Lunds universitet
Ekonomihögskolan
Informatik

Säkerhetsrisker för smarta mobiltelefoner i företag

Kandidatuppsats, 15 högskolepoäng, SYSK02 i informatik

Framlagd: 31 maj 2012

Författare: Viktor Bergvall
Johannes Forslund
Sebastian Persson

Handledare: Magnus Wärja

Examinator: Markus Lahtinen
Claus Persson

Abstrakt

Titel	Säkerhetsrisker för smarta mobiltelefoner i företag
Författare	Viktor Bergvall Johannes Forslund Sebastian Persson
Utgivare	Institutionen för informatik
Handledare	Magnus Wärja
Publiceringsår	2012
Språk	Svenska
Nyckelord	Säkerhetsrisker, smarta mobiltelefoner, malware, avlyssning, intrång.

Abstrakt

Mobiltelefoner liknar allt mer datorer och med detta kommer likartade risker. Följaktligen bör man därför skydda sig likvärdigt gentemot dessa hot och risker. Vi har därför undersökt om företag är medvetna om dessa hot och risker och om de har några utarbetade åtgärder för att skydda sina smarta mobiltelefoner mot dessa risker och hot. För att ta reda på detta har vi utfört intervjuer med fyra företag som vi valt utifrån några av oss förutsatta kriterier. Resultatet av vår undersökning visar och tar upp de främsta riskerna mot smarta mobiltelefoner i företag. Vidare visar resultatet att företag generellt sett har bristande alternativt helt saknar åtgärder som förebygger eller åtgärdar säkerhetsluckorna för smarta mobiltelefoner inom företaget.

Innehållsförteckning

Figur och tabellförteckning

Tabeller

Figurer

1. Inledning

Vi börjar det första kapitlet med att berätta lite om bakgrunden till uppsatsen samt varför vi anser detta vara ett relevant ämne att basera vår uppsats på. Vidare kommer vi ta upp vårt problemområde samt vilken problemställning vi kommer inrikta oss på och syftet till detta. Eftersom ämnet informationssäkerhet sträcker sig över ett väldigt brett område kommer vi beskriva hur vi avser avgränsa oss och vilken problemställning vi främst kommer inrikta oss på att analysera och fördjupa oss i.

1.1 Bakgrund

Smarta mobiltelefoner är idag ett viktigt verktyg hos anställda inom de flesta verksamheter och tillåter ett allt mer mobilt arbetssätt än vad som tilläts för tio till femton år sedan. Att använda sin smarta mobiltelefon som ett primärt planerings- och kommunikationsverktyg är idag för de flesta företag en självklarhet och bidrar till ett effektivt och flexibelt arbetssätt. Smarta mobiltelefoner gjorde sitt första insteg i företagsvärlden redan under mitten av 90-talet men har explosionsartat ökat under de senaste tio åren och fungerar idag mer eller mindre som ett substitut till en personlig dator. Enligt Gartner ökade försäljningen av smarta mobiltelefoner mellan 2010 och 2011 med 58 % och det totala antalet sålda enheter under 2011 uppgick till 472 miljoner (Gartner, 2012). Detta innebär att fler individer ägde en smart mobiltelefon i slutet av 2011 och att fler företag köpte in smarta mobiltelefoner som företagstelefoner. I sin tur innebär detta att allt mer hemlig företagsinformation lagras och behandlas i de anställdas enheter vilket innebär att förlust av dessa kan innebära förlust och läckage av kritiskt sekretessbelagda företagshemligheter som i fel händer kan åsamka omfattande skador på verksamheten. En mer omfattad användning medför också ett ökat intresse och därmed en högre risk för intrång och informationsförlust om säkerhetsrutiner och åtgärder inte övervägs och utformas noga.

De flesta mobiltelefontillverkarna tillverkar idag smarta mobiltelefoner. Enligt en undersökning gjord av Gartner visas den totala försäljningen av mobiltelefoner till slutanvändare via återförsäljare i hela världen.

Tabell 1,1. Worldwide mobile device sales to end users by vendor in 2011 (thousands of units), (Gartner 2012)

Company	2011 Units	2011 Market Share (%)	2010 Units	2010 Market Share (%)
Nokia	422,478.3	23.8	461,318.2	28.9
Samsung	313,904.2	17.7	281,065.8	17.6
Apple	89,263.2	5.0	46,598.3	2.9
LG Electronics	86,370.9	4.9	114,154.6	7.1
ZTE	56,881.8	3.2	29,686.0	1.9
Research In Motion	51,541.9	2.9	49,651.6	3.1
HTC	43,266.9	2.4	24,688.4	1.5
Huawei	40,663.4	2.3	23,814.7	1.5
Motorola	40,269.0	2.3	38,553.7	2.4
Sony Ericsson	32,597.5	1.8	41,819.2	2.6
Others	597,326.9	33.7	485,452.0	30.4
Total	**1,774,564.1**	**100.0**	**1,596,802.4**	**100.0**

Tabellen visar att Nokia hade hela 23,8 % av marknadsandelarna år 2011, följt av Samsung med 17,7 % (Gartner, 2012).

Enligt en undersökning gjord av Ponemon Institute i mars 2011 använde 84 % av de tillfrågade samma smarta mobiltelefon i arbetet som privat (Ponemon Institute, 2011). Detta medför att den information som är relaterad till arbetet kan finnas på telefonen även under användarens privata tid och utsätts därmed för en ökad risk. Vidare visar undersökningen att det endast var 11 % som inte lagrade någon sorts personlig data på sin smarta mobiltelefon (Ponemon Institute, 2011). Detta visar att en smart mobiltelefon med största sannolikhet innehåller känslig information som i fel händer kan skapa omfattande problem för ägaren av enheten.

Mobiltelefoner, i synnerhet så kallade smarta mobiltelefoner, är mer lika datorer nu än tidigare. De har blivit allt mer kraftfulla och användbara i långt fler situationer än vad de var för tio år sedan. Detta betyder att de också måste skyddas på samma vis som en dator. Telefonen utsätts för samma risker vid exempelvis internetsurfning och kräver då samma skydd som en dator för att förhindra såkallat phishing, malware, virus samt andra intrång som kan medföra informationsläckage eller i värsta fall förlust (Post- och Telestyrelsen).

1.2 Problemområde

I takt med en ökande användning av smarta mobiltelefoner ökar också riskerna för intrång och förlust av viktig information. Därmed blir det allt viktigare för företag som använder smarta mobiltelefoner i arbetet att vara medvetna om vilka risker och hot som finns, och hur det kan påverka det egna företaget. Många anställda använder idag samma smarta enhet till arbetet som till privat bruk, vilket innebär att känslig företagsinformation då kan följa med den anställda hem. Vad händer om en anställds smarta enhet exempelvis blir stulen eller borttappad? Har företaget någon säkerhetspolicy eller annan plan om/när detta sker? Utan väl genomtänka säkerhetspolicys eller riktlinjer är risken att information hamnar i fel händer överhängande. Säkerhetspolicys bör baseras på vilka risker och hot ett företag står inför och bör spegla ett företags krav på vilken säkerhet de själv förväntar sig inneha. Det bör också noga gås igenom vilken inverkan olika risker och hot har på företaget och hur de individuellt kan skada verksamheten. Det är viktigt att ha i åtanke att teknologi som en ensam faktor sällan kan förhindra intrång utan är i sin tur beroende av en väl utformad säkerhetspolicy som stöd (Jansen & Scarfone, 2008).

1.3 Forskningsfråga

För att få en bättre klarhet angående företags syn på säkerhetsrutiner gällande smarta mobiltelefoner vill vi besvara följande forskningsfråga:

- *Vilka risker och hot finns det mot smarta mobiltelefoner i företag och hur förebyggs informationsförlust och intrång av olika slag?*

1.4 Syfte

Syftet med uppsatsen är att genom undersökning och analys, påvisa och dra en slutsats om hur väl medvetna företag är om de risker som finns gällande smarta mobiltelefoner, och dess användning inom företaget. Vi vill också att rapporten ska bidra till en ökad förståelse bland företag för vilka risker som finns och vilka åtgärder som kan vidtas för att förebygga, eller minska effekten av dessa risker.

1.5 Avgränsningar

Anställda på företag kan använda sig av ett antal olika mobila enheter, exempelvis smarta mobiltelefoner. Under arbetet utsätts dessa enheter för olika risker. Företagsinformation finns som tidigare nämnt oftast i de anställdas smarta mobiltelefoner. Den här uppsatsen kommer endast att behandla anställdas smarta mobiltelefoner och riskerna relaterade till dessa för den information om företaget de arbetar på. Riskerna gällande privatpersoner och deras personliga information kommer inte att diskuteras.

1.6 Uppsatsens upplägg

Vi börjar den här uppsatsen med en genomgång av vad en smart mobiltelefon är, vilken information den kan innehålla samt vilka som är de största hoten mot smarta mobiltelefoner. Därefter tar vi upp ett exempel på en grundläggande variant av säkerhetspolicy som kan appliceras på smarta mobiltelefoner. Denna policy tar sedan upp hur dessa hot och risker kan hanteras och vilken policy som är kopplad till respektive risk. Utifrån våra risker genomför vi sedan vår undersökning. När undersökningen dokumenterats analyserar vi de resultat vi har fått fram relaterat till de tidigare nämnda riskerna och hoten mot smarta mobiltelefoner. Slutligen besvarar vi vår forskningsfråga med hjälp av all den information och empiriska data vi samlat in och presenterat i uppsatsen.

2. Litteraturgenomgång

I följande kapitel går vi igenom lite allmänt vad en smart mobiltelefon är för något och vad dessa kan användas till. Vi går också igenom olika säkerhetsrisker och hot som användare av smarta mobiltelefoner i företag ställs inför varje dag och hur denna kan skydda sig mot olaga intrång som följaktligen kan medföra förlust av sekretessbelagd information. Kapitlet behandlar också vilka risker som finns med att tappa bort sin smarta enhet samt hur man på bästa möjliga sätt återvinner en uttjänt produkt.

2.1 Inledning

2.1.1 Vad är en smart mobiltelefon?

En smart mobiltelefon eller som vi i denna uppsats även kommer att kalla ”smart enhet”, är en mobiltelefon som i regel är lite större än en vanlig mobiltelefon och kan utföra en mängd andra uppgifter utöver den primära uppgiften att ringa samtal. Det kan vara att skicka och ta emot e-post, behandla olika sorters dokument, möjligheten att presentera material och utnyttja olika sorters medier. De flesta smarta mobiltelefoner har också möjligheten att koppla upp sig mot internet via WiFi (Wireless fidelity). (Jansen & Ayers, 2007)

På de smarta mobiltelefonerna körs olika operativsystem beroende på vilken tillverkare telefonen kommer ifrån. Det kan vara exempelvis Android, iOS eller Symbian. Vidare styrs oftast den smarta mobiltelefonen med hjälp av en pekskärm eller ett litet tangentbord. (Nationalencyklopedin)

Möjligheten för en smart mobiltelefon att anpassas efter användarens behov genom olika applikationer är stor. De applikationer som finns tillgängliga varierar beroende på vilket operativsystem som den smarta mobiltelefonen använder men en del populära applikationer finns tillgängligt till mer än ett operativsystem (Jansen & Scarfone, 2008).

En smart enhet innehåller de flesta komponenter som en vanlig dator gör, exempelvis en processor, RAM-minne (Random Access Memory) och någon sorts lagringsutrymme, oftast i from av ett SD-kort (Secure Digital) (Jansen & Scarfone, 2008).

