är ett vanligt exempel skulle kunna tolkas som spionprogram. (Dubrawsky, 2007)

Likt virus sprider inte spionprogram sig själv, utan det kräver att man installerar och kör det för att det skall kunna reproducera och sprida sig.

De flesta antiviruspaket erbjuder även lösningar på problem med spionprogram. (Dubrawsky, 2007)

2.1.6 Social ingenjörskonst

Social ingenjörskonst innebär i korthet att man manipulerar en annan människa för att lura till sig information man egentligen inte skulle ha fått tillgång till. Besitter man goda sociala färdigheter är det ofta inte svårt att lura till sig information.

Den kriminella försöker ofta samla information innan för att framstå som mer trovärdig vid kontakten. Social ingenjörskonst kan tillämpas med de flesta medium som till exempel över telefon, chattar, e-post med mera (Dubrawsky, 2007; Chalmers.se: Human aspects of Computer Security, 2006)

Fördelarna med social ingenjörskonst är att det inte kräver avancerad teknik, det kan användas av alla och emot alla. (Chalmers.se: Human aspects of Computer Security, 2006)

2.2 ThreatSense.NET

Detta är ESET NOD Antivirus specialutvecklade teknik för att förhindra spridningen av virus. Verktyg möjliggör för ESETs antivirusprogram NOD32 att skicka anonyma datapaket med information om den potentiellt skadliga kod som upptäckts på datorn. ESET analyserar sedan datapaketet och ifall det visar sig vara skadlig kod, läggs det till i ESETs databas. Sedan distribueras informationen om den skadliga koden till andra NOD32 användare och gör dessa skyddade automatiskt. (ESET: ThreatSense.NET, 2010)

2.3 Attityder inför hot

Fear appeal är en känd marknadsföringsstrategi som effektivt ändrar attityder på en rad områden. *Protection motivation theory,* PMT, försöker hitta de variabler i Fear appeal som är avgörande vad gäller attityder inför faror och ställningstagandet inför skyddslösningen.

Konceptuellt är rädsla ett känslomässigt tillstånd där individen skyddar sig mot eller i ett motiverat tillstånd leder sig bort från något. Det sägs att tendensen att agera på ett särskilt sätt är kopplat till konsekvensen av agerandet och värdet av konsekvensen. (Rogers, 1975)

Modellen bestod ursprungligen av de tre variablerna (1) hur allvarlig hotet upplevs vara, (2) upplevd sannolikhet för att detta hot inträffar (3) samt hur effektivt den föreslagna lösning är (Rogers, 1975). Vid senare revidering utökades modellen med (4) hur effektiv individen själv upplever sin förmåga att vara för att tillämpa lösningen (Rogers & Maddux, 1983). Hur individen agerar kan bero på någon av variablerna, ensamma eller i kombination, vilket resulterar i att det kan finnas en rad olika anledningar till vald handling (Rogers, 1975). *PMT* lämpar sig för fall där de fyra variablerna är närvarande.

Dessa variabler påverkar kognitiva processer som tillsammans påverkar attityder genom att väcka en känsla av motivering till att skydda sig. Hur väl man adopterar lösningen på faran är sammankopplat med hur skyddsmotiverad individen är. Om individen inte uppfattar en händelse som allvarlig, trolig eller om denne inte kan göra något åt det, så skulle ingen motivation skapas och därmed inte heller någon beteendeförändring ske. Att man befinner sig i ett känslomässigt tillstånd av rädsla resulterar inte i attitydförändring, utan det beror på mängden skyddsmotivation (Rogers, 1975).

”Self efficacy”, den fjärde variabeln, hur individen upplever sin egen förmåga att genomföra önskvärt beteende är en stark indikator på huruvida denne kommer agera. Den uppfattade förmågan kan även påverka uppfattad effekt av variablerna angående sannolikheten att faran inträffar och effektiviteten på lösningen. (Rogers & Maddux, 1983)

I de fall där de andra tre variablerna ansetts milda men den egna förmågan hög, så brukar personen resonera att det är bäst att inte chansa och genomför lösningen i ren försiktighetsåtgärd. Om hotet anses vara högt och sannolikheten stor samtidigt som man anser att ens förmåga är stor så tenderar man att anamma lösningen vare sig den är effektiv eller inte. Även när förmågan ansågs låg men lösningen mycket effektiv på att undvika faran så anammade man lösningen. (Rogers & Maddux, 1983)

De som upplever att faran är jättestor är generellt lättare att övertala att följa rekommendationer medan om läget anses riktigt desperat kan man börja resonera att det ändå inte går att undvika. (Rogers & Maddux, 1983)

Att informera om att öka sin egen förmåga är mest effektiv på dem som tror faran är liten och att kopplingen mellan deras beteende och resultatet av beteendet är svag. Det är svårare med dem som tror kopplingen är stark mellan deras beteende och resultatet. Tror man inte att man har förmågan så kan man tro att resultatet inte blir som det som önskas. (Rogers & Maddux, 1983)

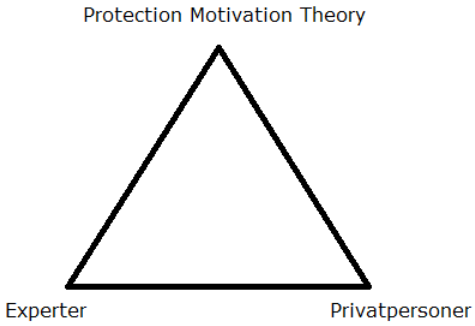
3. Metod

Vi använder oss av vad Jacobsen (2002) kallar en deduktiv ansats vilken han beskriver som att forskarna ger sin bild av verkligheten. Respondenterna får sedan tolka forskarens beskrivning på sitt sätt. Forskaren får sedan göra en ytterligare tolkning av resultatet. Forskaren kommer då till en slutsats som är mer eller mindre generell. Hur generell resultatet kan anses vara har med antal respondenter att göra (Jacobsen, 2002). Jacobsen (2002) berättar också om en alternativ metod som han kallar för den induktiva metoden. Den beskrivs som att forskaren inte ska ha någon egen inverkan på hur resultaten blir.

Den deduktiva ansatsen låter oss bestämma riktningen vi önskar på undersökningen. Då vi valt att undersöka situationer som är relaterat till vilka typer av problem som privatanvändare kan stöta på under internetanvändning så krävs det att vi sätter vår prägel på undersökningen.

När vi beskriver vårt resultat använder vi oss av en modell vi själva skapat bestående av en triangel med våra tre aspekter; Experter, PMT och Privatpersoner. Vi jämför experternas syn på skadlig kod med privatpersonernas bild för att sedan utröna vilka skillnader och likheter vi finner. Vi tar och analyserar detta med hjälp av Rogers & Madduz's (1983) PMT. Vi valde att skapa en triangel för att enklare förklara hur vi skall gå tillväga.

Figur 2: Jämförelsetriangeln



(Författarna, 2010)

3.1 Metodval

För att kunna jämföra vad som anses av både experter och användarna, så valde vi att skicka ut kvalitativa intervjufrågor till experter. Dessa arbetar inom antivirusbranschen. Till privatpersoner skickar vi istället kvantitativa undersökningsblanketter. Vårt enkätunderlag distribuerar vi ut elektroniskt som en bekvämlighetsundersökning. Vi riktar oss mot de som är innehavare av Internetuppkoppling och som är aktiva datoranvändare. Således riktar vi oss till våra kunder direkt genom vår valda distributionskanal.

Vi har vår syn på hur det egentligen ser ut och hur vi uppfattar att det ligger till, dels genom att ha läst liknande undersökningar och dels genom vår egen kompetens och realitetsuppfattning. Därigenom har vi utformat frågorna och svarsalternativen till undersökningsmaterialet. Dessutom har vi fått en del inspiration och tankar angående vad som kan vara relevant att fråga experterna. Detta ska få oss att förstå deras syn på hur det ligger till med privatanvändarnas kompetens och kunskap. Därigenom kommer vi få en bättre bild över hur långt ifrån användarna ligger i jämförelse med experterna. Vi ska se om den rekommenderade nivån avseende åtgärder och agerande mot olika typer av hot och risker stämmer överens.

3.1.1 Enkätundersökning

Hos den enskilda Internetanvändaren ligger ofta hotet i att inte använda en tillräcklig försiktighetsgrund och att inte ha tillräcklig kunskap för eventuella hot och risker som kan uppkomma med ett oförsiktigt agerande. Vi utförde därför en enkätundersökning med hjälp av Google ”Spreadsheet”, som har en funktion för att tillverka digitala enkäter. Vi distribuerade ut dessa inom den närmsta vänkretsen för att forska om ifall hot och risker skulle kunna övervinnas med hjälp utav utökad kunskap för användaren. Utöver att visa på hur säkerhetsmedveten den enskilda privatpersonen är vill vi också ha mer specifik information om hur de reagerar och vad de anser vara ett risktagande. Eller tvärtom, vad som ses som ett alltför litet hot för att man ska ta med det i beräkningarna vid aktiv Internetanvändning.

3.1.2 Expertintervju

Ett underlag för en kvalitativ intervju för att få en bild över hur experter uppfattar situationen för privatpersoner och deras användning av Internetrelaterade tjänster lades fram. Detta gav oss en bild över vad de uppfattar är en acceptabel nivå att ligga på. Detta gäller privatpersoner och deras säkerhetsrutiner i dagens alltmer hotfulla datormiljö, vilken kan bekräftas av våra expertundersökningar. Detta gäller framför allt då våra datorer ingår i allt större nätverk som hotas om skadlig kod eller felaktig programvara tar sig in på nätverket.

3.1.3 Urval

Vad gäller urvalet av experter, valde vi att rikta oss till de som har hand om olika analysprogram och antivirusprogram som vi vet används av privatpersoner.

Då vi vänder oss till privatpersoner som använder sig av Internet och dess tjänster är det över den kanal vi valt att distribuera våra frågor, både för experter och för privatpersoner. En Internetbaserad enkät kan också leda till att den tas mer seriös, då respondenterna har obegränsad tid att besvara frågorna. Det är också på internet man är utsatt för den största risken att drabbas. Vi har gjort ett urval i vår vänskapskrets och bekanta. Efter en närmare analysering kom vi fram till att vår enkätundersökning mest liknar ett så kallat bekvämlighetsurval, efter Jacobsen (2002). Detta innebär ofta en otillräcklig undersökning, då de som utesluts också kan

ha relevanta synpunkter. Men i detta fall när vi riktar oss till användare som befinner sig på Internet så finner vi populationen direkt.

3.1.4 Datainsamling

Vi samlade in data från 63 personer som medverkade i vår enkätundersökning och utefter analys och kontroll räkna bortfall och övriga icke giltiga svar. Detta för att kunna validera undersökningen under enkätanalysen. Vi tar också reda på hur nöjda privatpersoner generellt är med alternativen för att förhindra hot och risker. För att experterna ska fokusera så strikt som möjligt på vår forskningsfråga och hålla sig ifrån t.ex. företagsrelaterade hot och risker har vi lagt in en beskrivning i början av intervjuunderlaget. Där beskrivs vår definition av ”skadlig kod” för att inte experterna ska gå djupare in på ämnet och t.ex. börja diskutera hur det ser ut på företag.

Intervjuerna med experterna sker parallellt. För att detta ska vara möjligt och samtidigt för att det skulle vara svårt att ordna fysiska möten, så har vi sänt ut underlag som alla ser likadana ut till företagens respektive e-post. Kontaktpersonerna har sedan skickat vidare dessa till en expert för att vi ska få så trovärdighetsinvigande och korrekta svar som möjligt.

3.2 Etiska aspekter

För att analysera huruvida vårt tillvägagångssätt under denna undersökning är etiskt korrekt, har vi utgått från ”informerat samtycke” som innehåller fyra huvudpunkter; *Kompetens*; *Frivillighet*; *Full information* och *Förståelse*. Dessa aspekter/krav ska gå att finna hos respondenterna. (Jacobsen, 2002)

Kompetensnivån hos våra undersökta är fullgod då de annars inte skulle kunna ta del av en digitalt distribuerad undersökningsblankett. Vi har dessutom begränsat oss till personer med en minimiålder av 18 år. Frivillighet är ett uttryck som betyder att man inte ska behöva känna press eller påtryckningar från andra under deltagandet. Meningen har varit att gå ut med tydlig information om att det är valfritt att delta, vilket vi har tagit tag i på ett aktivt sätt.

I informationen om/på blanketterna har vi informerat att vi endast syftar till att undersöka hur verkligheten förhåller sig till teorin. Vi riktar oss till privatpersoner och dess vanor och kunskap för Internetanvändning och vilka risker och hot de riskerar att råka ut för. För att experterna respektive privatpersonerna fullt ska förstå vår undersökning och dess syfte har vi informerat på ett sätt som är enkelt att förstå.