2.1.2 Information som finns på enheten

Den vanligaste informationen som finns på smarta mobiltelefoner är e-mailadresser och kontaktlistor. En undersökning gjord utav Ponemon Institute år 2011 visade att hela 97 % av de tillfrågade hade e-mailadresser lagrade, 69 % hade olika kontaktlistor lagrade och 37 % hade någon sorts konfidentiell information lagrad på sin smarta mobiltelefon. Vidare visar undersökningen också att 26 % av de tillfrågade lagrade en betydande del personlig information på sin smarta mobiltelefon. (Ponemon Institute, 2011)

2.1.3 Operativsystem

Det finns ett flertal olika operativsystem för smarta mobiltelefoner. Alla operativsystem är mottagliga för hot och risker, vissa dock mer än andra. De vanligaste operativsystemen är:

Android - Android är Googles operativsystem för smarta mobiltelefoner, och har de senaste åren vuxit förbi Apples iOS och RIMs BlackBerry. Androidanvändarna utgör nu 46,9 procent av alla användare av smarta mobiltelefoner. Därmed är också Android mest intressant för de som utvecklar malware, då de kan nå ett större antal offer än om de inriktar sig på något annat operativsystem. Bara från juni till december 2011 ökade antalet malware-enheter som riktar sig mot Android-användare från 400 till 13 302. Något som gör Android extra attraktivt för malware är den öppna marknaden för applikationer, som gör det möjligt för utvecklare att ladda upp och distribuera applikationer utan någon kontroll. En utvecklare kan alltså utan problem ladda upp en applikation som innehåller skadlig programkod. (Juniper, 2012)

iOS - Apples iOS var under 2011 det näst mest populära operativsystemet för smarta mobiltelefoner, med 28,7 procent av användarna. iOS är dock inte lika utsatt som Android, främst på grund av att Apple har en strikt kontroll på vilka applikationer som är tillgängliga för nedladdning i deras butik, *App Store*. Denna begränsning av operativsystemet går dock att kringgå genom att låsa upp (jailbreaka) sitt operativsystem och därmed möjliggöra nedladdning av applikationer från tredje part. Det finns inte heller några säkerhetsprogram för användare av iOS att installera, då Apple inte tillhandahåller de nödvändiga verktygen som behövs för att utveckla detta. Om någon sorts malware skulle ta sig igenom Apples kontroll-process finns det alltså väldigt lite en användare kan göra för att skydda sig. (Juniper, 2012)

Övriga operativsystem - Utöver de två ovan nämnda finns ett antal andra operativsystem, som givetvis är utsatta för malware även dem. Research in Motion (RIM) *BlackBerry*, Nokias *Symbian* och övriga operativsystem utsätts även de för allt mer malware, ökningen har dock stannat av jämfört med tidigare år. Malware som har utvecklats för *Java ME* kan drabba flera olika operativsystem, framförallt Symbian- och Windows-telefoner. Eftersom Java ME-malware kan fungera på mer än ett operativsystem har utvecklingen av dessa fortsatt att öka, trots att användandet av operativsystemen har minskat. (Juniper, 2012)

2.2 Risker

Vi har utifrån teorin valt att ta upp fem säkerhetsrisker som anses vara relevanta för smarta mobiltelefoner idag. Riskerna är:

- Förlust av enhet
- Återvinna enhet
- Malware
- Avlyssning
- Intrång

Riskerna för smarta mobiltelefoner grundar sig i två olika faktorer. Dessa faktorer är de smarta enheternas storlek och portabilitet samt den trådlösa tillgängligheten och övriga associerade tjänster. (Jansen & Scarfone, 2008)

2.2.1 Förlust av enhet

En smart enhet har i regel storleken som en plånbok och finns oftast hos användaren större delen av tiden. Detta medför att den finns på många olika platser under dagen och riskerar att tappas bort. Enligt en undersökning gjord under sex månaders tid år 2005, som handlade om vad som glömdes kvar i taxibilar, visade det sig att det glömdes hela 3,42 mobiltelefoner/taxibil i Chicago, USA, under den tiden (Check Point, 2005). Vidare finns också risken för stöld av enheten. Stölder kan i stort sätt förekomma var som helst men risken att utsättas för stöld ökar då man vistas på offentliga platser.

Förebyggande återgärder

Installera mjukvara som gör det möjligt att fjärrstyrt kunna lokalisera och spåra den försvunna mobiltelefonen. Installera även mjukvara som gör det möjligt att fjärrstyrt kunna rensa och låsa, göra säkerhetskopior samt skydda och återställa informationen på mobiltelefonen. (Juniper, 2012)

2.2.2 Återvinna enheten

Det finns också tillfällen då enheten inte längre fyller sin fulla funktion och ska slängas eller återvinnas. Vid dessa tillfällen brukar en manuell återställning göras för att radera all data som finns på enheten. Efter en sådan återställning finns det fortfarande möjlighet att återställa den data som raderats genom olika sorters mjuk- och hårdvara (Jansen & Scarfone, 2008).

Ett verktyg som går att använda för att återskapa data som funnits på en mobiltelefon är en så kallad “Flasher box” (Jansen & Scarfone, 2008). Det är från början ett verktyg för att utföra olika sorters service på mobiltelefoner som exempelvis återställning av information eller uppgradering av mjukvara och består av mjukvara, hårdvara och drivrutiner (Al-Zarouni,

2007). Dessa verktyg går att införskaffa genom olika hemsidor på internet (Jansen & Scarfone, 2008).

Varje mobiltelefon, vare sig det är en smart mobiltelefon eller inte, innehar ett IMEI-nummer (International Mobile Equipment Identity). Detta nummer är till för att identifiera en mobiltelefon som kopplar upp sig mot det mobila nätet. Mobiltelefonen kan spärras genom IMEI-numret och då hamnar den spärrade mobiltelefonen i en svart lista som registreras i ett register som kallas EIR (Equipment Identity Register). Om mobiltelefonens IMEI-nummer finns med i den svarta listan kan det mobila nätverket vägra ge någon signal till den svartlistade mobiltelefonen. På så vis kan en stulen mobiltelefon spärras ifrån att användas utav en obehörig användare. (Al-Zarouni, 2007)

Som tidigare nämnt finns det ett verktyg som kallas "Flasher box" som kan användas för att återställa information på en mobiltelefon. Detta verktyg kan också användas för att ändra IMEI-nummert på en mobiltelefon, vilket kan göra en svartlistad mobiltelefon möjlig för normal användning (Al-Zarouni, 2007).

Förebyggande åtgärder

I och med att möjligheten finns att återskapa information som blivit raderad på enheten bör användaren aldrig spara information som kan tänkas vara känslig för användaren eller de företag som användaren arbetar för.

2.2.3 Malware

Malware är en förkortning av den engelska termen *malicious software* och används som samlingsnamn för mjukvara som är skapad för att på något sätt orsaka skada på en dator, server eller ett nätverk (Microsoft, 2003).

I takt med att mobiltelefoner utvecklades till smarta mobiltelefoner ökade också intresset för att skapa malware, för eget nöje eller för kriminella handlingar. I juni 2004 upptäcktes den första internetmasken vars mål var smarta mobiltelefoner. Masken gjorde ingen skada, utöver att den brukade batterikraft, utan spred bara sig själv mellan smarta mobiltelefoner genom Bluetooth-anslutningar. Sedan dess har mängden malware som riktar sig mot smarta mobiltelefoner ökat i ett rasande tempo. 2010 var mängden malware 11 138 enheter och 2011 hade siffran ökat med 155 procent till 28 472 enheter (Juniper, 2012).
Det finns flera olika sorters malware, som angriper smarta mobiltelefoner på olika sätt:

Virus - Ett virus är ett program som installerar sig själv i ett annat program, ett värdprogram, och därefter multiplicerar sig när värdprogrammet körs (Hypponen, 2006). Ett virus kan påverka användaren på många olika sätt. Det kan vara något så enkelt som att en irriterande dialogruta öppnas eller något så allvarligt som att filer raderas från hårddisken. Somliga virus är även programmerade att redigera sig själva för varje kopia som sprids, vilket gör varje kopia unik och därmed svårare att upptäcka. (Harrington, 2005)

Maskar - Maskar är själv-reproducerande mjukvara som automatiskt sprids via nätverk och andra anslutningar (Hypponen, 2006). Effekterna liknar ofta effekterna av ett virus, exempelvis kan de skada filer lagrade på hårddisken (Harrington, 2005).

Trojanska hästar - Trojanska hästar är program som utger sig för att vara något som användaren vill spara på sin dator eller smarta mobiltelefon, men som gömmer skadlig programkod (Hypponen, 2006). De trojanska hästarna kan användas av hackare för att öppna en sorts bakdörr till de system de vill ha åtkomst till. De kan också användas för att spåra en användares knapptryckningar i en fil, som sedan kan hämtas och utnyttjas av en hackare som har skapat sig tillgång till systemet. (Harrington, 2005)

Spyware - Mjukvara som samlar in och delar med sig av personlig information till obehöriga (Hypponen, 2006). Spyware, som tidigare kallades för *adware*, var från början tänkt som ett sätt för skapare av gratis programvara att inkludera reklam i sina program, för att på så sätt generera en inkomst. Tanken var att annonserna endast skulle samla in demografisk information om användaren för att sedan kunna visa annonser som intresserar just den användaren. Spyware har dock utvecklats sedan dess och samlar nu in all möjlig personlig information, och brukar sedan användarens anslutning för att skicka informationen vidare. (Harrington, 2005)

Malware kan spridas på flera olika sätt, till exempel genom kommunikationsnätverk, så som e-post eller MMS, eller genom att den smarta mobiltelefonen synkroniseras med en dator eller annan lagringsmedia (Jansen & Scarfone, 2008). Några vanliga spridningssätt är:

Nedladdning av filer på internet - Användaren laddar ner en fil som kan vara maskerad som ett spel, en säkerhetsuppdatering eller någon annan användbar applikation. Även programvara som i sig själv inte innehåller någon form av malware kan skapa problem, om de innehåller säkerhetshål som kan utnyttjas av malware. (Jansen & Scarfone, 2008)

Meddelandetjänster - Malware kan bifogas i e-post och MMS, och sedan installeras den skadliga programvaran på en smart enhet när användaren öppnar och installerar den bifogade filen. Även tjänster för snabbmeddelanden, till exempel MSN, som går att installera på det flesta smarta mobiltelefoner kan fungera för att skicka malware mellan olika enheter. (Jansen & Scarfone, 2008)

Bluetoothanslutning - Via en Bluetoothanslutning kan filer skickas mellan två olika enheter. Enheter kan ställas in i olika lägen vad gäller Bluetooth: synlig, vilket innebär att enheten är synlig för andra enheter som har Bluetooth aktiverat; anslutningsbar, vilket innebär att enheten kan ta emot och svara på meddelanden från anslutna enheter; eller helt avstängd. Malware kan alltså spridas genom att upprätta kontakt med en enhet som är försatt i synligt läge. (Jansen & Scarfone, 2008)

Förebyggande åtgärder

För att skydda sig mot malware på bästa sätt bör företag installera anti-malware mjukvara på samtliga smarta mobiltelefoner som behandlar information om företaget. Mjukvaran bör skydda mot alla de ovan nämnda sorternas malware. Företag bör också ständigt försäkra sig om att samtliga enheter har uppdaterat skydd mot malware genom att installera mjukvara som samlar information om vilket operativsystem som den smarta telefonen använder, vilken anti-malware mjukvara som är installerad samt *jailbreak*- eller *root*-status. Även en brandvägg bör installeras för att skapa maximal säkerhet. (Juniper, 2012)

2.2.4 Avlyssning

Vid ett viktigt eller mer privat samtal tenderar användaren söka sig från befolkade platser för att undvika att någon annan lyssnar på dennes samtal. Avlyssning eller "eavesdropping" som termen heter på engelska, är precis vad det heter. Användarens telefon blir avlyssnad utan dennes vetskap och användarens enskildhet är genast inkräktad utan att användaren vet om detta. (Jansen & Scarfone, 2008)

Den enklaste vägen för denna typ av malware att ta sig in i användarens telefon är genom spionprogram. Dessa spionprogram samlar in och skickar vidare information till en annan enhet och intrånget är därmed ett faktum. Spionprogrammen annonseras ofta som övervakningsprogram som t.ex. att hjälpa föräldrar övervaka sina barns aktiviteter med sina smarta mobiltelefoner eller andra övervakningssyften. En funktion som för många kan verka lukrativ. (Jansen & Scarfone, 2008)

En annan metod som används är att ett öppet nätverk imiteras och användaren luras att använda det imiterade nätverket i god tro att denna använder det "riktiga" nätverket. Detta kan ske på t.ex. caféer eller andra offentliga platser där öppna nätverk erbjuds. Personen som gör intrånget får på så sätt tillgång till användarens information han eller hon har på sin enhet och kan även genom denna metod modifiera informationen samt kontrollera trafiken till och från enheten. (Meyer & Wetzel, 2004)

Avlyssning är ett stort problem då avlyssning kan ske helt utan vetskapen från den utsatta att denna blir avlyssnad (Yi-Bing & Meng-Hsun, 2007). För att nämna ett exempel är detta fenomen ett relativt allvarligt problem med företagstelefoner då mycket sekretessbelagd kommunikation sker över samtal mellan smarta mobiltelefoner. Vid eventuell avlyssning kan hemlig företagsinformation enkelt läcka ut till obehöriga. Det är inte heller nödvändigt att avlyssning sker under just samtalet utan avlyssning kan ske utan att användaren aktivt använder sin telefon genom att ett spyware-program blir installerat på telefonen antingen genom att en applikation laddas ner eller genom meddelandetjänster såsom sms, e-mail eller tjänster för snabbmeddelanden såsom msn-messenger (Jansen & Scarfone, 2008).