3.3 Studiens validitet och reliabilitet

Vår uppfattning ligger till grund för undersökningen och därmed kan vi ha en påverkan hur resultatet och analyseringen går till och vad slutsatsen blir. En annan bidragande faktor är vår målgrupp. Den är inte så utspridd som man skulle kunna

önska, men mycket beror på tidsfaktorn. Arbetsbördan skulle bli övermäktig om vi skulle göra ett helt korrekt slumpmässigt urval för vår enkätundersökning. Experterna i sin tur har vi full respekt för då de är en bidragande orsak till att Sverige ändå ligger så pass bra till när det gäller säkerhetsmedvetenhet hos privatpersoner. Vi har i vår undersökning fått ca 49% av våra enkätutskick besvarade. Jacobsen (2002) diskuterar att om ca 50% av ens enkäter är besvarade när man utför en kvantitativ bekvämlighetsundersökning har man ett bra resultat. Vidare diskuterar Jacobsen (2002) att det är vanligt att man får mellan 5%-50%, så vår underökning är bra i det avseendet.

4. Resultat

4.1 Säkerhetsexperterna

Vi intervjuade två experter från två av de ledande utvecklarna av antivirus och skyddsmjukvara. Den första experten, Gustaf, är teknisk chef och den andra som vi kallar Fredrik har en teknisk roll.

Vilken typ av skadlig kod är den dominerande för tillfället och vilka typer tror Ni kommer vara dominerande om 5 år? (t.ex. virus, trojansk häst, malware)

Företaget som Gustaf arbetar på använder sig av ThreatSense.NET (se avsnitt 2.2) för att analysera hot av skadlig kod. Olika varianter av Conficker-masken är bland de vanligaste hoten i deras system. Annars något som privatpersoner ofta drabbas av är falska antivirusprogram, så kallade ”rogue security software”. De närmaste åren tros det komma mer personinriktade attacker. Dessa attacker kan vara av graden att de är personligt riktade med specialskriven kod eller att de sprids runt med hjälp av social ingenjörskonst för att lura till sig personer att installera den skadliga koden. Fredrik påpekar specifikt att mobilrelaterade hot kommer att öka, (vilket bara är en del av teknikens utveckling) och att webbaserade hot har klart störst del av marknaden.

Tror Ni mängden skadlig kod kommer öka eller minska? På vilka områden? Varför?

Svaret var att den troligen kommer att öka och att det kommer bli mer riktade attacker gentemot företag och större organisationer. Detta ger de kriminella större vinster då det kommer att vara svårare att stoppa denna typ av attacker. Fredrik verkade mer framåt och att den skadliga koden kommer öka var för honom en självklarhet.

Ser Ni några trender i vilka kanaler på Internet som spridningen av den skadliga koden sker? Finns det andra vägar än Internet?

En vanlig variant är att koda för att brottet ske vid anslutning av en extern enhet, som t.ex. när man stoppar in en USB-sticka i datorn. Det finns många hot som använder sig av flera olika sätt att sprida sig, vilket gör klassificeringen till ett dilemma. Som exempel kan nämnas att ett hot kan sprida sig som en mask, installera en bakdörr och gömma sig som ett rootkit. Användande av sökoptimeringsverktyg är en variant som ökar. Nyheter som läckt ut har tagits i behandling av kriminella som skapar skadlig kod vid aktivering av länkar. Datorer som är infekterade och hemsidor som är hackade används för detta ändamål. Fredrik var också inne på att webbattacker kommer att dominera. Gustaf gav ett exempel: Då t.ex. kändisar går bort kan man ofta finna länkar bland de första resultaten i sökmotorerna som innehåller någon form av skadlig kod. Själva installationen av den skadliga koden kan ske på väldigt skilda sätt, ofta sker det genom att utnyttja säkerhetshål i olika operativsystem eller webbläsare eller att användaren blir lurad att installera en viktig

uppdatering till t.ex. Flash eller något antivirusprogram.

Är dagens kod mer avancerad än den som funnits förut? Är den svårare att upptäcka och kan den orsaka större skada?

Spridning har ökat markant då det är många fler enheter dags dato som är uppkopplade mot Internet och som är kopplade till varandra. På det tekniska planet har det skett en nedgång hur pass avancerad koden är, men det är på uppgång nu igen. Så tidigt som på 90-talet har det varit avancerad kod som spridits som bl.a. skapat polymorfism och som försöker att dölja sig själv. Nu är datorer istället ofta uppkopplade och mindre avancerad kod krävs för att spridningen ska vara stor. Fredrik var inne på samma sak och berättade att dagens kod gör större skada, men att den samtidigt inte är lika farlig i sig. När man förr oftare spred koden genom disketter eller manuellt kopierade filer, så är det i dagsläget möjligt att sprida koder på några rader till miljontals användare världen över. Mer avancerad kod är på ingång, som rootkits och patchade system, där det kan vara nästan omöjligt att upptäcka ifall man inte startar datorn i en säker miljö. Till exempel kan man starta från en CD-skiva och därigenom göra en genomsökning. Koder som blir allt svårare att stoppa är de som utnyttjar sig av server-baserad polymorfism, vilka är i uppgång och gör att spridningen blir svår att analysera och att källan är svårare att spåra.

Vad kan Ni göra för att motarbeta social ingenjörskonst? Vad tror Ni om utvecklingen av detta fenomen? Har Ni någon bra lösning?

Utbildning och ökad medvetenhet tyckte både Gustaf och Fredrik är det effektivaste sätt för att inte bli drabbad av detta. Program kan vara skadliga och man ska inte lita på alla. Pengar finns i att användaren kör ett infekterat program eller att användaren litar på fel person. Ett vanligt fenomen är att användaren har övertro på sin egen säkerhet och att man tror att man är säker när man har ett antivirusprogram och sitter på t.ex. en arbetsdator som är säkerhetslåst. En ökning kommer troligen att ske av riktade attacker mot specifika mål som backas upp av social ingenjörskonst, då detta ger tillgång till mer pengar/information på kort tid och att det är svårare att bli upptäckt som brottsling. Detta kommer att vara mer effektivt till skillnad från att sprida koden och ta liten del information från flera olika håll. Vårt bidrag är bland annat utbildning, vi lägger upp en podcast varje vecka som går igenom de aktuella hoten och riskerna, samt informerar om hur man effektivt skyddar sig. Fredrik gav som exempel att ett skräppostskydd kan vara bra att ha.

Hur sker er analys av nya hot mot privatanvändaren?

Fredrik skriver bara att analysen sker automatiskt medan Gustaf berättar mer ingående; Analysen av nya hot sker mestadels automatiskt med ThreatSense.NET motorn, som gör att de får tillgång till anonym statistik och till nya hot från ny skadlig kod. Sedan används proaktiva metoder som kodanalyser för att kunna känna igen den skadliga koden. Om nya typer av en känd skadlig kod upptäcks av en användare, så får de in en kopia av filen och kan börja spåra hur spridningen kommer te sig och eventuellt se var koden har genererats. Virussignaturer och kodanalyser kan då också

uppdateras efter olika typer av den skadliga koden. Då varianter av skadliga koder har ökat markant och det är svårt att analysera varje fil för sig, så försöker man istället se trender och analysera spridningen och spåra källan. Klassificering sker ofta automatiskt genom olika system och under specifika analyser så sker endast en enklare signering. Buggning för större och farligare hot sker under en längre tid och mer ingående.

Hur stor bedömer Ni risken är att drabbas av skadlig kod vid vanlig Internetanvändning utan skydd? Tror Ni det är någon stor skillnad på nybörjaren och den mer datorvane?

Hur stor risken är att drabbas av skadlig kod om man inte har skydd vid vanlig Internetanvändning rådde lite delad mening om. Fredrik menade att risken alltid är stor för att drabbas vare sig man är van med datorer eller nybörjare. Fredrik underströk dock att det är klart större risk för nybörjaren. Gustaf tyckte det var svårt att uppskatta risken och att det mer berodde på hur Internetanvändningen såg ut. Risken var mindre ifall man besökte vanliga, ”kända”, sidor än om man har en tendens att klicka på roliga länkar eller håller på med fildelning. Fredrik anade att det är svårare att lura en datorvan användare att installera något program för att se en rolig film.

Vad anser Ni är ett minimikrav vad gäller skydd mot skadlig kod? Vidare vad anser Ni skulle vara en rekommenderad nivå?

Både enligt Gustaf och Fredrik var det viktigt att hålla alla program från operativsystemet till tredjepartsprogrammen såväl som antivirusprogrammet uppdaterade. Om man kontinuerligt uppdaterar alla program så täpper man till de hålen som exploateras. Fredrik tillade också att man bör ha någon form av brandvägg som minimum. Till rekommenderad nivå tillade Gustaf att man bör ha för vana att inte vara inloggade som administratörer i operativsystemet och att man vänjer av sig att installera/ klicka på allt det som visas på Internet. Gustaf menade att det är rätt vanligt idag att man gör en sida som seriös ut som ber att användaren installerar ett program, som sedan visar sig vara skadligt. Fredrik menade att det var rekommenderat att även ha någon form av backup-lösning.

Hur säker är man ifall man har skydd av den rekommenderade nivån men inte besitter kunskap om hur man använder Internet på ett säkert sätt?

Om man nu som användare väljer att implementera den av experterna rekommenderade nivån så är man relativt säker enligt samtliga intervjuade experter. Gustaf underströk ändå att det beror till stor del hur man använder Internet. Enligt Gustaf är man rätt säker med denna säkerhetsnivå ifall man endast surfar på kända och vanliga sidor som till exempel Aftonbladet eller Youtube. Skulle man dock istället surfa på många ”okända” sidor och använda fildelningsverktyg så var man inte särskilt säker med den rekommenderade nivån.

Hur anser Ni svenskar ligger till i jämförelse med andra länder i försiktighetsåtgärder och nivå av aktivt skyddande?

Sverige ligger bra till i jämförelse med andra länder i säkerhetstänk enligt experterna. Gustaf sade att det är ett vanligt problem i andra länder att användarna kör med gamla operativsystem som de slarvar med att uppdatera. Svenska användare däremot använder sig i större utsträckning av nyare operativsystem och något säkerhetsprogram. Gustaf trodde att detta kunde bero på kulturella och ekonomiska faktorer.

Hur medvetna om riskerna med Internetanvändning och att drabbas av skadlig kod tror Ni privatpersoner generellt är?

Experterna trodde att svenskar överlag har ganska god kunskap om en del av riskerna med Internetanvändning. Gustaf peka på att många användare tycker de är säkra så länge de inte surfar på hemsidor som ser tvivelaktiga ut, eller har tvivelaktigt innehåll. Gustaf påpekade att många inte tänker på att det ligger mycket stora intressen och pengar bakom dagens skadliga kod. Kriminella har ibland anställda som bara jobbar med att sprida koden och i vissa fall har de kriminella stora hemsidor som ser seriösa ut och har annonsplatser på andra seriösa sidor som till exempel Google. Användare har också svårt att förstå till vilken utsträckning de kriminella kan jobba för att få en dator infekterad. Gustaf menade också att vissa har attityden att de ändå inte har något hemligt och ifall deras dator blir infekterad, så är det bara att installera om och därmed behövs inte skyddslösningar.

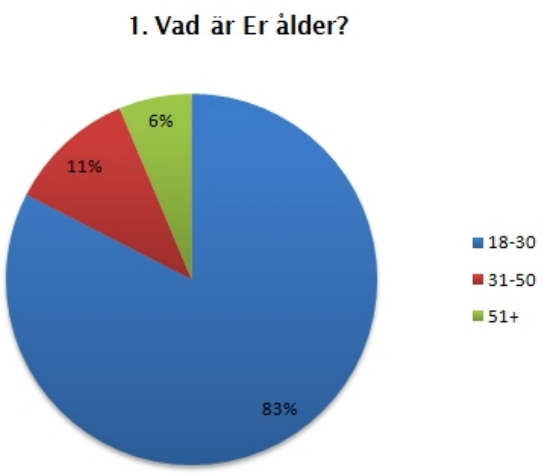
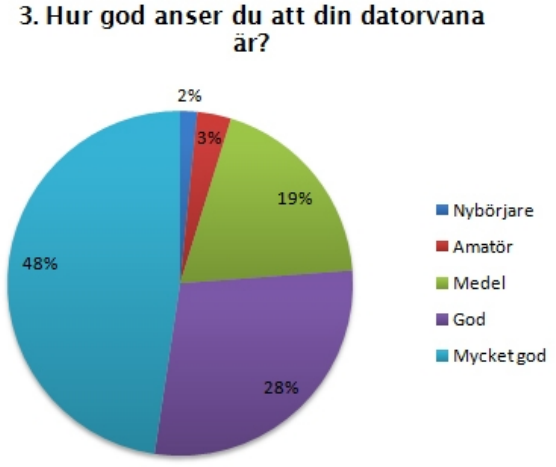
Vad anser Ni är ett effektivt sätt att bättra privatpersoners säkerhetsbeteende?

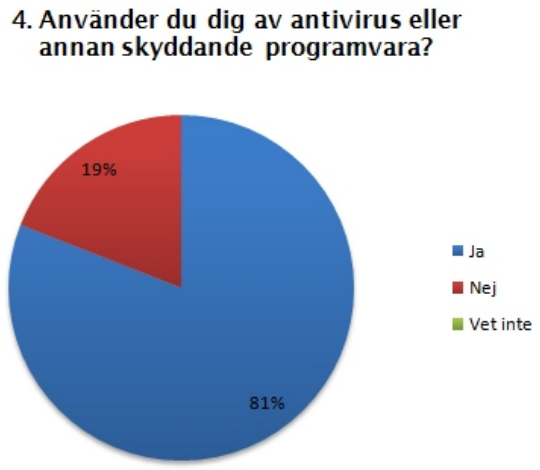
Enligt experterna är utbildning om hoten och säker Internetanvändning det effektivaste sättet att förbättra privatpersoners säkerhetsbeteende på Internet. Gustaf påpekade att det inte räcker hela vägen att bara hålla allt uppdaterat och använda ett antivirus utan att medvetenhet och utbildning även är en viktig del. Gustaf betonar dock att det är svårt att öka medvetenheten. Det är många apparater idag som är uppkopplade och utsatta för fara och ofta är det användarens egna agerande som orsakar problemen och att man installerar skadlig kod. Gustaf menade att social ingenjörskonst fortfarande är svårt att undvika, även trots ökad medvetenhet.

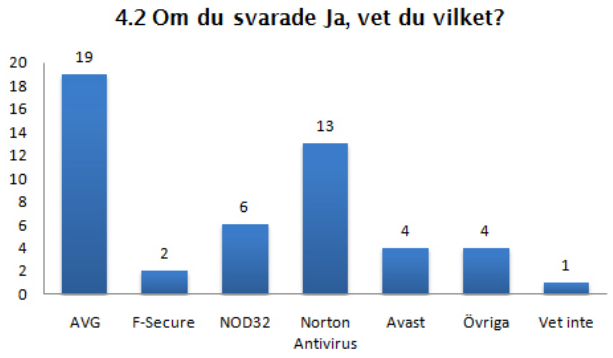
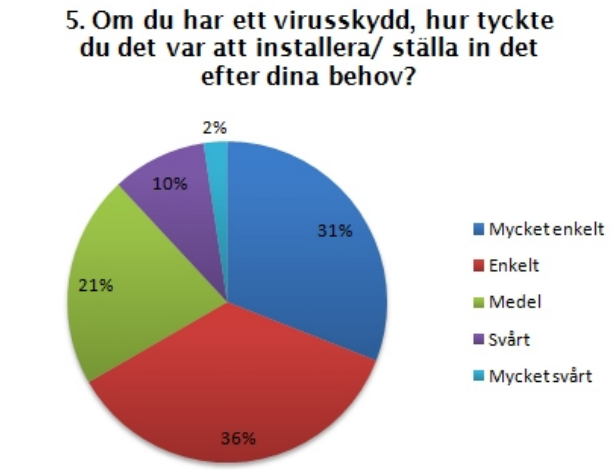
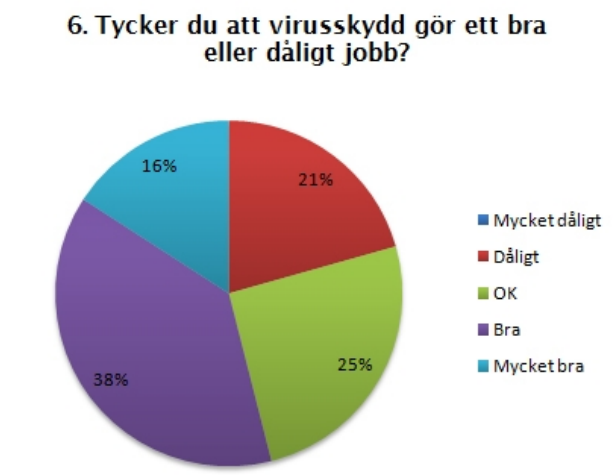
4.2 De Internetanvändande privatpersonerna

Av de 130 enkäter vi skickade ut fick vi svar från 63 (ca 49%). Som nämnt tidigare i metoden, är detta vad man som mest brukar kunna förvänta sig med ett bekvämlighetsurval.

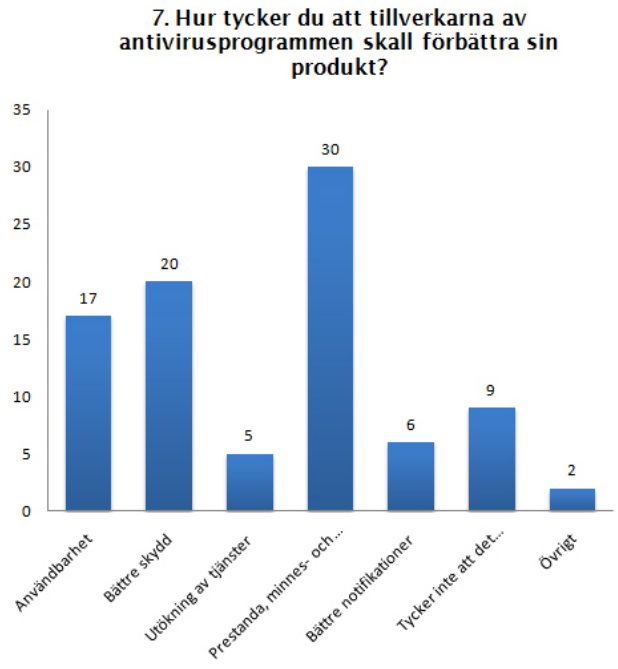
Tabell 1: Användarnas enkätresultat

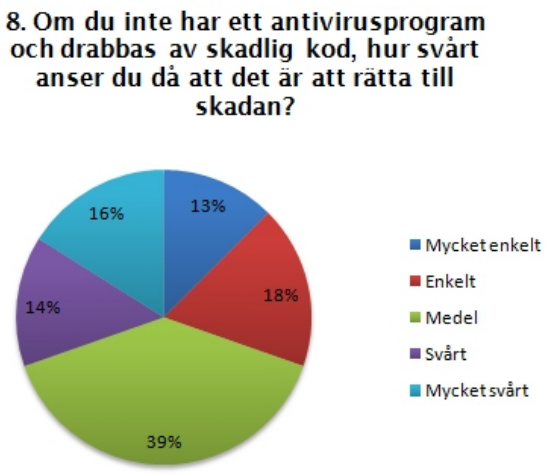
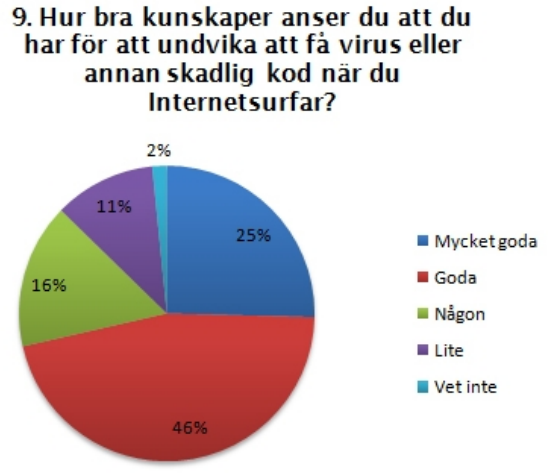
	Våra respondenter var åldermässigt ganska jämlika då 52, alltså mer än fyra femtedelar, tillhörde åldersgruppen 18-30. Det är dock inte konstigt då vi själva spred enkäten till personer vi känner först och främst. Dock var det 7 respondenter i åldrarna 31 till 50 och 4 stycken i åldrarna 51+ som svarade på enkäten.
	Av de som svarade på vår enkät så var det 45 personer som antigen läst något eller läser på universitetet. Med sina sju tiondelar utgjorde dessa den största gruppen av respondenter. Bara en enda respondent hade grundskola som högsta avslutade utbildning medan 17 stycken går på eller har avslutat en gymnasieutbildning.
	Till att döma av resultatet av enkäten så hade nästan hälften, 30 st, av våra respondenter mycket god datorvana. Ungefär en tredjedel, 18 st, ansåg de hade god datorvana och 12 tyckte de hade medelgod datorvana. Endast en mindre del av våra respondenter ansåg de var amatörer eller nybörjare, 2 respektive 1.

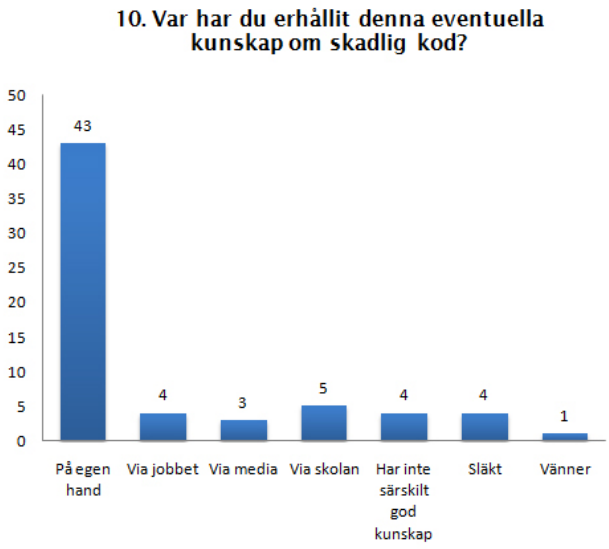
	Enligt resultatet på enkätundersökningen var det ingen som var osäker huruvida de hade ett antivirus eller annan skyddande programvara. 51, alltså lite mer än åtta av tio använde sig av någon form av skyddande programvara. Dock var det 12 som valde att inte använda sig av ett antivirus eller annan skyddande programvara.
4.1 Om du svarade nej, varför?	Det var bara tolv stycken som svarade nej på ifall de använde sig utav något antivirusprogram eller annan skyddande programvara och de flesta använde sig utav samma argument, så man kan dela upp användarna i två olika grupper. Den ena gruppen är de respondenter som totalt förlitar sig på sina MAC-datorer med tillhörande operativsystem (MAC OS X). Den andra gruppen tycker att antivirusprogram är onödiga eftersom de stjäl alldeles för mycket prestanda från datorn. Respondenterna anser att de vet vad de sysslar med och på så sätt inte får virus, men om de hade fått det så får de ta det den dagen. Värt att notera är att trots att de inte använder sig utav antivirusskydd så gör de flesta respondenter genomsökningar efter spyware lite då och då med diverse antispionprogram och nästan alla använde sig utav något fysiskt skydd, t.ex. en brandvägg. Undersökningen tog även fram att någon använde sig utav ett gammalt antivirusprogram som inte var uppdaterat på grund av att prenumerationen hade gått ut.

	AVG var det absolut vanligaste skyddsprogrammet som våra respondenter använde sig av, med sina 19 användare. Norton hade 13 användare, NOD32 6 st och Avast 4 st. Vidare var det 2 som använde sig av F-secure och resterande, som vi kallar övrigt, var program som endast hade en användare bland våra respondenter. En av våra respondenter visste inte vem tillverkaren var av dennes skyddsprogramvara.
	52 av respondenterna valde att svara på denna fråga, och 23 st tyckte att det var mycket enkelt att installera och ställa in programmen efter deras behov. Lite mer än en tredjedel, 15 st, att det var enkelt. Vidare tyckte 9 att det var medelsvårt medan 4 tyckte det var svårt. En av våra respondenter tyckte det var mycket svårt.
	Betyget som våra respondenter gav på hur bra jobb virusskydden gör var ganska gott. 24 tyckte att virusskydden gjorde ett mycket bra jobb, 10, ca två femtedelar tyckte att programmen gör ett bra jobb. Vidare tyckte 16 st att de gjorde ett OK jobb och 13 tyckte de gjorde ett dåligt jobb. Det var dock ingen av våra respondenter som tyckte att skyddsprogrammen gjorde ett mycket dåligt jobb.
6.1 Motivering på fråga 6	De mest generella erfarenheterna man kan se i undersökningen är att många klagar på att antivirusprogrammet tar mycket prestanda från datorn och därmed segar ner den under tiden som antivirusprogrammet körs, även om det bara sker i bakgrunden.