Förebyggande åtgärder

Vilka åtgärder kan då vidtas för att undvika att bli utsatt för denna typ av intrång? Till att börja med är det väldigt viktigt att användaren ser till att enheten inte används av fel personer eller på något annat sätt hamnar i fel händer. Att använda sig av lösenord eller "swipelocking" (ett låsningsalternativ som låter användaren låsa upp telefonen genom att dra fingrarna i ett av användaren förvalt mönster), när användaren vill in i telefonen är också en bra säkerhetsåtgärd för att i största mån undvika att obehöriga personer kommer åt ens enhet. Detta kommer förhindra att malware manuellt installeras på enheten men kommer naturligtvis inte hindra att malware i form av t.ex. spyware tar sig in i enheten via applikationer, mail, meddelande osv. För att förhindra detta behöver företagen som nämnt tidigare använda sig utav någon form av virusprogram som kontrollerar all trafik som kommer till enheterna. På detta sätt minskar risken avsevärt att få in skadlig malware i de smarta telefonerna som kan ställa till med stora bekymmer för användaren. Att sedan hålla dessa anti-malware program fräscha och fortsatt motståndskraftiga och effektiva är väldigt viktigt och görs som nämnt genom att hålla dem uppdaterade med de senaste versionerna (Guo, Wang & Zhu, 2004).

2.2.5 Intrång

En smart mobiltelefon är som tidigare nämnt precis som en dator fast i ett mindre format. Det medför att olaga intrång likt det som kan ske på en vanlig dator även kan ske på en smart mobiltelefon. Därför gäller det att minska riskerna för att bli utsatt för detta.

Oavsett om en mobiltelefon har aktiverat de inbyggda säkerhetsåtgärderna som exempelvis en pinkod och ett säkerhetslås, finns det fortfarande en risk att en obehörig person kan gissa vilken kod som använts eller gå förbi låsen med hjälp av rätt verktyg. Oftast används likartade lösenord som exempelvis "1234" som med fördel och med lätthet testas av en obehörig person. (Jansen & Scarfone, 2008)

En mobiltelefons möjlighet att skicka och ta emot SMS, MSS, skicka och ta emot data via Bluetooth och även synkronisera med en dator, utsätter mobiltelefonen för risker (US-CERT, 2010). Ett meddelande kan skickas via exempelvis SMS innehållande skadlig kod som vid ett öppnande gör det möjligt för obehöriga att ta sig in i mobiltelefonen genom en bakdörr (Jansen & Scarfone, 2008).

Förebyggande åtgärder

För att minska riskerna att en obehörig person kan komma åt information på en användares mobiltelefon kan några förebyggande åtgärder vidtas. Att försäkra sig om att mobiltelefonen innehar den senaste versionen av mjukvara så som operativsystemet, ökar mobiltelefonens säkerhet (US-CERT, 2010).
Vidare bör PIN-koden och eventuellt säkerhetslås vara aktiverad och inte innefatta de vanligaste kombinationerna som exempelvis "1234" (Jansen & Scarfone, 2008).
En ytterligare åtgärd kan vara att installera något sorts antivirusprogram som finns tillgängligt

och hålla det uppdaterat. Se till och ha som vana att ha Bluetoothanslutningen avstängd och var uppmärksam på märkliga meddelande som mottagits och inte öppna okända meddelanden kan också vara till en användares fördel. (US-CERT, 2010)

2.3 Säkerhetspolicys

Företag riskerar att råka ut för de risker och hot vi tagit upp och för att skydda sig mot dessa kan säkerhetspolicys användas för att definiera hur ett bra skydd ska utformas och varför det ska användas. (Osborne, 2006)

En säkerhetspolicy garanterar inte ett bra skydd mot intrång, malware och andra risker. Däremot kan den som nämnt ovan ge riktlinjer för hur ett bra skydd ska utformas och varför det ska användas. Det är farligt att fokusera för mycket på säkerhetspolicyn och därmed riskera att missa andra vitala delar av säkerhetsprocessen, som till exempel att faktiskt genomföra allt det som står i policyn. (Osborne, 2006)

Säkerhetspolicyn bör utformas för att stödja företagets säkerhetsstrategi. Den bör även följa nedanstående punkter (Osborne, 2006).

- **Ledande** - Policyn ska utformas som ett antal regler för informationssäkerhet som ska följas. Dokumentet är inte menat för diskussion eller för att efterfråga samtycke.

- **Oberoende av teknologi** - Policys ska skrivas så att det är möjligt att ändra operativsystem och annan teknologi utan att behöva ändra policyn.

- **Stöd från ledningen** - Företagets ledning måste stå bakom policyn för att den ska kunna införas på ett bra sätt.

- **Möjlig att implementera** - En policy måste vara realistisk och möjlig att genomföra och efterfölja.

- **Ägande** - Någon måste äga policyn, ha ansvar för att det uppdateras och efterföljs.

2.3.1 Exempel på säkerhetspolicy

Osborne beskriver i sin bok "How to Cheat at Managing Information Security" hur en enklare säkerhetspolicy gällande informationssäkerhet kan se ut.

Tabell 2,1. Säkerhetspolicy (Osborne 2006)

Policy:	Beskrivning:
Informations klassifikation:	Här ska det beskrivas hur information ska klassificeras.
Skydd av data:	Beskriva hur företaget ska skydda olika sorters data vid olika tillfällen.
Åtkomstkontroller:	Här skall följande beskrivas: Inloggningsprocesser, lösenordsregler, revisionsregler, dataroller.
Internetanvändning:	Beskriver acceptabel nätetikett.
E-postanvändning:	Varna användarna om vilka risker e-post medför.
Viruskontroll:	Beskriver reglerna som finns angående virusskydd samt vad de ska göra om deras enheter drabbas.
Backup och undanröjande av data:	Backup policyn bestämmer att system bör säkerhetskopieras när de är i bruk, samt att dessa säkerhetskopior ska testas och skyddas enligt företagets behov. Policyn angående undanröjande av data förklarar till exempel att hårddiskar ska förstöras, CD-skivor ska sandas (blästras) och brytas av, band ska avmagnetiseras innan de kastas bort.
Trådlös åtkomst:	Beskriver hur nätverket nås trådlöst.
Fysiskt skydd:	Beskriver det fysiska skyddet.
Kryptering:	Beskriver konfidentialiteten av informationen.
Mjukvarulicensiering:	Beskriver användningen av licensierad mjukvara.
Policy för godtagbar användning:	Denna del ska beskriva godtagbar användning utav enheten och beskriva de delar som är förbjudna att använda. Det är främst i utbildningssyfte.

Ovanstående policyexempel (tabell 2,1.), är enligt Osborne (2006) en bra grund för en säkerhetspolicy. Policyn tar upp ett antal punkter som beskriver hur företaget eller verksamheten i fråga ska förebygga olika risker. Policyexemplet beskriver hur en generell och relativt grundläggande policy kan se ut. Vårt exempel är inte djupgående vad gäller respektive hot utan beskriver snarare övergripande vilka riktlinjer som bör följas för att minska risker och hot.

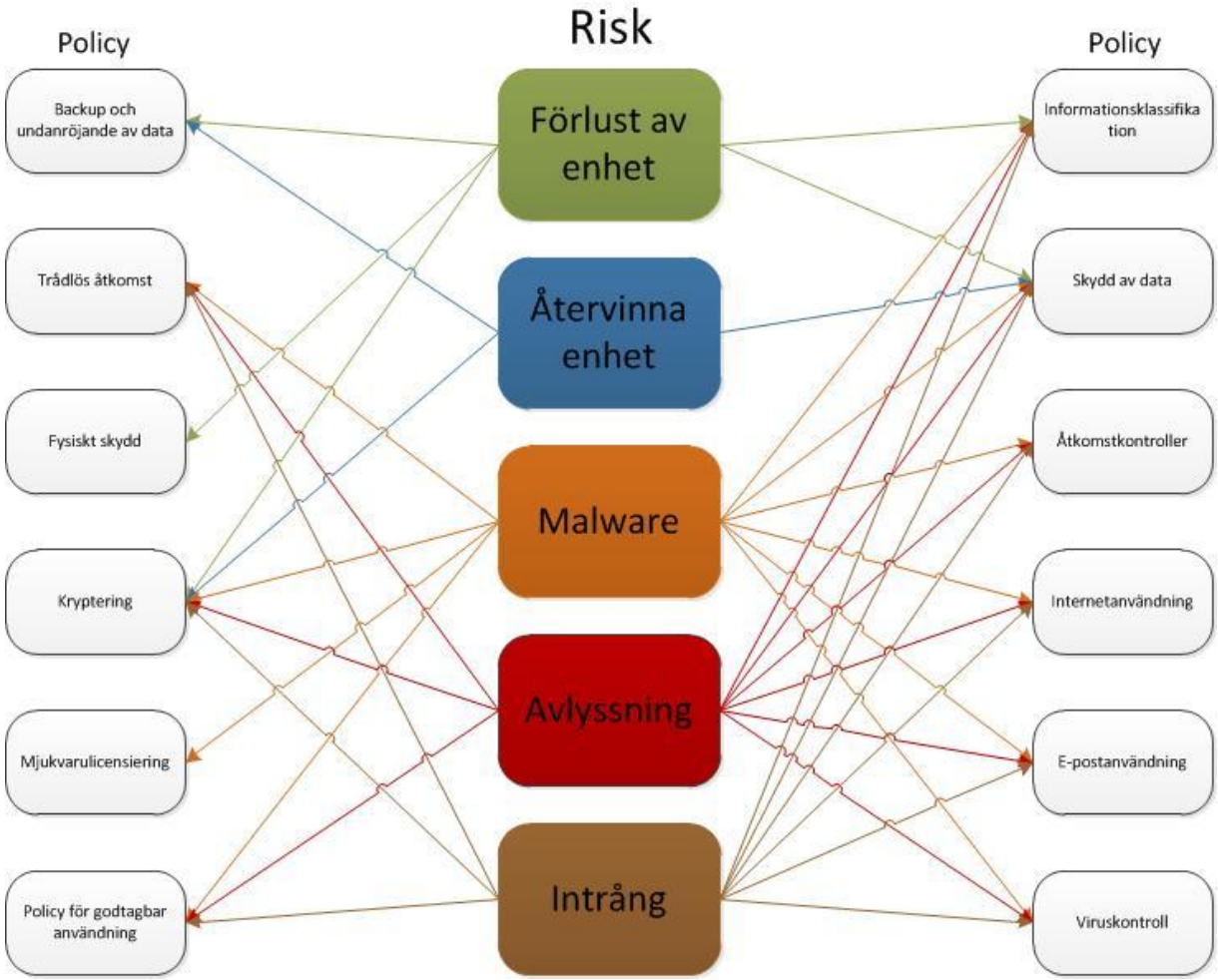
2.4 Undersökningsmodell

I det senaste kapitlet har vi tagit upp allmänna teorier angående säkerheten kring smarta mobiltelefoner. Inledningsvis beskrivs vad en smart mobiltelefon är för något och vilka plattformer som erbjuds samt vad som ligger till fördel respektive nackdel för de olika plattformerna. Följt av beskrivningen om vad en smart mobiltelefon är för något tas de generella säkerhetsriskerna upp som vi anser är de viktigaste att nämna. En mer ingående beskrivning av respektive säkerhetsrisk presenteras med en tillhörande förebyggande åtgärd som beskriver hur man kan undvika att drabbas i största möjliga mån. Slutligen går vi igenom en variant av säkerhetspolicy.