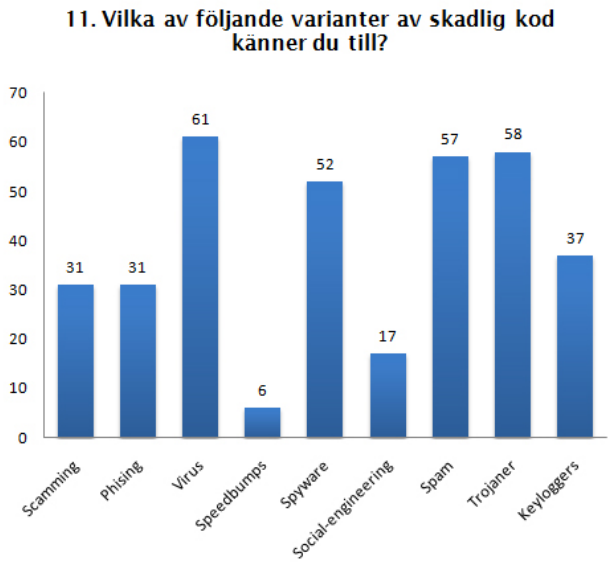
	Sedan har vi den motsatta bilden där man berättar att antivirusprogrammet inte märks överhuvudtaget och där användaren uppfattar att programmet sköter sitt jobb automatiskt och korrekt och därför är nöjda med det. En del av respondenterna uppfattade sitt virusprogram som krångligt och svårt att hantera. En del verkade vara lite irriterade över att antivirusprogrammet felanalyserar vissa filer som användaren vill installera och därför visar en varningsruta. En respondent skrev: *" tog […] bort mitt 'sub seven' [som är ett Remote Administration Tool program] gång på gång, även när jag hade packat ner det i en rar-fil. envist program..."* Man finner att någon anser sig säker för att de inte använder Windows eller att de inte surfar på "skumma" sidor på Internet. Det var dock en del som skrev att antivirusprogram aldrig skyddar en till 100 procent eller att man inte skulle utesluta att det kan finnas ytterligare hot, som antivirusprogrammen inte skyddar mot.

	Nästan alla respondenter hade någon synpunkt på hur skyddsprogrammen kan förbättras. Det vanligaste som respondenterna önskade sig var bättre prestanda och processor-, minneskraftshantering. 20 respondenter önskade förbättrad skydd, medan 17 ville ha bättre användbarhet. 9 av våra respondenter var dock helnöjda och tyckte inte att det behövdes några förbättringar.
7.1 Motivering på fråga 7	Många av respondenterna tyckte att antivirusprogrammet segade ner datorn för mycket vilket är ett stort problem och en anledning till varför vissa inte vill använda sig utav just sådana här produkter. Några av respondenterna tyckte att antivirusföretagen bör samarbeta mer med de företagen som tillverkar fysiska skydd så som brandväggar eftersom då lyckas man få bort ”prestandaboven” från datorn och lägger detta på en fysisk produkt så inte datorns prestanda påverkas så mycket, utan allt sköts via den fysiska enheten. Några av respondenterna påpekade att notifikationerna bör simplifieras så de även kan förstås av personer som inte är vana med datorer. Vidare tyckte de att antivirusprogrammet skall finnas där i bakgrunden och skydda en mot virus utan att användaren får upp en massa notifikationer. Användbarheten är olika bra i olika program enligt undersökningen och de

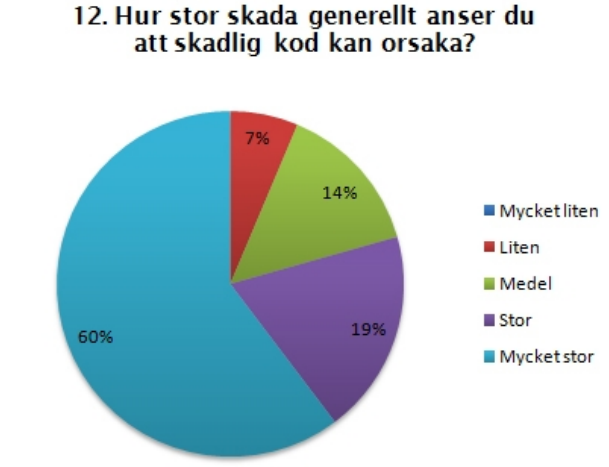
	respondenter som nämnde detta tryckte på att antivirusföretagen inte borde göra det så krångligt för att få det att fungera korrekt. Vill man sen göra extra inställningar så skall detta givetvis vara möjligt men en oerfaren användare ska inte behöva gå igenom en massa inställningar den inte vet något om för att få det att fungera.
	56 av respondenterna valde att svara på frågan och enligt svaren så bedömde 6 st att det var mycket enkelt att rätta till skadan efter man drabbats av skadlig kod även ifall de inte har ett antivirusprogram. Vidare ansåg 9 att det var enkelt, 20 tyckte det var medelsvårt,6 tyckte det var svårt medan 4 bedömde det som mycket svårt.
	En fjärdedel av våra respondenter (16 st) ansåg de besatt mycket goda kunskaper om hur man kan undvika att drabbas av skadlig kod när de surfar på Internet. 29 ansåg de hade goda kunskaper, 10 tyckte de hade någon kunskap medan 7 ansåg att de endast hade lite kunskap. Endast en av våra respondenter hade ingen kunskap om hur man kan undvika skadlig kod när man använder Internet.



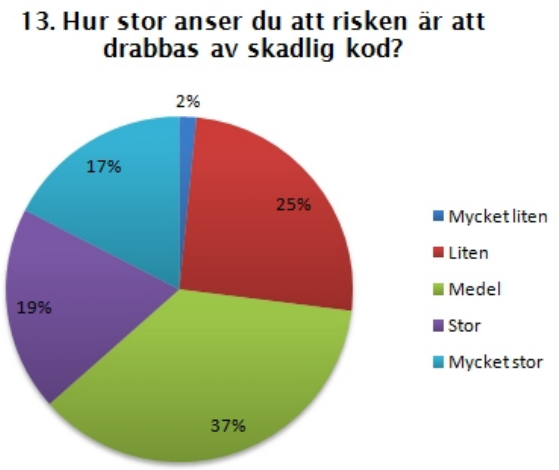
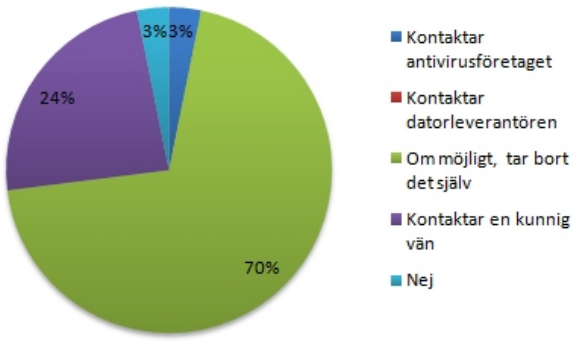
Det vanligaste sättet som respondenterna i undersökningen erhållit sin kunskap om skadlig kod var på egen hand. Med 43 personer så var det mer än de andra sätten tillsammans. 4 stycken hade fått informationen via jobbet, 3 via media, 5 via skolan, 4 via släkten och 1 via vänner. 4 av respondenterna hade inte särskilt god kunskap.



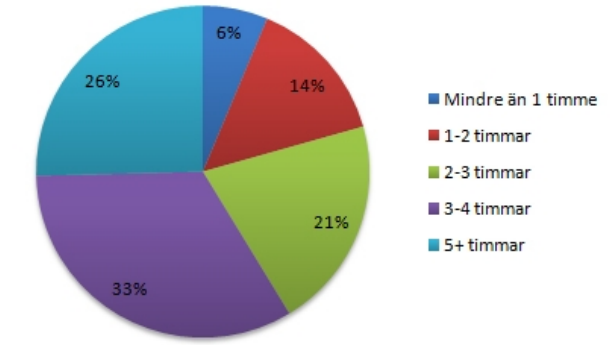
De flesta av respondenterna kände till virus, spyware, spam och trojaner. Ungefär hälften så många av dem kände till scamming, phising och keyloggers. En tredjedel av respondenterna kände till social-engineering och 6 stycken tyckte sig även känna till det påhittade ”speedbumps”.



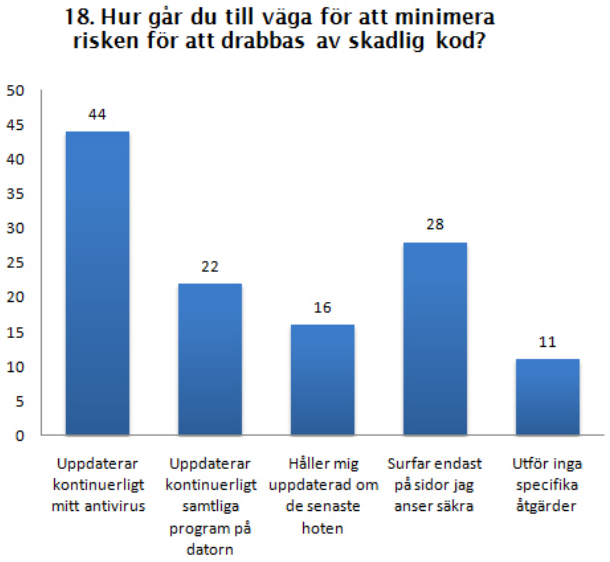
De flesta av våra respondenter, 38 st, ansåg att skadlig kod kan ställa till med mycket stor skada om man drabbas. 12 ansåg att skadan skulle bli stor medan 9 ansåg det skulle ställa till medelstor skada. Ingen respondent ansåg att skadan skulle vara mycket liten men 4 ansåg skadan skulle bli liten.

	Endast en av våra respondenter ansåg att risken för att drabbas av skadlig kod var mycket liten. 16 st, alltså styvt en fjärdedel av våra respondenter bedömde risken som liten medan lite fler, 23 st, bedömde risken som medelstor. Vidare ansåg 12 att risken var stor och 11 bedömde risken att drabbas av skadlig kod som mycket stor.
	De flesta av respondenterna (44 st) försökte först och främst att ta bort den skadliga koden själv. Näst vanligast var det att man kontaktar en kunnig vän (15 st). 2 st visste inte hur de skulle gå till väga ifall de drabbades och lika många skulle kontakta antivirusföretaget.
	Majoriteten av våra respondenter, 39 st, resonerade inte att det bara händer andra vid frågor angående IT-säkerhet. 16 st svarade att det faktiskt händer att de tänker så och 8 var lite osäkra.

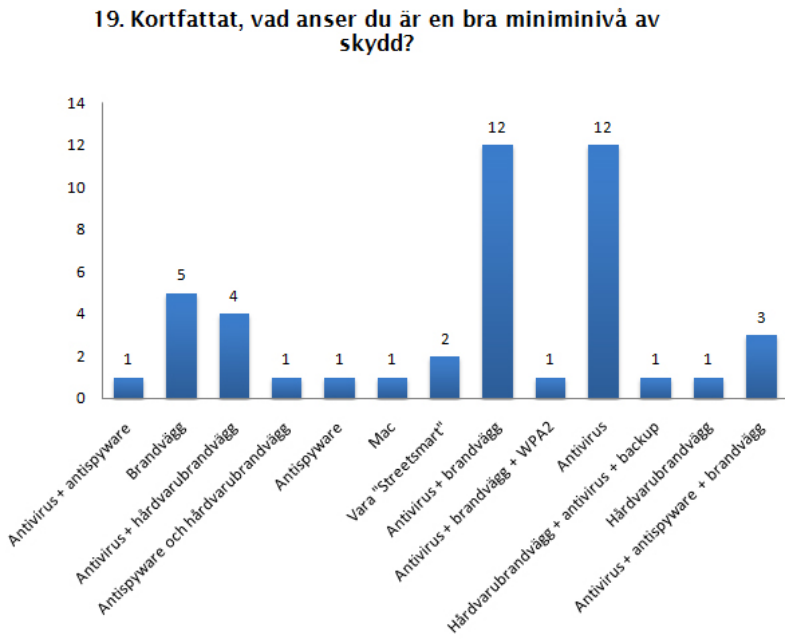
58 av respondenterna var uppkopplade när datorn var igång medan 5 begränsade uppkopplingen till då de skulle använda en tjänst som krävde Internet.



Ungefär en fjärdedel (16 st) av respondenterna använde sin dator mer än 5 timmar varje dag medan de flesta, 21 st, använde datorn 3 till 4 timmar varje dag. 13 stycken använde datorn 2-3 timmar, 9 stycken använde den 1-2 timmar medan 4 stycken av respondenterna använde sin dator mindre än en timme i snitt per dag.



44 av respondenterna uppdaterade antiviruset kontinuerligt. 28 begränsade sin surfning till sidor som de ansåg säkra. 22 uppdaterade kontinuerligt samtliga program på datorn och 16 höll sig uppdaterade om de senaste hoten. 11 av respondenterna utförde inga specifika åtgärder för att minimera risken för att drabbas av skadlig kod.



På denna fråga där respondenterna kort fick beskriva vad de anser är en bra miniminivå av skydd ledde till ett ganska varierande resultat. 45 av respondenterna valde att svara på denna fråga.

19.1 Hur svårt tycker du att det är att installera och underhålla denna nivå?	Eftersom resultaten på vad respondenterna tyckte var en bra miniminivå av skydd skiljde sig så grupperade vi alternativen med tillhörande vald svårighetsgrad och tog sedan fram medelvärdet. Antivirus fick ett svårighetsvärde på 1,75, alltså mycket nära enkelt. Alternativen ”antivirus + antispyware”, ”antivirus + hårdvarubrandvägg”, ”Mac” och ”hårdvarubrandvägg + antivirus + backup” bedömdes alla vara mycket enkla att installera och underhålla av respondenterna. Vidare bedömdes ”antispyware + hårdvarubrandvägg”, ”antispyware”, ”vara streetsmart”, ”antivirus + brandvägg”, ”antivirus + brandvägg + WPA2”, ”hårdvarubrandvägg” och ”antivirus + antispyware + brandvägg” till att vara enkelt att installera och underhålla enligt de respondenter som ansåg dessa alternativ var en rimlig miniminivå. De som tyckte brandvägg var en rimlig miniminivå bedömde detta till en svårighet av 1,6, alltså nästan mitt mellan mycket enkelt och enkelt.

5. Analys och diskussion

5.1 Säkerhetsläget på Internet

Enligt statistiken (Microsoft, 2010) har Internetbaserade hot ökat samtidigt som experterna pekar på att det kommer fortsätta att öka i framtiden.

Vi fann också att användandet av antivirusprogram och -spionprogram är vanligt. De flesta, vare sig de var insatta i ämnet eller ej, använde sig av skydd. Alla i undersökningen visste om vilka skydd de hade eller om de inte hade något antivirusskydd.

Resultatet pekar på att nästan alla var varse om att skadlig kod kan drabba dem, vare sig de är nybörjare eller erfarna datoranvändare. Experterna menade att man aldrig är säker utan skydd, oavsett hur duktig man anser sig vara. Det är bara en tidsfråga innan man blir drabbad. Dock påpekade experterna att man inte är fullt skyddad med den rekommenderade nivån av skydd, utan de krävs även viss nivå av försiktighet när man använder Internet. Som nämnt i teorin, är ofta skadlig kod dold och vissa användare kan därför tro de inte blivit drabbade då de inte ser några symptom.

Vi ställde en fråga om ifall våra enkät-respondenter tänkte ”det händer inte mig” när det gäller IT-säkerhetsfrågor. Ett antal av respondenterna valde alternativet ”osäker”, som vi tolkar som att man kan tänka detta i vissa situationer.

Enligt PMT så finns det en faktor som framhäver att det kan infinna sig en falsk känsla utav säkerhet. Detta kan medföra att man därmed inte skyddar sig för eventuella hot för att man kanske övervärderar kunskapen man besitter. IT-säkerhetsexperten på Panda Security Sweden, Sebastian Zabala styrker detta genom att berätta följande:

”*en falsk känsla av säkerhet som gör att användare i dagsläget inte tror att de är utsatta för någon fara. När de blir infekterade ser de väldigt sällan några symptom*” - Panda Security Sweden, 2009

5.2 Likheter och skillnader mellan användare och experter

Här nedan jämför vi några utav de viktigare frågorna för att skapa en lättare överblick om vad de båda ansåg i samma fråga.

Tabell 2: Jämförelse av experternas och användarnas svar

Fråga	Experterna sa	Användare sa
Risken att drabbas av skadlig kod?	Mycket stor. Svår att uppskatta.	Liten. Medelstor.
Skillnad för datorvana?	Ja, man blir inte lurad till att klicka för att det verkar ”intressant” lika enkelt.	De som är datorvana har bättre koll. Använder ofta sunt förnuft.
Vilken är miniminivån?	Antivirusprogram/-paket. Brandvägg. Uppdatering av programvaror.	Antivirusprogram. Brandvägg. Sunt förnuft. Eventuellt någon kryptering.
Hur ska man få personer att använda säkerhetslösningar?	Utbildning. Gör folk mer uppmärksamma på enklare åtgärder som att uppdatera operativsystemet och andra programvaror. Öka Medvetandet.	Göra program mer lättillgängliga. Gör så programmen inte tar så mycket dataresurser/processorkraft. Gör programmen så de inte märks av under vanlig datoranvändning.

Experterna anser att det är väldigt svårt att uppskatta hur stor risk det är att bli infekterad utav skadlig kod, men även att risken är stor, för alla. Användarna svarade däremot att de ansåg att det var en mindre risk att bli infekterad och vi antar att det är för att de tillfrågade har hög datorvana och anser sig vara säkra när de är ute och surfar på Internet, men de är ändå medvetna om riskerna. Resultatet visar antagligen på att det inte är så många som blivit infekterade utav skadlig kod.

När man har stor datorvana så menar experterna precis som användarna att det är en mindre risk för att bli infekterad eftersom man ofta använder sitt sunda förnuft och på så vis inte blir lurad till att trycka på någon länk som ser intressant ut, men som har ett helt annat innehåll. Man anser t.ex. att det är för bra för att vara sant och på så sätt struntar man i att gå in och titta. Detta skulle kunna tyda på att användare är mer försiktiga än vad vi faktiskt trodde, i alla fall de i populationen som är i någorlunda samma kategori både vad gäller utbildningsnivå och ålder som de som vi undersökte.

Minimikraven för att man skall vara säker på Internet gav ett liknande svar men användarna ansåg att man även kunde använda sig utav någon sorts kryptering för att göra det ännu svårare att bli angripen. Värt att nämna, så tryckte även användarna på att det är viktigt att använda sig utav sitt sunda förnuft för att undvika faror. Detta tyder på att man har ett högt säkerhetstänk idag och det beror på att Internet allt mer blivit en del av vardagen. På så sätt har man också blivit upplyst om vilka risker som finns och hur man undviker dem.

För att få användarna att använda sig mer utav olika säkerhetslösningar så anser

experterna att man ska informera användarna om enklare åtgärder som ökar ens skydd mot skadlig kod, t.ex. hur man uppdaterar sitt operativsystem, men även andra programvaror och varför man gör det. Användarna är inne på samma spår, man ska göra allt lättillgängligt och man ska inte märka av att ett program arbetar i bakgrunden. Varför många användare inte använder sig utav skydd är även för att de anser att det gör datorn långsammare. Användare tycker att säkerhetsexperter och företag ska rikta in sig mer på användarvänliga programvaror.

Våra experter anser att den vanligaste vägen att bli drabbad av skadlig kod är via Internet och webbläsaren. Detta samband kunde vi även finna i enkätsvaren, då en del skrev att man ska vara försiktig dels med vad man installerar från okända källor och att man ska hålla sig borta ifrån misstänkt opålitlig reklam och skumma länkar.

Spionprogram är en vanlig form av skadlig kod i dagsläget som mycket gärna involverar sig i webbläsaren och ofta följer med mindre program man installerar. Detta nämnde experterna som ett stort problem då webbläsaren var en av de största bidragande faktorerna till att man blev infekterad utav skadlig kod. Majoriteten av våra respondenter känner till vad spionprogram är och med tanke på att de hade en väldigt god datorvana kan man dra slutsatsen att respondenterna alltid granskar vilka program som följer med ett annat program. Detta är väldigt vanligt i mindre program som utför en specifik sak och med det programmet medföljer det ett verktygsfält som samlar information som i sin tur skickas vidare till utvecklarna som på så sätt kan kartlägga hur man surfat och skapa reklam därefter (Dubrawsky, 2006) Granskar man sen även hur våra respondenter agerar ifall de blir infekterade utav skadlig kod så ser man att de flesta åtgärdar problemen själva vilket även styrker att de är säkerhetsmedvetna och datorvana.

En annan sak att nämna är att experterna ansåg att social ingenjörskonst var en faktor som bara växer och växer. Det finns inget riktigt skydd emot detta på en fysisk nivå utan man måste skapa utbildningar inom detta område eller i alla fall ta med risken i en säkerhetsutbildning. Att vara medveten om vad det är och hur det går till, finslipa på sina protokoll över hur informationen får spridas i organisationen är saker man bör lära ut till alla. Detta gäller även för privatpersoner. Man måste alltid vara kritisk när någon undrar över något, så man inte går i fällan. Av våra respondenter så visste färre än hälften vad detta innebar och på så sätt kan man se att det krävs mer utbildning på denna front, även för personer som har bra datorvana.

Respondenterna menade även att skadlig kod idag är väldigt farligt och ska tas på allvar däremot var 98 % av respondenternas datorer ständigt uppkopplade till Internet när datorn var igång, oberoende av vad man skulle göra. Experterna förklarade att idag krävs det bara några få rader kod för att en mask ska sprida sig. På så sätt är man ett lätt offer för skadlig kod, trots man gör något som inte kräver uppkoppling emot Internet. Det var även här experterna återigen tryckte på att se till så att man har uppdaterade programvaror för att förhindra detta.
En annan viktig sak som togs upp var vilka förbättringar utav antivirusprodukterna våra respondenter ville se.

En av våra experter förklarade hur deras analys av nya hot fungerar och på så sätt så

kan man dra slutsatsen att ifall man vill att nya virus ska upptäckas snabbare så skall man aktivera ThreatSense.NET (Gustaf, 2010) som skickar anonym information till antivirusföretaget som sedan granskas och ifall det beaktas vara farligt, läggs det ut en uppdatering till samtliga klienter som använder sig utav denna antivirusprogramvara. Som privatperson hjälper man alltså till att förhindra att virus sprider sig.

Att man kan drabbas av skadlig kod och andra hot även som mer datorvan var våra respondenter och experter överens om. Detta tyder på att de som är mer datorvana aldrig går säkra oavsett hur säkerhetsmedvetna de är. Detta kan man framförallt syfta på att social ingenjörskonst är allt mer utbrett och att det inte finns så mycket att göra åt den mänskliga faktorn.

5.3 Orsaker till användarnas valda säkerhetsnivå

Anledningen till att vi väljer att tillämpa PMT på resultatet från vår undersökning är dels för att försöka utröna om mönstren vi ser liknar dem som syns generellt när människor ställs inför faror, men även om vi får liknande resultat som tidigare undersökningar inom området (Enbody et al, 2008; Clarke et al, 2010; Postin & Stafford, 2010; Chenoweth et al, 2009) fått fram.

PMT antar inte att personen tar beslut som man annars skulle klassificera som rationella.(Chenoweth et al, 2009)

Bland de 12 som sade nej på frågan om de hade antivirus fanns en som svarat så pass underligt att vi inte kan lita på att det är sant, därför bortser vi från denne persons svar då de är helt osammanhängande. Tre av de 12 var MAC användare och använde inte något antivirus av den anledningen. Resterande 8 av dem som inte använde sig av antivirus hade en rad olika anledningar till varför.

Alla utom en hade inhämtat kunskapen på egen hand och en av respondenterna hade inte särskilt god kunskap av de som inte hade antivirusprogram. Även i Clarke et al, (2010) undersökning på samma ämne så var det också bland det vanligaste att inhämta information på egen hand. Vilka typer av skadlig kod respondenterna kände till varierade, men det kan vara värt att nämna att två av dem kände till det påhittade speedbumps. Vanligast var att respondenterna inte utförde några specifika åtgärder för att minimera risken att drabbas av skadlig kod. Vanligt var också att de endast surfade säkra sidor och höll sig uppdaterade om de senaste hoten. Användarna av Internet är generellt medvetna om hoten mot deras datorsäkerhet enligt Postin & Stafford (2010).

5.3.1 Hur allvarligt användarna upplever hotet med skadlig kod

Nästan en tredjedel av våra respondenter bedömde att de själva enkelt eller mycket enkelt skulle kunna rätta till skadan som kan uppstå av skadlig kod på egen hand utan att ta hjälp av något antivirusprogram. Samtidigt så anser tre av fem av våra

respondenter att den potentiella skada som virus eller annan skadlig kod kan orsaka är mycket stor. Ungefär 20% bedömde att den skadliga koden kunde ställa till stor skada. Endast 7% ansåg att endast liten skada kunde uppstå medan ingen ansåg att skadlig kod orsakar mycket liten skada.