Utifrån dessa fem risker kommer vi undersöka företags medvetenhet kring säkerhetsrisker för smarta mobiltelefoner. Riskerna som är genomgående för hela uppsatsen är till grund för vår undersökning och kommer styra hur vi samlar in empiriskt material.

Figur 2,1. Undersökningsmodell

På nästa sida presenteras en modell (figur 2,2) på en policy baserad på de fem säkerhetsrisker vi tog upp i början av kapitlet. Modellen beskriver vilken del av policyn som hanterar en viss risk. Detta för att validera att våra fem utvalda risker går att applicera på en säkerhetspolicy. Vi har även gjort en modell (se bilaga 4) på en mer ingående säkerhetspolicy (se bilaga 3) för att ytterligare validera att de fem riskerna är möjliga att applicera på en säkerhetspolicy.



Figur 2,2. Risker och de policys de är kopplade till

Varje pil i modellen ovan (figur 2,2) visar vilken policy som är kopplad till respektive risk. Varje risk kan vara kopplad till många policys och vice versa. Exempelvis kan ”förlust av enhet” kopplas till fem olika policys. T.ex. backup som en förebyggande åtgärd är viktig att utföra för att kunna återställa förlorad information. Vidare är undanröjande av data vid förlust av en enhet viktigt för att minska risken för att företagshemlig information hamnar i fel händer.

3 Metod

Följande kapitel kommer behandla och beskriva våra metoder vi använt oss av för att besvara vår forskningsfråga. Det kommer följaktligen beskrivas vilken typ av undersökning vi gjort och hur denna bidragit till vår slutsats. Vidare kommer det också beskrivas vad som gått bra respektive mindre bra med genomförandet av undersökningen och vilka faktorer som kan anses ha bidragit till positiva respektive negativa utfall.

3.1 Undersökningsmetod

Vid undersökningens början planerade vi först genomföra en kvantitativ enkätundersökning, då vi trodde att detta skulle ge oss en större målgrupp och ett större antal svar. Genom att använda oss av denna metod får vi större möjlighet att generalisera och strukturera svaren (Jacobsen, 2002). Enkäten visade sig dock vara svår att få svar på, och en allt för låg svarsfrekvens gjorde att vi istället tog beslutet att göra kvalitativa intervjuer. Den låga svarsfrekvensen berodde troligtvis både på det känsliga ämnet, att få var villiga att lämna ut information som rör företagets säkerhet över internet, samt på att frågorna var utformade på ett sätt som uppmuntrade respondenterna att utveckla sina svar, vilket många kan ha ansett vara för tidskrävande.

Vi valde därefter att göra en kvalitativ undersökningsmetod i form av intervjuer. Detta eftersom vi genom denna metod får fram den verkliga förståelsen samt en individuell och unik tolkning av situationen (Jacobsen, 2002). För att utföra våra intervjuer skapade vi en öppen intervjuguide som strukturerade upp intervjun, men ändå lämnade plats för respondenten att utveckla sina svar och för oss att ställa följdfrågor. Detta gav oss möjlighet att få svar på alla de frågor som kunde dyka upp under intervjuns gång, och vi var inte låsta till specifika svarsalternativ eller specifika frågor. Intervjuerna har genomförts både vid möte med respondenten samt över telefon i de fall då möten inte varit möjliga. Från intervjuerna har vi fått den primärdata som är nödvändig för att besvara vår forskningsfråga och dra slutsatser relaterade till denna.

3.2 Val av respondenter

Vi valde ut företag efter några kriterier vi satte upp för vilka egenskaper företaget i fråga skulle ha för att vara en godkänd intervjukandidat. Vårt första krav eller riktmärke var att företaget skulle använda sig av smarta enheter i arbetet och i hela företaget. Det skulle således vara mer eller mindre majoriteten av personalen som tillhandahölls en smart mobiltelefon när de började arbeta för företaget. Orsaken till detta är naturligtvis att undersökningen i annat fall hade saknat grund och företaget hade troligtvis inte haft någon anledning att oroa sig eller tänka på riskerna smarta enheter kan utsättas för. Ett andra krav vi satte upp var att företaget inte skulle vara ett litet företag, och därmed ha minst 50 anställda för att enligt oss kunna räknas som ett tillförlitligt underlag (Europa, 2006). Detta eftersom vi anser att ett företag med 50 anställda eller fler utgör en större måltavla för hot och risker än vad ett företag med färre anställda utsätts för. Ett sista krav vi hade på företagen som intervjuades var att de skulle vara inriktade mot IT-branschen på något sätt. Detta eftersom vi också här antog att IT-företag ofta är medvetna och långt framme med teknologin i företaget och därför är mest troliga att ha tänkt på säkerheten kring mobila enheter.

3.3 Intervjuguide

Vår intervjuguide är baserad på den modell (figur 2,2.) vi utformat i teorigenomgången. Intervjun inleds med att vi frågar om vilken roll respondenten har på företaget, samt hur länge han eller hon har arbetat där. Detta gör vi för att säkerställa att respondenten i fråga har kunskap om företagets medvetenhet om risker och hot som finns riktat mot smarta mobiltelefoner. Därefter frågar vi efter en generell policy för mobiltelefoner, för att ta reda på om företagen har tänkt på andra aspekter av mobiltelefonanvändande, utöver de som gäller säkerheten kring smarta mobiltelefoner.

Utifrån de fem riskerna som vi nämner i undersökningsmodellen (Figur 2,2.), har vi skrivit frågor som vi anser vara relevanta för att bedöma om företagen vi intervjuar har en riskmedvetenhet kring säkerheten för smarta mobiltelefoner, och i så fall vilka risker. Utifrån det har vi sedan möjlighet att ställa följdfrågor som behandlar de olika risker, eller i de fall då företaget inte har någon riskmedvetenhet, ställa frågor om anledningen till detta.

3.4 Genomförande

Som tidigare nämnt har intervjuerna genomförts både vid möte med respondenten samt över telefon. I samtliga fall har intervjuerna spelats in och sedan transkriberats. Valet att spela in intervjuerna var enkelt, då detta innebär att vi inte missar något av det som respondenten berättar, och vi har möjlighet att i efterhand spela upp intervjun om det är något vi är osäkra på.

Respondenterna har fått möjlighet att förbereda sig på intervjun om de så önskar, då vi i förhand skickat ut vår intervjuguide. Därmed kommer inte frågorna som en överraskning för respondenten och han eller hon slipper känna osäkerhet över vad intervjun kommer att handla om. Intervjuerna har tagit ungefär 30 minuter att genomföra.

3.5 Transkribering

För att göra vår transkribering så överskådlig som möjligt har vi valt att lista frågorna i den följd som de ställdes under intervjuerna. Till varje fråga listas svaret bredvid som respondenten svarat i samma följd. Vi har i största mån följt den intervjuguide vi skapat för att göra det lättare att analysera resultatet. Upprepningar och hummanden har inte tagits med då det inte är av relevans.

Utifrån vår undersökningsmodell (figur 2,2.) har vi gjort vår egen kodmodell (figur 3,1.) där varje risk tilldelats en bokstav. Dessa bokstäver används sedan i våra transkriptioner och beskriver relevansen hos varje fråga samt vilket område de berör.

Kod:	Risk:	Kod:	Risk:
A	Förlust av enhet	E	Intrång
B	Återvinna enhet	R	Relevant info.
C	Malware	IR	Irrelevant info.
D	Avlyssning		

Figur 3,1. Kodmodell för transkribering

3.6 Analysmetod

Vid analysen av vår kvalitativa data har vi börjat med att registrera intervjuerna genom att spela in och transkribera dessa. Detta ger oss ”tjocka beskrivningar” vilka är alldeles för omfattande (Jacobsen, 2002). För att lättare skapa en överblick över informationen vi samlat in har vi därefter kategoriserat informationen enligt vår kodmodell (figur 3,1.). När informationen har kategoriserats, börjar vi tolka och analysera datan utifrån de fem riskerna vi valt att använda oss av.

3.7 Validitet och Reliabilitet

För att validera vår undersökning har vi utgått från Jacobsens (2002) två krav för insamlingen av empiriskt material. De två kraven är:

1. Empirin måste vara giltig och relevant (Validitet)
2. Empirin måste vara tillförlitlig och trovärdig (Reliabilitet)

För att uppnå en bra validitet har vi grundat vår intervjuguide på vår undersökningsmodell (figur 2,2.). Därmed säkerställer vi att vi mäter det vi vill mäta. Intervjuguiden är i sin tur uppbyggd på öppna frågor och baserad på de fem risker som också utgör vår undersökningsmodell (figur 2,2.). För att säkerställa en reliabilitet eller en stark tillförlitlighet, har vi spelat in och transkriberat samtliga intervjuer för att garantera att vi inte går miste eller förvränger uttalad information. Transkriptionerna har även skickats till respondenterna för validering.

Löpande genom uppsatsens gång har vi lagt stort fokus på att konstant referera till källor vi använt oss av och hämtat information ifrån. På så vis har vi tillfört uppsatsen hög validitet genom att hela tiden försäkrat oss om att det vi skriver är relevant.

3.8 Etik

Under uppsatsens gång kommer vi hela tiden att låta våra respondenter och de företag de representerar vara anonyma. Detta är dels för att personen i fråga inte ska försättas i en besvärlig situation gentemot sitt företag, men också för att företaget som helhet inte ska utsättas för några säkerhetsrisker. Anonymitet har i de flesta fall även varit ett krav från respondenten, av samma anledningar som vi själva valt att hålla dem anonyma. Vi kommer också att noggrant referera till den litteratur som vi använt oss av under uppsatsens utformande för att inte kränka författarna till litteraturen.

4 Empirisk presentation och analys

I detta kapitel avser vi gå igenom den respons och det material vi samlat in från våra intervjuer och analysera detta. Vi har fortsatt att använda oss av de fem risker vi använt oss av löpande genom hela uppsatsen för att underlätta förståelsen och läsbarheten. Till varje risk har vi hämtat in några av de svar vi fick under intervjun med de olika respondenterna. I slutet av varje stycke analyserar vi empirin och drar några slutsatser om utfallet.

Vi har intervjuat fyra stycken företag och fyra olika respondenter. Vid början av varje intervju har vi inlett med att fråga vilken roll personen har i företaget och hur länge de har jobbat där. Respondent A är HR- chef och har jobbat inom företag A i 12 år (Respondent A, fråga 0 och 1). Respondent B är IT- Chef och har jobbat inom företag B i sju år men har varit IT- chef två av de åren (Respondent B, fråga 0 och 1). Respondent C är platschef och har ett IT ansvar inom företaget samt har arbetat på företaget i två år (Respondent C, fråga 0 och 1). Respondent D är tekniskt kundansvarig och har jobbat inom företaget i fem år men har varit kundansvarig i lite mer än ett år (Respondent D, fråga 0 och 1).

Efter varje citat vi lagt in löpande i texten hänvisar vi till var i bilagan man kan finna varje citat. Exempelvis *Respondent A, Fråga 11,* finner man i bilagan för respondent A och svaret i fråga 11.