De som inte använde något antivirusprogram:
Bland de respondenterna som inte hade ett antivirus så bedömde de att det skulle vara lätt (2,2 på en femgradig skala) att rätta till skadan som skadlig kod ställer till med, även då de inte har ett antivirusprogram. Således tycker de kanske att de skulle kunna rätta till skadan nästan lika enkelt och bra som ett antivirus själva eller att hotet i sig inte är särskilt komplicerat. På så sätt kanske de förminskar hotet och inte gör något åt det av den anledningen (Enbody et al, 2008).

Intressant var att på frågan hur stor skada skadlig kod kan orsaka så tyckte de som inte använder antivirus i snitt att de kan ställa till stor till mycket stor skada (4,45 på en femgradig skala). Tidigare undersökningar indikerade att om man uppfattar hotet som litet eller stort så var man mer benägna att bete sig säkert (Enbody et al, 2008), vilken skiljer sig från dem som inte skyddade sig i vår undersökning då de upplevde hotet som ganska allvarlig skademässigt.

5.3.2 Hur stor upplever användarna att sannolikheten är att drabbas.

Nästan tre av fyra bedömer att de har goda eller mycket goda kunskaper om hur de kan undvika att drabbas av skadlig kod när de använder Internet. 25% av respondenterna ansåg att risken att drabbas av skadlig kod var liten medan 37% ansåg att risken var medelstor. Dock ansåg sammanlagt 36% att risken var stor till mycket stor att drabbas av skadlig kod vid Internet användning. De flesta av våra respondenter var medvetna om att de faktiskt kunde drabbas och endast en fjärdedel brukar ha tankebanor där de resonerar att det händer bara andra.

De som inte använde något antivirusprogram:
Bland dem som inte använde sig av antivirus resonerade någon av våra respondenter att denne aldrig innan haft virus, vad denne visste och därför trodde denne sig klara sig utan ett antivirusprogram. 4 av respondenterna svarade ja att det hände att de tänkte att det är bara andra som drabbas, 6 sa nej och en var osäker.

5 av respondenterna ansåg sig ha mycket goda kunskaper om hur man kan undvika få virus, 3 ansåg sig ha goda, 1 ha någon, 1 hade lite och en av respondenterna visste inte.

Risken att drabbas bedömde de i snitt till medelstor (2,8 på en femgradig skala).

5.3.3 Hur effektiv på att lösa problemet anser respondenterna att skyddsprogramvara är.

Ingen av våra respondenter tyckte att antivirus gör ett mycket dåligt jobb, men dock tyckte ungefär en av fem att virusskydden inte var effektiva utan att de gör ett dåligt jobb. En fjärdedel ansåg att antivirus gör ett helt OK jobb, medan två av fem tyckte

programmen gör ett bra jobb och vidare tyckte en av sex att antivirusen gör ett mycket bra jobb. Den absolut vanligaste förbättring av programmens effektivitet som våra respondenter önskade var bättre prestanda samt minnes- och processorkraftshantering. Med andra så ord vill de ha skyddsprogram som är mer datakrafteffektiva så man inte märker av lika mycket på datorns prestanda när man kör skyddsprogrammen. Två andra vanliga önskemål om förbättringar var användbarhet och att programmen skulle erbjuda bättre skydd.

De som inte använde något antivirusprogram:
Bland dem som inte använde sig av något antivirus var det några som valde att inte installera ett på grund av att de upplevde att de förlorade mycket av datorns prestanda. Några av respondenterna påpekade också att de tyckte det var jobbigt med alla notifikationer och krav om uppdateringar. Hälften av respondenterna skulle vilja ha bättre prestanda och processor och minneskraftshantering. Användbarhet var också önskat ett par gånger. Enbody et al (2008) fann att användare överväger alltid fördelarna med kostnaderna för både säkert som osäkert beteende. För vissa användare är inte fördelarna eller de möjliga negativa kostnaderna med deras beteende självklara. Säkerhet kan ibland enligt vissa användare kosta för mycket tid och pengar att införskaffa och uppdatera. (Enbody et al, 2008) Chenoweth et al (2009) pekade också på att personer som tyckte att skyddsprogramvaran var effektiv och relativt enkelt att använda hade större tendens att använda sig av programmen.

En av respondenterna menade att man inte behövde ett antivirus, utan en bra brandvägg var fullt tillräcklig.

Dock tyckte de som inte använde ett antivirus i snitt att antivirusprogrammen gör ett OK jobb (3 på en femgradig skala).

5.3.4 Hur effektiva anser användarna att de själva är på att implementera lösningen?

Majoriteten av våra respondenter upplevde sig som väl orienterade med datorer då 74% av dem tyckte att de hade god eller mycket god datorvana. Vidare tyckte de flesta som använde sig av virusskydd att det var enkelt eller mycket enkelt att installera och ställa in skyddsprogramvaran efter deras behov. Endast en marginell grupp, 12% av respondenterna, tyckte det var svårt till mycket svårt att anskaffa programvaran och att ställa in den. På frågan som behandlade hur svårt respondenterna upplever det är att installera och underhålla en miniminivå av skydd tyckte 80% att det var lätt eller mycket lätt. Endast en marginell grupp tryckte det var svårt.

De som inte använde något antivirusprogram:
Bland dem som svarade att de inte hade något antivirus så ansåg de sig i snitt att inneha god datorvana (4,27 på en femgradig skala). Enbody et al (2008) pekade på att vissa inte använder skyddsprogramvara på grund av att de är nybörjare och inte klarar av att implementera lösningen, detta var dock inte fallet bland våra respondenter. Personens egna uppfattning om dennes datorvana samt hur väl denne klarar av att hantera avancerade skyddsåtgärder är en viktig variabel. (Enbody et al, 2008) Detta stämmer med vad man brukar se när man använder PMT. (Rogers & Maddux, 1983)

Chenoweth et al (2009) i sin tur kom dock fram till att den upplevda självförmågan att genomföra lösningen spelade mindre roll. Chenoweth et al (2009) resonerade att det antagligen inte handlade om personens upplevda förmåga att installera ett program utan mer om deras uppskattning av hur kostsam lösningen är. Likt Chenoweth et al (2009), såg vi också detta mönster i vår undersökning.

Att underhålla miniminivån som de själva angett tycker de i snitt är mellan enkelt och mycket enkelt (1,6 på en femgradig skala).

5.3.5 Vad kan vara anledningen till respondenters val att inte skydda sig?

Den fjärde variabeln som oftast väger tungt (Rogers & Maddux, 1983) ifall en person tänker tillämpa vad som klassas som ett säkert beteende eller inte visade sig spela mindre roll i vår undersökning. Likt Chenoweth et al (2009)s undersökning så tyckte inte våra respondenter att det var särskilt svårt att anskaffa och underhålla en miniminivå av skydd, tvärtom, de bedömde det som mellan enkelt till mycket enkelt.

Våra respondenter bedömde att skadan som den skadliga koden potentiellt kan orsaka är stor till mycket stor. Risken att drabbas bedömdes till medelstor.

Hos våra respondenter verkade anledningen ligga i att de helt enkelt tyckte det kostade för mycket energi, både för dem själva och datorn, att använda ett antivirusprogram. De flesta som inte använde något program påpekade att datorn gick slöare och man fick en rad notifikationer som upplevdes som störande. I PMT termer så var det alltså effektiviteten på lösningen som inte var tillräcklig enligt dem som valde att inte använda sig av lösningen. Både bland annat Enbody et al (2008) och Chenoweth et al (2009) påpekade att användare tittar på effektiviteten och kostnaderna, för att sedan jämföra det med vinsterna.

5.4 Öka medvetandet genom utbildning

Båda experterna som vi intervjuade var eniga att det bästa sättet att öka medvetandet om den skadliga kod som man exponeras för vid Internetanvändning var utbildning. Frågan är då bara vilket medium som är effektivast att kanalisera denna utbildning genom. I vår undersökning så frågade vi användarna var de erhållit den eventuella kunskap de har om skadlig kod som de besitter.

Att leta information på egen hand var den absolut vanligaste vägen att införskaffa kunskap bland de som svarade på vår enkät. Detta reser dock nya frågor som till exempel på hur mycket de faktiskt kan eftersom de själva väljer att läsa om det de själv vill. I vissa fall kanske de inte ens är medvetna om det hela spektrumet av skadlig kod och kan därför inte söka ut information om det som de inte ens vet existerar. Tidigare undersökningar om privatsäkerhet pekar just på denna problematik att det är mycket svårt att mäta hur god kunskap människor faktiskt besitter då man inte har någon kontroll eller kriterier att följa när man söker på egen hand (Clarke et al, 2010). Om man bara tittar på vad respondenterna kände till i vår

undersökning så var de flesta, likt i Clarke et al (2010), medvetna om virus, spam och trojaner.

Om man tittar på vad användarna i vår undersökning själva bedömde nivån på deras kunskap om skadlig kod så tyckte de flesta, 7 av 10, att de hade god eller mycket god kunskap om vilka hot som finns. Bland dessa som ansåg sig ha goda eller mycket goda kunskaper så var det 9 av 45 (3 använder MAC) som inte använde någon form av skyddande programvara. Då kan man reflektera över att de kanske har hört talas om de olika hoten men inte är insatt i magnituden av hoten, eller rent av inte själva upplever skadlig kod som något större hot. Enbody et al (2008) fann även att personer som ansåg att hoten var marginella tillämpade säkerhetslösningar i mindre utsträckning och det är kanske så att de respondenterna i vår undersökning som ansåg sig vara mycket kunniga resonerar att de kan undvika hoten med hjälp av sin kunskap. Experterna vi intervjuade var eniga och påpekade att man absolut inte är säker utan antivirus eller annan skyddsprogramvara och att det mer är en tidsfråga innan man blir drabbad.

Enbody et al (2008) fann att det bästa sättet att förmedla information om ett hot var när man samtidigt förmedlade information om hur man kan hantera hotet. Det är även viktigt att man hjälper användarna att behärska de svårare skyddsåtgärderna. När man argumenterar för säker Internetanvändning bör man inte bara fokusera på de primära fördelarna såsom att man minskar chansen att drabbas av skadlig kod, en del fokus bör även läggas på de sekundära fördelarna som mer effektiv datoranvändning och minskat behov av reparationer. (Enbody et al, 2008)

Enligt Enbody et al (2008) kan man som oftast öka en persons säkerhetsbeteende om man belyser att det är dennes eget ansvar att tillämpa säkert beteende. Dock fungerar inte denna taktik på de som antigen förminskar hotets betydelse eller för de som inte anser sig själv kapabla att tillämpa önskvärt säkerhetsbeteende.

Det är viktigt att man har rätt kunskap och kan applicera den på ett korrekt sätt när man kommer ut i arbetslivet. När det gäller hemarbete och kundkontakt för företag är det viktigt att användare har korrekt utbildning inom IT-säkerhet. För organisationer inom IT-branschen är säkerhet bland de viktigaste aspekterna för att de ska tas på allvar och anses professionella.

6. Slutsatser

Efter att ha granskat resultaten både från enkätundersökningen och från expertintervjuerna, så kan vi dra slutsatsen att det som experterna ville poängtera ofta var känt hos de flesta av privatpersonerna. Idag är det naturligt att man dagligen uppdaterar sitt virusskydd, operativsystem och tredjepartsprodukter. Användarna vet att säkerhetsbrister kan uppstå om man inte uppdaterar sin programvara till senaste versionen.

Man kan dra slutsatsen att våra respondenters säkerhetstänk är bra. Enligt enkätundersökningen såg vi också svar från respondenterna som var i klass med experternas svar gällande t.ex. minimikraven för ett säkert Internetanvändande. Något vi även noterade var att några respondenter beskrev den rekommenderade säkerhetsnivån på ett mer avancerat sätt än vad experterna svarade på samma frågeställning. Kunskapsnivån bland de vi frågat är bra i allmänhet.

Man kan använda sig av specialiserade analysmotorer som ThreatSense.NET (som vi även beskrivit tidigare i teorin) för att bli än mer framgångsrik när det gäller analysering av nya hot och nya typer av skadlig kod. Dessa verktyg kan vara till stor hjälp för användare och får dem att känna sig säkrare. Med denna metod finns också möjligheten att sända en misstänkt fil till antivirusföretaget och få bekräftat om det är något att ta i beaktande eller inte. Visar det sig sedan att det är ett hot, så ges detta en signatur i deras system och vid nästa uppdatering finns filen med som ett hot som fastnar under analysen.

Bland dem som inte använde sig sig av någon skyddsåtgärd, fanns två läger. Det ena lägret var de som använder sig av MAC-datorer, och hävdar att de inte är utsatta. Vidare undersökningar på huruvida detta stämmer eller inte hade varit av värde. Det andra lägret var de som inte använde sig av skyddslösningar då de tycker dessa är ineffektiva. Det visade sig att den tredje variabeln i *PMT* vägde tungt för våra respondenter. För att skydda sig mot skadlig kod, kände de att de fick offra för mycket.

B1 Enkät- och intervjufrågor

B1.1 Expertfrågor

Vi kommer att ställa frågor om vad Ni ser för trender inom skadlig kod, hur hotbilden mot privatpersoner ser ut, samt hur säkerhetsmedveten man bör vara som privatperson. Syftet med undersökningen är att få en bra bild av vilka risker den enskilda datoranvändaren står inför, för att sedan använda detta som en grund när vi letar övrig teori och som en hjälp för att bättra på vår egen kunskap.

- Vilken typ av skadlig kod är den dominerande för tillfället och vilka typer tror Ni kommer vara dominerande om 5 år? (t.ex. virus, trojansk häst, malware)

- Tror Ni mängden skadlig kod kommer öka eller minska? På vilka områden? Varför?

- Ser Ni några trender i vilka kanaler på Internet som spridningen av den skadliga koden sker? Finns det andra vägar än Internet?

- Är dagens kod mer avancerad än den som funnits förut? Är den svårare att upptäcka och kan den orsaka större skada?

- Vad kan Ni göra för att motarbeta Social Engineering? Vad tror Ni om utvecklingen av detta fenomen? Har Ni någon bra lösning?

- Hur sker er analys av nya hot mot privatanvändaren?

- Hur stor bedömer Ni risken är att drabbas av skadlig kod vid vanlig Internetanvändning utan skydd? Tror Ni det är någon stor skillnad på nybörjaren och den mer datorvane?

- Vad anser Ni är ett minimikrav vad gäller skydd mot skadlig kod? Vidare vad anser Ni skulle vara en rekommenderad nivå?

- Hur säker är man ifall man har skydd av den rekommenderade nivån men inte besitter kunskap om hur man använder Internet på ett säkert sätt?

- Hur anser Ni svenskar ligger till i jämförelse med andra länder i försiktighetsåtgärder och nivå av aktivt skyddande?

- Hur medvetna om riskerna med Internetanvändning och att drabbas av skadlig kod tror Ni privatpersoner generellt är?

- Vad anser Ni är ett effektivt sätt att bättra privatpersoners säkerhetsbeteende?

Det skulle dessutom vara intressant om Ni ville berätta något ytterligare som skulle kunna vara relevant för vår undersökning men som vi inte tagit upp i våra frågor.

Ps. Om ni har tid så skulle vår handledare vilja veta vilka programvaror/tjänster ni kan rekommendera att han berättar om och ger förslag på under sin IT-säkerhetskurs framöver. Ds.

Tack för er medverkan!

Med vänliga hälsningar
Dan, André & Thomas

B1.2 Enkätfrågor

Detta är en enkät som belyser området IT-säkerhet hos privatpersoner. Enkäten tar ett par minuter att svara på. Vi kommer att sammanställa era svar på frågorna för att sedan analysera dem och försöka dra slutsatser. Dessa slutsatser kommer vi att använda oss av i vårt examensarbete vid Lunds Universitet.

Alla svar behandlas anonymt!

Begreppet skadlig kod omfattar all kod och alla program som har för avsikt att orsaka datoranvändaren ekonomisk skada eller skada på mjuk-/hårdvaran.

Vi skulle uppskatta att Ni besvarar alla frågor så gott ni kan.

Var vänlig och besvara denna enkät endast en gång.

Tack på förhand!
André, Dan & Thomas

Frågor markerade * är obligatoriska.

1. Vad är er ålder?*
[] 18-30
[] 31-50
[] 51+

2. Vilken är din högsta pågående/ avslutade utbildning?*
[] Grundskola
[] Gymnasieskola
[] Högskola/ Universitet

3. Hur god anser du att din datorvana är?*
[] 1 nybörjare
[] 2
[] 3

[] 4
[] Mycket god

4. Använder du dig av antivirus eller annan skyddande programvara?*
[] Ja
[] Nej (Motivera gärna under 4.1 och hoppa sedan till fråga 6)
[] Vet inte

4.1 Om du svarade Nej, varför?

4.2 Om du svarade Ja, vet du vilket?
[] AVG
[] F-secure
[] McAfee
[] NOD32
[] Norton Antivirus
[] Panda
[] Vet inte
[] Övrigt ___

5. Om du har ett virusskydd, hur tyckte du det var att installera/ ställa in det efter dina behov?
[] 1 Mycket enkelt
[] 2
[] 3
[] 4
[] 5 Mycket svårt

6. Tycker du att virusskydd gör ett bra eller dåligt jobb?* Motivera gärna under 6.1
[] 1 Mycket dåligt
[] 2
[] 3
[] 4
[] 5 Mycket bra

6.1 Motivering av svar på fråga 6

7. Hur tycker du att tillverkarna av antivirusprogrammen skall förbättra sin produkt? Motivera gärna under 7.1. *Flera val är möjligt*
[] Användbarhet
[] Bättre skydd
[] Utökning av tjänster
[] Prestanda, minnes- och processorkraftshantering
[] Bättre notifikationer
[] Tycker inte att det behövs några förbättringar
[] Övrigt: ___

7.1 Motivering

8. Om du inte har ett antivirusprogram och drabbas av skadlig kod, hur svårt anser du då att det är att rätta till skadan?
[] 1 Mycket enkelt
[] 2
[] 3
[] 4
[] 5 Mycket svårt

9. Hur bra kunskaper anser du att du har för att undvika att få virus eller annan skadlig kod när du Internetsurfar?
[] Mycket goda kunskaper
[] Goda kunskaper
[] Någon kunskap
[] Lite kunskap
[] Vet inte

10. Var har du erhållit denna eventuella kunskap
[] På egen hand
[] Via jobbet
[] Via media
[] Via skolan
[] Har inte särskilt god kunskap
[] Övrigt: ___

11. Vilka av följande varianter av skadlig kod känner du till? *Flera val är möjligt*
[] Scamming
[] Phising
[] Virus
[] Speedbumps
[] Spyware
[] Social-engineering
[] Spam
[] Trojaner
[] Keyloggers

12. Hur stor skada generellt anser du att skadlig kod kan orsaka?*
[] 1 Mycket liten
[] 2
[] 3
[] 4
[] 5 Mycket stor

13. Hur stor anser du att risken är att drabbas av skadlig kod?*
[] 1 Mycket liten
[] 2
[] 3
[] 4

[] 5 Mycket stor

14. Vet du hur du skall gå tillväga ifall du drabbas av skadlig kod?
[] Kontaktar antivirusföretaget
[] Kontaktar datorleverantören
[] Om möjligt, tar bort det själv
[] Kontaktar en kunnig vän
[] Nej

15. Händer det att du tänker ”det händer bara andra” när det kommer till IT-säkerhetsfrågor?
[] Ja
[] Nej
[] Osäker

16. När är du uppkopplad mot Internet i vanliga fall?
[] När datorn är igång
[] När jag använder tjänster som kräver Internet
[] Vet inte

17. Hur mycket använder du din dator på fritiden i snitt per dag?
[] Mindre än 1 timme
[] 1-2 timmar
[] 2-3 timmar
[] 3-4 timmar
[] 5+ timmar

18. Hur går du till väga för att minimera risken för att drabbas av skadlig kod? *Flera val är möjliga*
[] Uppdaterar kontinuerligt mitt antivirus
[] Uppdaterar kontinuerligt samtliga program på datorn
[] Håller mig uppdaterad om de senaste hoten
[] Surfar endast på sidor jag anser säkra
[] Utför inga specifika åtgärder

19. Kortfattat, vad anser du är en bra miniminivå av skydd?

19.1 Hur svårt tycker du det är att installera och underhålla denna nivå?
[] 1 Mycket lätt
[] 2
[] 3
[] 4
[] 5 Mycket svårt

B2 Intervju 1

- Den mest dominerade skadliga koden idag kommer in via webbläsaren. Webbläsaren har väldigt många brister idag och detta utnyttjar virustillverkarna, se därför till att hålla de uppdaterade. Det går inte riktigt att gissa vad som kommer att vara det största hotet om fem år men utav vad jag märkt här så kommer skadlig kod för mobiltelefoner öka radikalt med tanke på mobilteknikens framfart på senaste.
- Skadlig kod kommer garanterat att öka med tiden, eftersom tekniken går framåt!
- Den största spridningen av skadlig kod sker helt klart på Internet, framförallt inom webbläsare.
- Dagens skadliga kod är väldigt mycket mer avancerad om man jämför med tidigare typer av skadlig kod. Den är framförallt mycket svårare att upptäcka och kan med all sannolikhet skapa mer problem idag än vad den gör ifall virustillverkarna velat detta. Dock gjorde gårdagens skadliga kod mer skada då mycket av dagens virus inte är skapade för att förstöra.
- Fenomenet social engineering, att lura användare kommer definitivt att öka och bli mer sofistikerat än vad det är idag. För att minska detta fenomenet så anser jag att utbildning är den bästa lösningen för detta och ur ett produktperspektiv så kan man även minska detta problemet med ett välutvecklat skräppostskydd.
- Denna typ av analys sker i stort sätt automatiskt.
- Risken idag för att bli utsatt för skadlig kod är mycket stor. Självklart så är det enklare för en nybörjare att bli angripen av skadlig kod men detta gör inte att den erfarne användaren är immun utan den kanske överskattar sina förmågor istället.
- Minimikravet är självklart ett säkerhetspaket som innehåller dels antivirusprogram men även en bra brandvägg. Rekommenderad lösning är att ha ovanstående paket fast med backup-lösningar inbyggda samt att man ständigt uppdaterar samtliga programvaror på datorn.
- Ifall man har det rekommenderade ovanstående paketet så är man relativt säker trots man inte har någon direkt datorvana.
- Enligt min åsikt och erfarenhet så är svenskar bättre skyddade idag jämfört med omvärlden.
- Enligt min uppfattning så är kunskapen för Internetanvändning generellt bra idag, speciellt om man jämför med gårdagens generation.
- För att öka privatpersoners säkerhetsbeteende så anser jag att utbildning är den bästa vägen för att verkligen lära sig något på ett säkert sätt.

Mvh ”Fredrik”

B3 Intervju 2

Vilken typ av skadlig kod är den dominerande för tillfället och vilka typer tror Ni kommer vara dominerande om 5 år? (t.ex. virus, trojansk häst, malware)

Det vi ser mest av för tillfället i ThreatSense.NET (beskrivning nedan) är fortfarande varianter av Conficker-masken. Rent generellt så det som folk drabbas mest av (som de märker av) är troligtvis falska antivirusprogram ("rogue security software"). Mer riktade och personligt anpassade attacker kommer troligtvis att öka mer de närmaste åren, både i form av skadlig kod som är unik och anpassad för attackmålet, och större användning av social ingenjörskonst för att lura personer att installera skadlig kod.

Tror Ni mängden skadlig kod kommer öka eller minska? På vilka områden? Varför?

Vi tror att den kommer öka, och förmodligen se fler riktade attacker mot företag och organisationer. Det är redan en miljardindustri med skadlig kod, och med mer utvalda specifika attackmål blir det både svårare att skydda sig, och har större möjlighet till ekonomiska vinster för brottslingarna.

Ser Ni några trender i vilka kanaler på Internet som spridningen av den skadliga koden sker? Finns det andra vägar än Internet?

Skadlig kod som utnyttjar sig av "autorun.inf" är fortfarande rätt vanlig. De utnyttjar möjligheten att automatiskt starta program när man stoppar i en extern enhet i datorn (t.ex. ett USB-minne). Många hot är flerfacetterade och använder sig av flera olika sätt att sprida sig, vilket gör att det nu för tiden kan vara svårt att klassificera vissa hot (t.ex. något som sprider sig som en mask, installerar en bakdörr, och gömmer sig som ett rootkit).

Vi har även sett en stor ökning av utnyttjande av sökmotoroptimering för att sprida skadlig kod. Vi har sett flera fall där stora nyheter utnyttjas av brottslingar innan de har tagits upp av "normal" nyhetsmedia.

De utnyttjar sig av infekterade datorer och hackade hemsidor för att få bättre resultat i sökmotorer, och vid till exempel kändisars dödsfall har det hänt att de flesta sökresultaten på förstasidan varit länkar till skadlig kod.

På sidorna så är det sedan olika sätt för att installera den skadliga koden, antingen utnyttjande av olika säkerhetshål för flera olika operativsystem och webbläsare, att de försöker lura användaren att installera det själv (genom att utge sig för att vara en uppdatering till exempelvis Flash, eller ett säkerhetsprogram), eller en kombination

av flera olika metoder.

Är dagens kod mer avancerad än den som funnits förut? Är den svårare att upptäcka och kan den orsaka större skada?