4.1 Förlust av enhet

Förlust av enhet kan ske på framförallt två olika sätt, stöld eller att någon tappar bort sin enhet. Vid stöld är det av självklara skäl som så, att enheten oftast inte lämnas in till polisen och därmed kommer till rätta igen. Om en person tappar bort sin enhet finns dock möjligheten att han eller hon får tillbaka den, om personen som hittar den lämnar in den till exempelvis polisen. Att skydda sig mot förlust av enhet är svårt, däremot finns det flera åtgärder som kan vidtas i förebyggande syfte, för att skydda enheten när den väl är förlorad (se kapitel 2, avsnitt "Förlust av enhet").

Våra respondenters åtgärder vid förlust av enhet skiljer sig en hel del, från att inte göra någonting utom möjligtvis polisanmäla händelsen vid stöld till att göra en "remote wipe"(Fjärrstyrt radera informationen på enheten), om detta är möjligt. I de båda nedanstående fallen använder sig företagen mestadels av iPhones, vilket innebär att "remote wipe"-funktionen finns inbyggd redan från start. Trots detta är det inte något som utnyttjas av båda företagen:

> *"Det beror på, det var en person som blev rånad på sin mobil ute på stan och då polisanmäler man ju. Men jag har aldrig varit med om att någon gjort av med sin telefon." (Respondent A, fråga 11)*

> *"Då utför vi en "remote wipe" först och främst. Så en "remote wipe" initieras men det är ju inte alltid de fungerar eftersom om de är stulna så tar de ofta ut simkorten och då har vi inte kontakt med telefonen längre. Men sen polisanmäler vi det och sen köper vi en ny telefon. Det är inte mer än så." (Respondent B, fråga 13)*

Respondent C och Respondent D använder sig av telefoner från flera olika tillverkare och operativsystem, vilket innebär att det inte alltid finns möjlighet från start att utföra "remote wipe". I de fallen måste alltså programvara för detta installeras på telefonerna, något som endast Respondent D verkar vara medveten om.

> *"Ja vi har åtgärder. Vi spärrar telefonen om vi kan det. Där är ju problemet att det hänger på leverantören. Har man något nummer för den.. Vi kan ju spärra telefonabonnemanget, men vi kan väl egentligen aldrig spärra själva telefonen." (Respondent C, fråga 9)*

> *"Ja, då är det "Remote wipe" som gäller. Då blåses hela telefonen. Det kan varje användare göra via sin Outlook webaccess. Då blåses den och låses den." (Respondent D, fråga 8)*

Två av fyra respondenter har alltså inga åtgärder för att skydda den data som kan finnas på telefonerna i form av faktiska dokument, men också i form av e-post. Respondenternas anledningar för att inte ha några åtgärder skiljer sig dock åt. Respondent A menar sig inte ha haft någon anledning att införa några åtgärder för detta, även om det är något som respondenten medger bör finnas i en framtida policy (Respondent A, fråga 12). Respondent C verkar däremot, enligt citatet ovan, vara omedveten om de åtgärder som finns att vidta. I båda fallen handlar det dock om att användningen av smarta mobiltelefoner som företagstelefoner är så pass ny att säkerhetsplaner och riktlinjer för att hantera förlust av sådana enheter inte hunnit utvecklas än.

De två företag som redan nu har säkerhetsplaner i form av en policy för att hantera förlorade enheter använder sig av möjligheten att utföra "remote wipe" på sina telefoner. Detta gäller både för de som använder iPhones samt för de som använder exempelvis Android-telefoner. Respondent D, vars företag tillåter flera olika sorters smarta mobiltelefoner, berättade dock att ett av kraven på telefonerna är just att det ska vara möjligt att utföra "remote wipe".

Möjligheten att låsa sin telefon med hjälp av en pinkod eller något liknande har funnits sedan länge, och är inget nytt för smarta mobiltelefoner. Detta kan också utgöra ett skydd vid förlust av enhet, då det försvårar för obehöriga att få åtkomst till innehållet i telefonen. Trots att

denna enkla åtgärd är möjlig på i stort sett alla telefoner är det endast två av fyra intervjuade företag som har detta som krav:

> *"Nej det har vi nog inte, tror jag, men vi borde haft det och vi borde haft det på våra telefoner också." (Respondent A, fråga 22)*

> *"...Man måste ha låskod på den, vi kan "remote wipa" dem, vi kan kolla positionerna på dem, inte för att vi gjort det någon gång men vi kan och vi kan kräva lösenkodbyten osv. så det är inget användarna ser egentligen, de bara tänker att så är det så det sköts helt via servern trådlöst..." (Respondent B, fråga 7)*

> *"Nej. Den säkerheten vi har för telefonen finns inne i vårt nät med inloggning osv." (Respondent C, fråga 13)*

> *"Ja, det innebär att telefonen låser sig, du måste slå in din pinkod igen efter tio minuter om du inte använt telefonen." (Respondent D, fråga 5)*

Majoriteten av företagen i undersökningen är eniga om sin syn på förlust av enhet som ett hot mot den information som kan finnas på telefonerna. Tre av fyra respondenter svarar att de har, eller borde ha, åtminstone ett kodlås på telefonen för att skydda den om den skulle tappas bort eller bli stulen. Det är endast en respondent som inte nämner kodlås som en säkerhetsåtgärd. För den respondenten finns säkerheten istället i själva nätverket, med inloggning. Detta skyddar dock inte den information som redan har hämtats från nätverket och ligger lagrad på telefonen, och ett kodlås är därför något som även respondent C bör överväga.

4.2 Återvinna enheten

Återvinning av enheter har idag blivit ett allt mer utbrett alternativ eftersom detta inte bara sparar på miljön utan också erbjuder att ännu ej uttjänta enheter kan fortsätta användas av andra personer. Att återvinna sin enhet är däremot något man bör vara försiktig med då information sparad på enheten kan återställas och komma i fel händer (se kapitel 2, avsnitt "Återvinna enheten"). Det är därför en generell säkerhetsrisk man bör överväga innan man skickar in sin uttjänta eller inte längre använda telefon till ett återvinningsföretag. Efter respektive intervju med våra respondenter inser vi att riskerna med att skicka in enheterna till återvinningsföretag bidrar till att många av de intervjuade företagen helt låter bli att skicka in dem och lagrar istället sina uttjänta enheter i en låda i källaren. Några av våra respondenter anser sig inte ha tillräckligt med tid för att på ett säkert sätt radera innehållet vilket innebär att telefonen formateras flera gånger i följd. Detta för att göra det så svårt som möjligt att kunna återskapa informationen igen. En process många företag anser är alldeles för tidskrävande och utan någon större vinning för företaget då ersättningen för en uttjänt enhet sällan är någon större summa pengar och därför inte motiverad för företaget att ödsla tid på. En av

respondenterna svarade:

> *"...Allt ligger på en rimlig nivå, allt är tidskrävande. Bara att återställa 60 telefoner tar tid och ännu mer tid hade det tagit att återställa dem fem gånger för att göra det på ett säkert sätt och det har man inte tid med." (Respondent B, fråga 15)*

En gemensam regel företagen i fråga har, är att de anställda sällan själva raderar innehållet på enheterna innan dessa lämnas in på reparation eller säljs vidare och återvinns. Ett visst företag har som policy att de anställda inte själva får radera företagsinformation från sina enheter utan detta ska en ansvarig i företaget göra åt dem.

> *"Det går också tillbaka till den generella IT-policyn. Kravet där är att lämna över den icke-raderad. Dom får inte själva radera företagets material, det materialet äger vi. Alla har ju någon form av privata saker i sin dator, och det raderar man själv, men det som är jobbrelaterat vill vi kunna kontrollera och vara hundra på att vi har kvar. Detsamma gäller i princip för mobilen." (Respondent A, fråga 15)*

Två andra företag har i stort sett samma syn på raderingen av information även om det inte är integrerat i deras policy utan fungerar mer som en oskriven regel inom företaget och bland dess anställda.

> *"...Skickar vi in dem på reparation eller något liknande så återställer vi dem alltid fullt innan vi skickar in dem. Och det är samma, skulle vi slänga dem eller sälja dem vidare till någon återvinning så skulle vi "wipa" dem innan." (Respondent B, fråga 15)*

> *"...Vi följer samma regler som vi har med datorerna. Vi fabriksåterställer dem. Men, vi lämnar nästan aldrig över en telefon. Det ska vara om man slutar tidigt och då finns det en värdig telefon som en ny anställd kan få, men annars är den så sliten och omodern så att vanligtvis slänger vi bort dem." (Respondent C, fråga 11)*

Generellt för företagen vi intervjuat är att enheterna sällan går i arv såvida en anställd inte slutar tidigt efter denna blivit anställd och enheten den anställda hade, fortfarande är modern och brukbar. Eftersom marknaden för mobila enheter ser ut som den gör och det hela tiden kommer nya bättre alternativ anser respondent C att gamla enheter inte är till fördel för företaget att använda då detta kan ses som ett hinder för den anställde som innehar en äldre enhet. Ett annat generellt problem med gamla enheter är också att de inte har samma säkerhetsstandarder som nyare enheter har samt att de företag vi intervjuat gärna är konsekventa och helst använder sig av en viss typ eller märke av smarta enheter med likadana operativsystem. Detta främst för att öka kompabiliteten och driftsäkerheten så att enheterna

smidigt fungerar med varandra och med företagets lösningar i form av synkroniseringsservrar och dylikt.

> *"...Vi lämnar nästan aldrig över en telefon. Det ska vara om man slutar tidigt och det då finns en värdig telefon som man kan få, men annars är den så sliten och omodern så att vanligtvis slänger vi bort dem."*
> *(Respondent C, fråga 11)*

Efter att ha gjort intervjuerna har vi fått en förståelse för hur företag ställer sig till återvinnandet av smarta enheter. Majoriteten av företagen har inte tänkt särskilt ingående om hur de ska hantera sina uttjänta enheter utan de flesta förvarar dem i ett förråd för att vid ett senare skede kasta dem. Många av företagen är medvetna om att information kan återställas från en enhet som blivit raderad men de flesta av respondenterna ser ändå inte detta som ett direkt hot. Troligtvis eftersom de inte bryr sig om att sälja vidare sina enheter men också i många fall eftersom de anser att informationen som lagrats på enheterna inte är av större värde och inte kan skada företaget i fråga i någon större utsträckning.
Vidare svarade många av respondenterna att det tar för mycket tid att radera informationen på enheterna till den grad då det inte längre är möjligt att återställa någon information. Tid är sällan någon överskottsvara i företag och argumentet är därför befogat. En funktion som tillåter bättre, snabbare och en mer permanent radering av informationen på enheterna hade varit till fördel för företag då detta bidragit till en säkrare återvinning och i sin tur att fler företag faktiskt återvinner sina uttjänta enheter vilket är bättre för miljön på många olika sätt. Kontentan är alltså att företag i många fall är medvetna om vilka risker det finns med att återvinna uttjänta enheter och dels på grund av detta avstår ifrån att återvinna helt och hållet.

4.3 Malware

Malware är ett samlingsord för mjukvara som är skapat för att orsaka skada på datorer, nätverk eller servrar. I takt med att smarta mobiltelefoner får samma kapacitet som vanliga datorer blir även dessa hotade av malware. Malware kan ta formen av virus, trojanska hästar, maskar och spyware. Virus är ett program som installerar sig i ett så kallat värdprogram och kopierar sig själv när värdprogrammet körs. Viruset kan exempelvis åstadkomma skada på hårddisken. Maskar är själv-reproducerande mjukvara som automatiskt sprids via nätverk och andra anslutningar. Trojanska hästar är program som ser ofarliga ut men som gömmer skadlig kod som kan öppna upp bakdörrar för hackare. Spyware är mjukvara som samlar in och delar med sig av personlig information till obehöriga. (se kapitel 2, avsnitt "Malware")

I takt med att företag allt mer använder sig utav smarta mobiltelefoner ökar också risken att bli utsatta för olika sorters malware (Juniper, 2012). Osborne beskriver hur en säkerhetspolicy gällande informationssäkerhet kan se ut. Där nämns "Internetanvändning" som en punkt att beskriva hur användandet bör genomföras (Osborne, 2006).

Respondenterna har olika svar gällande de hemsidor som är tillåtna att besöka via telefonen

men generellt har de inga direkta restriktioner på vilka sidor som får besökas i deras säkerhetspolicy för smarta mobiltelefoner. Istället kan det vara IT-policyn som ska vara en riktlinje för detta.

> *"Ja det gör ju det, men egentligen bör det ju skrivas något specifikt för mobiltelefoner för det skiljer sig ganska mycket åt."*
> *(Respondent A, fråga 6)*

> "*I korta drag kan man väl säga att den inte får användas för piratkopiering, pornografi, extrempolitik och sabotage. Och det är samma som för vår vanliga IT-policy, att som anställd får man inte förekomma i forum som har med detta att göra.." (Respondent C, fråga 4)*

För att bilda oss en uppfattning om hur stor användningen av antivirusprogram är frågade vi respondenterna hur de skyddar sig mot malware och om de använder sig utav antivirusprogram. Alla svar pekar åt samma riktning, antivirusprogram används inte.

> *"Ingenting." (Respondent A, fråga 18)*

> *"Inte ett smack, förutom det som eventuellt finns inbyggt i en iPhone." (Respondent A, fråga 19)*

> *"Vi har iOS på dem! Det är det enklaste och bästa. Nya Windows mobile, eller Windows phone som den heter nu, hade också varit tillämpbar eftersom den också är väldigt bra, den har en väldigt bra säkerhetsmodell." (Respondent B, fråga 16)*

> *"Vi hade inga virusskydd. Och det var väl den stora anledningen till varför vi gick ifrån Android också." (Respondent B, fråga 16)*

> *"Nej, vi har inget antivirusprogram." (Respondent C, fråga 12)*

> *"Nej, inget sådant på mobilerna än så länge. Det är något som vi håller på att kika på. Det kommer i stort sett komma när som helst." (Respondent D, fråga 15)*

Nedladdning av filer eller applikationer via internet kan sprida malware (se kapitel 2, avsnitt "Malware"). För att minska riskerna för det, kan restriktioner i en säkerhetspolicy för vad som får laddas ner till mobiltelefoner beskrivas. Frågan gällande dessa restriktioner ställdes till samtliga respondenter och svaren blev likartade.

> *"Nej, så är det ju, vi har inga restriktioner för vilka applikationer som får installeras, men å andra sidan har ju Apple rätt så hårda restriktioner själva så man kan ju inte lägga in precis vad som helst." (Respondent A, fråga 27)*

> *"Den kontrollen gör Apple till oss. Det är väl där Google och Android är lite sämre." (Respondent B, fråga 22)*

> *"Man kan också säga att det skiljer sig lite ifrån datorpolicyn som säger att man inte får lov att installera privata program på din dator, även om du får lov att ta hem den får du inte lov att installera dina privata spel eller vad du nu har för något. När det gäller smartphonen har vi en policy som säger att du får lov att göra det." (Respondent C, fråga 4)*

Frågan ställdes till respondent D om det var fritt fram för de anställda att ladda ner vad de ville på deras smarta mobiltelefoner.

> *"Ja." (Respondent D, fråga 17)*

Vi kan se att de som endast använder sig utav Apples iPhone litar till stor del på att Apples restriktioner gällande den mjukvara som kan laddas ned ifrån "App Store" är tillförlitlig. I motsats till Googles "Android Market" kontrollerar Apple de applikationer som laddas upp mot "App Store" innan de blir tillgängliga för Apple-användarna (se kapitel 2, avsnitt "Operativsystem").

En anledning till att samtliga respondenters säkerhetspolicys eller riktlinjer gällande smarta mobiltelefoner verkar vara allmänt tunna, kan bero på att medvetenheten i företagen angående de hot och risker som finns mot smarta mobiltelefoner generellt är låg. Frågan ställdes om respondenterna var medvetna om de olika hot som smarta mobiltelefoner kan utsättas för.

> *"Delvis, men inte jättemycket." (Respondent A, fråga 10)*

> *"Alltså vi har gjort det väldigt lätt för oss i och med att vi har iPhones då dessa är säkra i grund och botten. Sen finns de vissa som synkar från Android, det handlar om en eller två personer, och där är det ju kanske lite mer riskfyllt. Men man håller ju en allmän koll på säkerhetssituationer så att säga och kommer det något som riktar in sig på just stöld av synkroniseringsuppgifter eller spionage på mail och så*

vidare, då kanske man får spärra Androidenheterna...” (Respondent B, fråga 12)

“.... Man gör ju en riskbedömning löpande på den informationen som finns på marknaden. Vi resonerar lite så att är det något stort och brett virus som kommer och söker allting, är vi kanske ett mål. Men vi känner oss inte som ett mål för någon som gör ett ”Custom made” virus, alltså ett anpassat virus bara för oss...” (Respondent B, fråga 12)

“Alltså nä. Det vore kaxigt att svara ja på det. Vi är naturligtvis inte det till fullo, det är vi inte. Visa delar vet vi om och vad jag har skrivit i policyn är att vi, i en smartphone inte ska lägga företagsinformation, vi ska inte lägga word-dokument som är relaterat till våra kunder, hemlig information.” (Respondent C, fråga 6)

“Ja, det är vi. Och det börjar bli allt mer. Den enda policyn vi har nu går på via Exchange. Vi har inget extra ”Management Device” som vi skjuter på mobilerna än så länge. Det är något vi håller på att kolla på och det ligger ganska högt upp på prioriteringslistan.” (Respondent D, fråga 7)

Som vi ser ifrån svaren är det respondent D som tydligt säger att de är medvetna om de hot och risker som finns. Övriga respondenter är medvetna om att det finns hot och risker mot smarta mobiltelefoner men inte i vilken utsträckning.

Efter att ha ställt frågor gällande malware till respondenterna har vi bildat oss den uppfattning att det är sunt förnuft för användarna av de smarta mobiltelefonerna som gäller. Restriktionerna är överlag låga men användarna bör använda sunt förnuft när de använder sin enhet. Vidare kan vi fastställa att de flesta företag vi intervjuat har någon sorts förståelse för de hot och risker som finns men den är överlag ganska låg. Användandet av antivirusprogram hos respondenterna är nästan obefintligt. Det kan bero på att de har stor tillit för Apples säkerhetsmodell, både när det gäller operativsystemet och säkerhetskontrollen gällande de applikationer som finns tillgängliga på App Store.

4.4 Avlyssning

Avlyssning är ett hot inte många företag är medvetna om finns. Avlyssning kan som nämnt i tidigare avsnitt om avlyssning (se kapitel 2, avsnitt “Avlyssning”), ske utan någon som helst vetskap eller förvarning om att användaren är utsatt för detta. Vanligast är det att den skadliga malwaren i form av avlyssning eller “eavesdropping” som termen heter på engelska, tar sig in i den mobila enheten genom mjukvara i olika form. Denna mjukvara kan vara applikationer användaren laddar ner i god tro att mjukvaran i fråga utger sig för att vara det den är beskriven att vara, eller mjukvara som överförs via ett trådat eller trådlöst medium utan användarens godkännande. Avlyssning anser vi utgör ett klart hot gentemot företag på så vis

att företagsinformation som byts ut över t.ex. ett samtal, kan relativt enkelt med hjälp av rätt sorts mjukvara installerad på den utsattas mobiltelefon, "stjälas" och komma i fel händer och användas i sammanhang där det kan skada företagets integritet och kanske till och med affärskoncept. Ett konkret exempel hade varit om t.ex. en anställd på Coca-cola haft ett telefonsamtal om receptet på drycken och detta skulle bli avlyssnat och därmed stulet. Detta hade naturligtvis skadat Coca-cola som verksamhet och som varumärke.

Vår intervjuguide innefattar en fråga som handlar om avlyssning och hur företag skyddar sig mot dessa. Nedan plockar vi ut några exempel på svar vi fick från de olika respondenterna och hur de ställer sig till avlyssning som ett hot:

Frågan: Hur skyddar ni er mot avlyssning och intrång?

> *"Ingenting" (Respondent A, fråga 18)*

> *"Nja, man kan ju resonera såhär: Man måste jämföra kostnaden för att skydda information, eller data i vårt fall, jämfört med kostnaden för att bli av med den. Vi har liksom ingenting som skulle vara så farlig om det kom ut. Vi har ingen produktutveckling, som Microsoft till exempel, inga patent, så vi har inga sådana grejer utan det är ju vidareutveckling av kunders system." (Respondent A, fråga 25)*

Respondent A anser att vidta åtgärder för att skydda sig mot avlyssning inte är relevant för företaget i fråga då dessa inte har någon direkt patentskyddad produkt som genom avlyssning eller intrång kan skada företaget om det skulle nå konkurrenterna. Företaget har därför svarat "ingenting" på frågan om hur de skyddar sig mot intrång och avlyssning.

Ett annat företag svarade enligt följande på frågan vi ställde:

> *"...inga speciella skydd" (Respondent B, fråga 20)*

> *"Nej, vi har inget antivirusprogram." (Respondent C, fråga 12)*

Följande företag svarar enligt följande på frågan "har ni mycket känslig information på telefonerna som i fel händer kan skapa problem för företaget?"

> *"Ja, i och med att många synkar sin mail och den innehåller ofta information som kan vara företagshemlig." (Respondent D, fråga 11)*

Följaktligen svarar respondenten enligt följande på frågan angående avlyssning:

> *"Det blir samma svar som jag sa innan. Vi har inget sådant än så länge." (Respondent D, fråga 14)*

Respondenten hänvisar alltså till ett tidigare svar om företaget är medvetna om vilka hot som finns till smarta mobiltelefoner där respondenten svarar att de är medvetna om detta och att det just nu ligger ganska högt på prioriteringslistan:

> *"Ja, det är vi. Och det börjar bli allt mer. Den enda policyn vi har nu går på via Exchange. Vi har inget extra "Management Device" som vi skjuter på mobilerna än så länge. Det är något vi håller på att kolla på och det ligger ganska högt upp på prioriteringslistan." (Respondent D, fråga 7)*

Företag D är alltså fullt medvetna om att det finns ett flertal hot som är benägna att stjäla företagsinformation som företaget i fråga anser i vissa fall kan vara affärshemligheter. Företaget har kommit så pass långt att de börjat tänka över alternativ om hur de ska implementera en framtida skyddsplan till företagets mobila enheter. Men än så länge har företaget inga som helst virusskydd på de smarta mobiltelefonerna i verksamheten.

Fråga: Inget virusprogram?

> *"Nej, inget sådant på mobilerna än så länge. Det är något som vi håller på att kika på. Det kommer i stort sett komma när som helst." (Respondent D, fråga 15)*

Vi har efter intervjuerna insett att varje företag verkar ha gjort någon form av riskbedömning där de antingen anser att den information som hanteras utav mobila enheter inte kan komma att skada företaget om denna läcker ut, eller att den information som skulle kunna skada företaget inte hanteras av mobila enheter. Övriga företag tillåter att känslig information hanteras av företagets mobila enheter men att de än så länge inte har vidtagit några åtgärder gällande virusskydd eller andra skydd som skulle minska risken för informationsläckage. Orsaken till att företagen inte har några klara direktiv om vilka skydd som ska/bör användas tror vi kan bero på att företag inte är tillräckligt informerade om hur utspritt virus till mobila enheter egentligen är. Jämför man med hur noga informationen spritts till privatpersoner angående datorer och hur viktigt det är att ha virusskydd på dessa ligger informationen och utvecklingen av virusskydd för smarta enheter långt efter vad den relativt sett borde göra. Detta kan i sin tur bero på att ingen stor och övergripande attack som nått allmänheten inträffat än vilket i sin tur leder till ett minskat riskmedvetande bland företag och privatpersoner generellt.