Eftersom datorer och andra enheter är mer uppkopplade och sammankopplade än förut så finns det mycket större potential nu för skadlig kod att få stor spridning, eller att det "råkar" hamna på enheter med viktig/känslig information.

Tekniskt sett så har det varit en nedgång i hur "avancerad" koden är, men det börjar gå uppåt igen. Redan under 90-talet så användes avancerade tekniker för att skapa polymorfism och kod som försökte dölja sig själv, men i samband med Internets genombrott, och en bredare användarskara så har det inte behövts så avancerad kod för att sprida sig. Ett enkelt skript på några rader kunde enkelt sprida sig till miljontals användare världen över, något som tidigare bara kunde sprida sig via exempelvis disketter och manuellt kopierade filer.

Däremot så har vi sett en större uppgång nu för tiden med avancerade rootkits och patchade system där det ofta är nästintill omöjligt att upptäcka den skadliga koden på en infekterad dator om man inte startar upp den från en "ren och säker" miljö (exempelvis en CD-skiva) och där gör genomsökningen. Även större utnyttjande av server-baserad polymorfism har ökat, vilket gör att antivirusföretagen inte har lika stora möjligheter att undersöka hur den skadliga koden har genererats, och får svårare att stoppa olika varianter av koden.

Vad kan Ni göra för att motarbeta Social Engineering? Vad tror Ni om utvecklingen av detta fenomen? Har Ni någon bra lösning?

Utbildning och medvetenhet är det mest effektiva för att slippa bli drabbad. Man måste inse att man kan inte köra vilka program som helst, och att man inte ska lita på vem som helst. Det finns stora pengar för folk att tjäna bara på att man litar på fel person, eller kör ett till synes harmlöst program. Vi ser även ofta personer som har övertro på sin säkerhet, och bara för att de är på jobbets "nedlåsta" dator, eller kör ett antivirusprogram så tror de att de kan köra vad som helst för att det inte bör kunna göra någon skada.

Som sagt så kommer troligtvis riktade attacker, förstärkta av social ingenjörskonst, att öka mycket då det är ett effektivt sätt att få mycket pengar/information från ett färre antal mål, och innebär mindre chans för upptäckt, än att försöka få mindre summor från flera olika.

Vi försöker satsa mycket på utbildning, och vi producerar även en podcast varje vecka (som finns på www.eset.se) där vi tar upp aktuella säkerhetshot och händelser, samt informerar och tipsar om hur man kan skydda sig. Vi håller den fri från marknadsföring och den kan således användas som en opartisk källa för säkerhetsutbildning och fortbildning inom datasäkerhet och integritet.

Hur sker er analys av nya hot mot privatanvändaren?

Alla våra produkter utnyttjar sig av något som kallas ThreatSense.NET. Det är en motor som gör att vi får tillgång till anonym statistik om nya hot, och även har möjlighet att få tillgång till nya varianter av skadlig kod som upptäcks med hjälp av våra proaktiva metoder (främst via kodanalys för att känna igen skadlig kod). Så när en person någonstans i världen stöter på exempelvis en ny variant av Conficker, så får vi information om det, och även en kopia på filen om vi inte redan har tillgång till den. Det gör att vi snabbt får information om hur stor spridning vissa hot får, och om vi upptäcker att det skapas flera olika varianter av viss skadlig kod. På så sätt kan vi fokusera på att ta reda på, och stoppa, källan till spridningen, och även se till att anpassa både virussignaturer och vår kodanalys för att ännu effektivare kunna stoppa eventuella ändrade framtida varianter av koden.

Det har dock ökat markant de senaste åren. Vi får in över hundratusen (checksummeunika) filer per dag med skadlig kod. Det innebär att man inte har möjlighet att manuellt undersöka alla filer, men det är ju sådant som redan stoppats proaktivt, så man försöker istället se trender över vilka varianter av hot och källor som används, och riktar in sig på att stoppa varianterna och källan som används för spridningen.

För direkt analys av skadlig kod används flera olika metoder. Mycket kan automatiskt klassificeras genom automatiska system, och sedan så gör en virusanalytiker bara en snabbare koll och skapar en signatur för att hitta det.

Mot större och "farligare" hot så krävs det ofta en mer avancerad ingående analys, vilket kan ta lång tid när man analyserar och debuggar koden manuellt.

Hur stor bedömer Ni risken är att drabbas av skadlig kod vid vanlig Internetanvändning utan skydd? Tror Ni det är någon stor skillnad på nybörjaren och den mer datorvane?

Det är väldigt svårt att uppskatta. Det beror stort på hur Internetanvändningen ser ut. Om man har sina "vanliga" hemsidor man besöker, eller om man ofta "klickar på roliga länkar", eller håller på med fildelning.

Oftast så är det svårare att bli lurad om man är mer datorvan. Man vet att webbläsaren inte kan söka igenom datorn efter virus automatiskt, och man blir kanske inte lika lätt lurad att installera något program för att se en "lockande" film.

Vad anser Ni är ett minimikrav vad gäller skydd mot skadlig kod? Vidare vad anser Ni skulle vara en rekommenderad nivå?

Jag ser tre "tekniska" punkter som absolut viktigast:

1. Håll operativsystemet uppdaterat (t.ex. via Windows Update)
2. Håll tredjepartsprogram uppdaterade (t.ex. Flash, Java och PDF-läsare)
3. Ha ett uppdaterat antivirusprogram installerat

Det innebär att man stoppar mycket av den skadliga koden, oavsett om den utnyttjar säkerhetshål i operativsystemet, webbläsaren eller något annat program, eller om man luras att köra någon fil som kan hittas av antivirusprogrammet.

Som rekommenderad nivå vill jag gärna att folk även inte ska vara inloggade som administratörer, och att de vänjer sig att inte installera/klicka på vad som helst på hemsidan. Det är trivialt att få en hemsida att verka seriös och rekommendera en uppdatering av exempelvis Flash som egentligen innehåller skadlig kod. Det är väldigt svårt att vänja folk av med att installera program "direkt från webbläsaren". Troligtvis kommer användandet av exempelvis AppStore på iPhone, och Software Repositories i Linux att öka och användas i större utsträckning även i andra operativsystem.

Hur säker är man ifall man har skydd av den rekommenderade nivån men inte besitter kunskap om hur man använder Internet på ett säkert sätt?

Man är relativt bra skyddad, men det beror helt på hur man använder Internet. Om man bara besöker aftonbladet och kanske kollar på youtube-klipp så är naturligtvis riskerna mindre än om man ofta besöker "okända" sidor, eller laddar ner filer via olika fildelningsverktyg.

Hur anser Ni svenskar ligger till i jämförelse med andra länder i försiktighetsåtgärder och nivå av aktivt skyddande?

Jag tycker att svenskar i allmänhet är rätt bra skyddade. Ett vanligt problem i andra länder är att man fortfarande har kvar väldigt gamla versioner av sitt operativsystem, och inte håller det uppdaterat. Det är vanligare i Sverige att man ser att folk håller sina datorer uppdaterade med nyare operativsystem, och även använder sig av något säkerhetsprogram. Troligtvis är det en blandning av kulturella och ekonomiska anledningar.

Hur medvetna om riskerna med Internetanvändning och att drabbas av skadlig kod tror Ni privatpersoner generellt är?

I Sverige tror jag att folk generellt är medvetna om en del av riskerna. Många tycker exempelvis att de klarar sig så länge som man inte surfar på hemsidor med "tvivelaktigt innehåll". Det de inte tänker på är att eftersom det ligger så mycket pengar bakom det, så är det oftast så mycket mer avancerat än så. Kriminella som är

anställda för att sprida skadlig kod, eller till och med ge support för falska antivirusprogram! De betalar sökmotorer och stora vanliga hemsidor för att (utan hemsidans kännedom) ha "helt normala" annonser som pekar på sidor med skadlig kod, och de kan betala för att få en professionellt designad hemsida. Sådant är folk inte lika medvetna om.

Folk är heller inte lika vana vid riktade attacker och till vilken nivå de kriminella är beredda att gå för att få en dator infekterad.

Många håller fortfarande kvar vid "varför skulle de bry sig om mig och min dator, jag har inget hemligt. Spelar inte så stor roll om jag blir infekterad heller, bara att installera om", vilket är en farlig omedvetenhet om vidden av det hela.

Vad anser Ni är ett effektivt sätt att bättra privatpersoners säkerhetsbeteende?

Att få folk att hålla sina system uppdaterade, och ha ett säkerhetsprogram installerat räcker inte alltid, men det räcker till en stor del. Utbildning och medvetenhet är det effektivaste, men istället kanske det svåraste att uppnå. Allt eftersom folk blir mer vana att ha tillgång till Internet och webbtjänster både hemma och i mobilen så kommer de behöva inse att det finns och kommer alltid finnas sårbarheter både i hård- och mjukvara, men även att det oftast är deras eget aktiva agerande och deras handlingar är det som orsakar problem. Att luras via social ingenjörskonst eller fås att köra skadlig kod kan vara väldigt svårt att undvika, men med en viss medvetenhet så kan man stoppa mycket.

Med vänlig hälsning,
”Gustaf”
EUROSECURE

7. Referenser

Chalmers.se,2006. *Human aspects of Computer Security*
Tillgänglig på: http://www.ce.chalmers.se/edu/year/2006/course/EDA262/oh06/ohF12_human_aspects.pdf
[Avläst 5.5.2010].

Chenoweth, T., Gattiker, T. & Minch, R. (2009): Application of Protection Motivation Theory to Adoption of Protective Technologies. *2009 42nd Hawaii International Conference on System Sciences,* ss. 1-10.

Clarke, N., Furnell, S. & Talib, S. (2010): An analysis of information security awareness within home and work environments. *2010 international conference on availability, reliability and security,* ss. 196-203.

Dubrawsky, I. (2007) *How to cheat at securing your network*. Burlingtom: Syngress

Enbody, R., LaRose, R. & Rifon, N. (2008): PROMOTING PERSONAL RESPONSIBILITY for Internet SAFETY. *Communications of the ACM,* 51, ss. 71-77.

ESET, 2010. *ThreatSense.NET*
Tillgänglig på: http://www.eset.eu/threat-center/threat-sense.net
[Avläst 20.5.2010]

Gollmann, D. (2006): *Computer Security*, Chichester: John Wiley & Sons.

Jacobsen D. I. (2002): *Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.,* Studentlitteratur, Lund.

Maddux, J.E. & Rogers, R.W. (1983): Protection motivation and self-efficacy. A revised theory of fear appeals and attitude change. *Journal of experimental social psychology,* 19, ss. 469-479.

Microsoft, 2010. *Microsoft Security Intelligence Report Volume 8*
Tillgänglig på: http://www.microsoft.com/downloads/details.aspx?FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5&displaylang=en
[Avläst 10.5.2010]

Microsoft, 2002. *Danger: Remote Access Trojans*
Tillgänglig på: http://technet.microsoft.com/en-us/library/dd632947.aspx
[Avläst 12.5.2010]

Panda Security, 2009. *Sverige har näst minst antal infekterade datorer i världen*
Tillgänglig på: http://www.pcm.se/pcm/nyheter/press/pdf/PR_090930_Sverige_nast_minst_antal_infekterade_datorer_i_varlden.pdf
[Avläst 19.5.2010]

Pfleeger C. P. och Pfleeger S. L. (2003): *Security in Computing: Third Edition*, Pearson Education, Inc. Upper Saddle River, New Jersey.

Postin, R. & Stafford, T.F. (2010): Online security threats and computer user intentions. *Computer,* 43, ss. 58-64.

Stanford, 2010. *The Trojan War*
Tillgänglig på: http://www.stanford.edu/~plomio/history.html
[Avläst 12.5.2010]

MIT 1992. *The Robert Morris Internet Worm*
Tillgänglig på: http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html
Groups.csail.mit.edu
[Avläst 19.4.2010]

Rogers, R.W. (1975): A protection motivation theory of fear appeals and attitude change. *Journal of pshychology,* 91, s. 93.

Symantec, 2010. *Crimeware: Trojans & Spyware*
Tillgänglig på: http://www.symantec.com/norton/cybercrime/trojansspyware.jsp
[Avläst 5.5.2010]

Symantec, 2004. *Datavirus allt svårare att upptäcka*
Tillgänglig på: http://www.symantec.com/region/se/press/n040316_se.html
[Avläst 19.4.2010]

Symantec, 2010. *Trojan Horse*
Tillgänglig på: http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99&tabid=2
[Avläst 12.5.2010]

Symantec, 2010. *Spyware: Vad innebär det för dig?*
Tillgänglig på: http://www.symantec.com/sv/se/norton/clubsymantec/library/article.jsp?aid=cs_spyware_what_it_means_to_you
[Avläst 5.5.2010]