4.5 Intrång

En smart mobiltelefon kan idag utsättas för försök till intrång på en mängd olika sätt. Är telefonen låst med pinkod kan en obehörig med lite tur gissa sig till denna kod, och sedan få fri tillgång till telefonens innehåll. SMS, MMS, Bluetooth och synkronisering med datorer kan även det vara riskfyllt för smarta mobiltelefoner då skadlig kod kan överföras till telefonen som vid körning gör det möjligt för obehöriga att ta sig in i telefonen via en sorts ”bakdörr”. (se kapitel 2, avsnitt ”Intrång”)

> *”Ingenting.” (Respondent A, fråga 18)*
>
> *”...Man måste ha låskod på den..” (Respondent B, fråga 7)*
>
> *” Nej, vi har inget antivirusprogram.” (Respondent C, fråga 12)*
>
> *” ...och den måste klara av att ha företagslås på sig.” (Respondent D, fråga 4)*
>
> *” Nej, inget sådant på mobilerna än så länge. Det är något som vi håller på att kika på. Det kommer i stort sett komma när som helst.” (Respondent D, fråga 16)*

Att skydda sig mot intrång genom att använda sig av någon sorts låskod är något som endast två utav fyra intervjuade företag har nedskrivet i någon form av policy eller säkerhetsplan. Kodlåsen skyddar dock inte mot den skadliga kod som kan öppna upp ”bakdörren” till en telefon, och här krävs istället ett större medvetande hos telefonens användare. Att användaren inte ska öppna filer från okända avsändare, inte tillåta Bluetooth anslutning med okända enheter samt att inte synkronisera telefonen med en dator som kan bära på skadlig kod är saker som bör stå med i en eventuell policy för hur telefonen ska användas. Skulle användaren ändå öppna och köra en fil som innehåller skadlig kod kan ett anti-virusprogram skydda telefonen mot intrång. Detta är dock något som inget utav företagen använder sig av. Anledningen kan vara en låg medvetenhet om riskerna. I avsnittet om malware behandlas detta mer ingående, då den typen av skadlig kod faller under kategorin malware. Kortfattat kan dock sägas att företagen som använder sig av iPhone, respondent A och B, litar på Apples kontroll av den programvara som läggs upp i App Store, respondent C är inte medveten om virus till smarta mobiltelefoner (se citat nedan), vilket såklart är ett skäl till att det inte omnämns i någon policy och respondent D menar på att det är något som är på väg att införas inom en snar framtid, vilket tyder på att de är medvetna om risken, men ännu inte har vidtagit några åtgärder för att skydda sig.

> *” Jag har aldrig hört talas om att det finns något virus till smartphone men jag vet att det finns virusskydd..” (Respondent C, fråga 7)*

5 Fördjupad analys och tolkning

I följande kapitel återkopplar vi respondenternas svar på intervjuerna med den teori vi tog upp i litteraturkapitlet (kapitel 2). Återigen följer vi i detta kapitel de risker vi tagit upp tidigare för att på så sätt fortsätta skapa en djupare förståelse för ämnet och de risker vi valt att behandla. I detta kapitel tolkas och analyseras vidare respondenternas svar för att djupare analysera respektive företag och dess säkerhetsrisker samt eventuella befintliga åtgärder.

5.1 Förlust av enhet

Vid analys av respondenternas svar beträffande de risker som finns vid förlust av enhet framgår det att det inte är en självklarhet att på något sätt skydda sig mot dessa. Varken krav på kodlås eller möjligheten att utföra "remote wipe" finns skrivet i en policy, säkerhetsplan eller som riktlinjer hos två av fyra intervjuade företag. Detta trots att riskerna som är kopplade till förlust av enhet kan vara förödande för ett företag som lagrar information om företaget och dess affärer på sina smarta mobiltelefoner, vilket majoriteten gör i form av e-post och andra dokument (se kapitel 2.1.2). Ett företag, representerat av respondent A, menar på att den information som finns på de smarta mobiltelefonerna inte skulle göra någon större skada om den läckte ut. Kostnaden för att skydda informationen skulle därför bli större än kostnaden av att informationen läcker ut, enligt respondenten. Respondenten medger dock att ett kodlås bör vara obligatoriskt på företagets smarta mobiltelefoner. Anledningen till att företaget som representeras av respondent C inte har vidtagit några åtgärder för att skydda sig vid förlust av enhet är en omedvetenhet om de åtgärder som finns att vidta.

Vad gäller de olika telefonernas operativsystem är de intervjuade företagen jämnt fördelade, två av dem använder sig av Apples iOS medan de andra två även tillåter Android och Windows Mobile. De som har valt att använda sig av iOS påstår att en av huvudanledningarna till detta är just säkerhetsaspekterna som följer med operativsystemet, vilket saknas i övriga operativsystem (se kapitel 2.1.3). Detta är dock ingen garanti för att företagen använder sig av de säkerhetsverktyg som finns. De som använder sig av andra operativsystem än iOS måste själva installera och konfigurera applikationer för exempelvis "remote wipe". Att utföra ett sådant installationsarbete kan vara avskräckande för den som inte har gjort det förr, eller vet exakt hur det ska gå till.

Hälften av företagen har alltså en policy för att skydda sig vid förlust av enhet, och andra hälften saknar riktlinjer. Samtliga verkar dock vara medvetna om att förlust av enhet innebär en risk, och de två som inte redan har en policy eller säkerhetsplan, verkar vara på god väg att införa en.

5.2 Återvinning

Genom att analysera våra respondenters svar och de företag de representerar kan vi konstatera att återvinning av företagens enheter är något företagen inte tänkt på eller finner någon vinning i att utföra. Framför allt grundar detta sig i att majoriteten av företagen anser att den manuella processen att radera information från enheterna på ett sådant sätt att det blir nästintill omöjligt att återskapa den, är alldeles för tidskrävande och medför ingen fördel för företagen utan det blir lättare att helt enkelt förvara enheterna i en låda för att sedan göra sig av med dem på ett sätt som gör att ingen annan kommer i kontakt med dem (se kapitel 2.2.2). Genom analys av intervjuerna verkar det inte som att företagen vi intervjuat planerat att införa någon form av policy för hur mobilerna ska och bör återvinnas. Processen är helt enkelt alldeles för tidskrävande vilket medför att respondenterna väljer att spara på de uttjänta enheterna istället för att sedan kasta dem.

5.3 Malware

Vi kan efter analys av respondenternas svar gällande malware konstatera att de överlag innehar väldigt svaga restriktioner för hur de ska använda sina smarta mobiltelefoner. Malware kan som tidigare beskrivits, spridas på flera olika sätt och skapa stor skada för exempelvis företag (se kapitel 2.2.3). Ett av spridningssätten är när en användare laddar ner skadliga filer till sin smarta mobiltelefon, exempelvis olika applikationer. Därför bör internetanvändningen beskrivas i en säkerhetspolicy för att minska riskerna och hoten som malware utgör (se kapitel 2.3). Enligt samtliga respondenter finns det inga restriktioner i deras säkerhetspolicy gällande detta. De respondenter som till största del använder sig utav iPhone har väldigt stor tillit till Apples säkerhetsmodell gällande App Store och litar på att de kontroller som görs där är tillräckligt säkra.

Vidare saknar samtliga respondenter någon form av antivirusprogram. Även här riktas stor tillförlit till Apples säkerhetsmodell gällande App Store samt iOS för de respondenter som använder iPhone. En anledning till att avsaknaden av antivirusprogram på smarta mobiltelefoner är så stor kan bero på att medvetenheten gällande de hot och risker de utsätts för är relativt låg. Två av respondenterna säger rakt ut att de har låg medvetenhet om de risker och hot som finns. En av respondenterna medger att de är medvetna till den grad att de inte ska lägga känslig företagsinformation som exempelvis hemlig information eller information om kunder på deras smarta mobiltelefoner. Vidare nämns hos en respondent att de är medvetna om riskerna och ser Apples säkerhetsmodell som tillförlitliga.

5.4 Avlyssning

När frågan ställs om företagen ser avlyssning som ett hot svarar majoriteten att det inte klassas som ett hot enligt dem och mångdelen har inte hört talas om begreppet förut. Majoriteten av respondenterna anser att informationen som hanteras på de smarta mobiltelefonerna inom verksamheten inte är av den karaktär att en förlust av denna skulle

skada företaget på något utbrett sätt, utan klassas som en mindre risk. När frågan tas upp om respondenterna känner till att en smart enhet kan bli avlyssnad eller utsatt för "eavesdropping" (se kapitel 2.2.4), har samtliga intervjuade antingen aldrig hört talas om detta fenomen alternativt aldrig brytt sig om fenomenet som en eventuell risk. Detta tyder på att företag inte är tillräckligt medvetna om vilka risker de utsätter sig själva för vid användandet av smarta enheter som ett verktyg inom företaget. När fenomenet förklaras för respektive respondent håller de fast vid sitt uttalande om att de anser att risken att något sådant kommer hända är en minimal risk och inte intressant för företagen i fråga att lägga ner varken tid eller pengar på att skydda sig emot.

5.5 Intrång

De intervjuade företagen har överlag dåligt skydd mot intrång, endast två företag har obligatorisk låskod på sina smarta mobiltelefoner. Skydd mot intrång via Bluetooth, dator-synkronisering, SMS och MMS i form av virusskydd saknas dock hos samtliga. Troligtvis beror detta på att inget av företagen ser sig själva som en måltavla för intrång, och därför aldrig ens har reflekterat över möjligheten att någon skulle försöka sig på att göra intrång i företagets mobiltelefoner. Till viss del stämmer detta, enligt oss, men företagen kan ändå utsättas för intrång som är mer allmänt inriktade och inte bara har ett specifikt företag som måltavla. En policy för hur de anställda får använda sina smarta mobiltelefoner kan vara ett bra sätt att definiera hur ett bra skydd mot intrång ska utformas (se kapitel 2.3).

Dålig medvetenhet, samt en känsla av att "det händer inte oss" verkar vara anledningarna till att företagen inte vidtar några större åtgärder för att skydda sig mot intrång. Ett visst grundskydd som skyddar mot allmänna attacker bör dock finnas, enligt oss.

5.6 Summering av fördjupad analys och tolkning

Vid jämförelse till en dator är det en självklarhet att så fort en ny dator köpts in, skaffas ett väl utformat antivirusprogram som ger det skydd ett företag kan tänkas behöva. Medvetenheten kring de smarta mobiltelefonerna borde således inte vara annorlunda då dessa fungerar som nämnt på näst intill exakt samma vis och utsätts för mer eller mindre likartade hot. Generellt sett anser mångdelen av de företag vi intervjuat i denna undersökning att många av riskerna som finns ute idag inte utgör ett tillräckligt stort hot för just deras företag och de anser att skydd bör finnas i viss mån men att många risker troligtvis aldrig kommer beröra dem och aldrig kommer kunna göra så pass stor skada att det skulle skada företaget i fråga. Ett antagande till dessa uttalanden kan vara att företag antingen inte är tillräckligt informerade om vilka risker och hot som finns och vad de kan åstadkomma eller att företagen helt enkelt inte anser att tiden och kostnaderna för vad ett vattentätt skydd för de mobila enheterna i företaget kostar, är värt det i det långa loppet.

6 Slutsats

Vårt huvudsakliga syfte med uppsatsen har varit att undersöka vilka risker och hot det finns mot smarta mobiltelefoner i företag samt hur informationsförlust och intrång av olika slag förebyggs. Efter litteraturgenomgången har vi kommit fram till att de fem största riskerna för smarta mobiltelefoner är förlust av enhet, återvinning av enhet, malware, avlyssning och intrång (se kapitel 2.2).

Efter att ha gjort intervjuerna har vi bildat oss en uppfattning om att de företag vi intervjuat har en mindre bra plan för hur risker och hot bör förebyggas för att på bästa sätt skydda en verksamhet och dess smarta mobiltelefoner. Vid jämförelse av intervjuerna och vår framtagna undersökningsmodell (figur 3,1.), kan vi konstatera att de antingen helt saknar en plan, exempelvis en policy, eller endast behandlar ett fåtal av riskerna gällande säkerhetsaspekterna kring smarta mobiltelefoner.

En anledning till att en sådan plan saknas i merparten av våra intervjuade företag är att kostnaden för att bygga upp ett vattentätt skydd för användningen av smarta mobiltelefoner i företaget är för stor i jämförelse med kostnaden av att drabbas av någon av de hot vi tidigare tagit upp. Detta hör ihop med att företagen inte ser sig själva som en måltavla och därmed inte löper en stor risk att utsättas för några attacker riktade specifikt mot företaget.

Detta anser vi är ett kortsiktigt resonemang som kan straffa sig i slutänden. Endast ett av fyra företag anser att de själva har ett otillräckligt skydd på sina smarta mobiltelefoner som i sin tur hanterar affärshemligheter och viktig information som skulle kunna skada företaget vid förlust. Detta företag planerar att inom en snar framtid införa någon form av policy där det finns tydliga direktiv om huruvida mobila enheter ska skyddas och hanteras i verksamheten.

6.1 Sammanfattande slutsats

- **Risker och hot mot smarta mobiltelefoner i företag**
    - Förlust av enhet
    - Återvinning av enhet
    - Malware
    - Avlyssning
    - Intrång
- **Hur förebyggs dessa risker i företag?**
    - Saknar ofta förebyggande åtgärder
        - Kan bero på kostnaden för att förebygga riskerna
    - Ett av fyra intervjuade företag har en policy för användning av smarta mobiltelefoner

Bilagor

Bilaga 1 – Använda förkortningar

Förkortning:	Förklaring:
PDA	Personal Digital Assistant
RAM	Random Access Memory
SD	Secure Digital
IMEI	International Mobile Equipment Identity
EIR	Equipment Identity Register
MMS	Multimedia Messaging Service
SMS	Short Message Service
MSN	Microsoft Network
OS	Operativsystem
Java ME	Java Micro Edition

Bilaga 2 – Intervjuguide

Vi utgår från dessa sju frågor och ställer därefter följdfrågor beroende på respondentens svar för att samla in den information vi anser oss behöva för att genomföra en analys och besvara vår forskningsfråga.

1. Vilken titel har du och hur länge har du arbetat på företaget?
2. Har ni några policys för hur era anställdas smartphones får användas?
3. Är ni medvetna om de olika hot som finns mot smartphones?
4. Vilka åtgärder vidtas om en anställd tappar bort sin enhet eller om den blir stulen?
5. Hur hanterar ni en enhet som inte längre brukas av en anställd eller är förbrukad på grund av exempelvis slitage?
6. Hur skyddar ni era smartphones mot malware?
7. Hur skyddar ni era smartphones mot avlyssning och intrång?

Bilaga 3 – Säkerhetspolicy enligt SANS

Generella policykrav (SANS, 2008):

Policy:	Beskrivning:
Policyöverenskommelse	IT-avdelningen måste säkerställa att alla anställda som använder handhållna enheter accepterar säkerhetspolicyn innan de tillåts använda handhållna enheter i arbetet.
Användare: roller och ansvar	Användarna måste använda enheter med sunt förnuft. Om en användare är osäker ska IT-avdelningen kontaktas för att klargöra hur situationen ska hanteras. Användarna måste skydda enheten från förlust samt avslöjande av information som tillhör företaget. Innan användaren ansluter en enhet till företagets nätverk måste han eller hon säkerställa att enheten är godkänd att ansluta av IT-avdelningen. Om någon misstänker en brist i säkerheten måste IT-avdelningen genast meddelas. Kostnader för enheten, utöver de som företaget godkänt är användarens eget ansvar.
Användande av privat enhet i företagsmiljö	IT-ledning måste definiera privata enheter får anslutas till företagets nätverk. *Privata enheter tillåts ej:* I högsäkerhetsfaciliteter måste privata enheter förbjudas. I dessa fall bör enheterna samlas in innan den anställde får tillträda faciliteten. Privata enheter tillåts i kontorsmiljö, men dessa enheter får inte ansluta till interna nätverk. Enheterna får inte heller synkroniseras med arbetsstationer som är anslutna till interna nätverk. Nätverken måste även de skyddas, och får inte tillåtas lämna ut företagsinformation till oregistrerade enheter. *Privata enheter tillåts:* Alla privata enheter som kan ansluta till företagets nätverk måste först godkännas av IT-avdelningen. Privata enheter måste registreras precis som företagets enheter, men identifieras som privata. Detta för att förhindra att data försvinner från enheter vars ägare inte kan identifieras.
IT-avdelning: roller och ansvar	IT-ledningen är ansvarig för säkerhetspolicyn och bör utföra en riskanalys för att

	dokumentera de skydd som ska användas för de olika sorters enheter som ska användas i nätverket samt de enheter som ägs av företaget. Policyn bör granskas årligen av IT-ledningen för att få med ändringar angående utrustning, hot med mera. IT-ledningen är ansvarig för att utveckla procedurer för att implementera policyn. IT-avdelningen ska tillhandahålla och underhålla en lista över godkända enheter som får användas på nätverket. IT-avdelningen ska tillhandahålla listor över godkända och icke godkända applikationer som får användas.
Användarutbildning	Användarna måste utbildas i korrekt användning av enheter och företagets resurser. Fokus ska läggas på företagsapplikationer och grundläggande säkerhetsfunktioner.
Register över handhållna enheter	Ett register över enheter som används måste finnas. I registret ska enheter kunna kopplas ihop med ägare och identitet för nätverksåtkomst. Enheterna ska kunna identifieras av till exempel IMEI, ägarens id, användar-id eller enhetens namn.
Tillåtna tjänster och applikationer	Endast godkända applikationer får installeras på enheten. Listan över godkända applikationer bör tillhandahållas av IT-avdelningen. Om den önskade applikationen inte finns på listan, kan en förfrågan skickas till IT-avdelningen. Om applikationen klarar de krav som finns läggs den till på listan och kan därefter installeras.
Förbjudna tjänster	IT-avdelningen ska tillhandahålla en lista över otillåtna tjänster och applikationer. Listan måste vara tillgänglig för användarna via intranätet.
Förbjudna handlingar	Användare får inte ändra säkerhetsinställningar utan att ha fått godkännande från IT-avdelningen. Om en användare inte följer denna regel bör disciplinära åtgärder vidtas.

Fysisk säkerhetspolicy:

Policy:	Beskrivning:
Fysisk säkerhet	I de fall en användare tappat bort eller har blivit bestulen på sin enhet måste denna rapportera direkt till IT- avdelningen eller supporten så att rätt åtgärder kan vidtas så snabbt som möjligt. Procedurer om vad som måste göras vid förlust av enhet måste vara tydliga och väl informerade till alla användare.
Enhetens säkerhet	Användandet av handhållna enheter är beskrivet i godtagbar användandepolicyn enligt nedan: Att ringa ett telefonsamtal eller använda den mobila enheten under framförandet av ett fordon anses vara en säkerhetsrisk. Föraren borde använda enheten endast när fordonet är parkerat eller föraren befinner sig utanför fordonet. om föraren måste använda enheten under körning kräver företaget i fråga att en hands-free enhet används.
Lösenordspolicy	Åtkomsten till den mobila enheten måste alla gånger vara lösenordsskyddad.
Ägareinformation	Ägarens uppgifter skall vara skrivna på enheten men dock på ett sådant sätt att företagsnamnet inte avslöjas. Detta kan göras på två sätt: • De skrivs på enhetens låsskärm • Uppgifterna skrivs på en etikett som sedan klistras på enhetens baksida Detta tillåter vid upphittande av enheten att denna återlämnas till ägaren.
Trådlöst	En enhet tillhörande företaget i fråga skall erbjuda trådlös radering eller åtminstone blockering av informationen. Denna funktion hjälper företaget att skydda sig själv mot informationsförlust eller informationsstöld av obehörig vid förlust av en enhet. Noteras bör dock att uttagbara SD-kort eller andra typer av minneskort bör vara krypterade då dessa enkelt kan plockas ut ur en stulen enhet och användas i en annan och därigenom få tillgång till informationen på den.
Användandet av kamera	Kameran i de mobila enheterna kan komma

	att tvingas vara inaktiverad inom begränsade områden beroende på företagets ifråga riskanalys. I känsliga områden kan kameran användas för att fotografera och därmed stjäla hemlig information varpå den sedan kan skickas med bildmeddelande eller e-mail.

Operativsystemsäkerhet:

Policy:	Beskrivning:
Firmware version, uppdatering och tillägg	Enheters firmware måste uppdateras. Uppdateringsprocessen är IT-avdelningens ansvar och denna måste dokumenteras och testas innan uppdateringen görs på samtliga enheter i företaget. Backup måste göras innan uppdateringen installeras.
OS version, uppdatering och tillägg	Enheters OS måste uppdateras. Uppdateringsprocessen är IT-avdelningens ansvar och denna måste dokumenteras och testas innan uppdateringen görs på samtliga enheter i företaget. Backup måste göras innan uppdateringen installeras.
Osignerade applikationer	Användare får inte installera några osignerade applikationer eller teman på sina enheter, detta för att förebygga malware.
Signerade applikationer från tredje part	IT-avdelningen måste skapa en lista över tillåtna applikationer. Säkerhetsansvariga måste undersöka om tredje parts applikationer är nödvändiga. Om de är nödvändiga ska de alltid testas innan de används på enheterna
Certifikathantering	Endast IT-avdelningen har tillåtelse att hantera certifikat på handhållna enheter. IT-avdelningen har ansvar för att installera nödvändiga certifikat på enheterna i företaget.
Antivirus policy	Samtliga enheter måste ha antivirus-mjukvara installerad för att förhindra att virus sprids i företagets nätverk.
Brandvägg	Brandvägg ska installeras på alla de enheter det finns möjlighet att göra det på.

Personal Area Network(PAN) säkerhetspolicy:

Policy:	Beskrivning:
Bluetooth version	Ingen Bluetooth-enhet som inte stödjer Bluetooth version 2.1får användas utan skriftligt tillstånd från informationssäkerhetschefen.
PAN PINs och parning	När två enheter paras ihop med hjälp av PAN, måste användarna säkerställa att de inte befinner sig på en allmän plats. Om utrustningen kräver lösenord efter det att de blivit ihop parade måste användarna neka förfrågningen och rapportera detta omedelbart till IT-avdelningen eller supporten. Detta eftersom ovanstående är ett tecken på intrångsförsök. Användarna måste vara försiktiga så att avlyssning ej sker när parning via Bluetooth utförs.
Bluetoothenhetens säkerhetsinställningar	Alla Bluetoothenheter skall besitta ”säkerhetsläge 3”, som tillåter kryptering åt båda hållen mellan bluetoothenheterna och den tillkommande utrustningen. Använd Bluetooth i ”dolt läge” och ha funktionen aktiverad endast när denna används.
Filöverföring (beaming) med hjälp av PAN	Filöverföring mellan enheter inom nära räckhåll (PAN), som sker via Bluetooth eller infraröd kommunikation får endast ske mellan autentiserade parter som båda måste komma överens om en lösennyckel. Anonym koppling får under inga omständigheter ske.
PAN säkerhetsgranskning	Informationssäkerhetspersonal ska utföra granskning av användandet av Bluetooth och IrDA för att säkerställa att denna policy följs. Processen för granskning får dock aldrig innehålla moment som innefattar avlyssning av samtal eller dylikt.
Otillåten användning av Bluetooth eller IrDA	Följande handlingar faller under kategorin otillåten användning av Bluetooth eller IrDA-enheter: • Avlyssning • ”Spoofing” (stöld) av en enhets ID • DoS-attacker • Andra attacker emot Bluetooth eller IrDA stödda enheter • Använda företagsägd utrustning på en icke företagsägd Bluetooth/IrDA-enhet • Otillåtlig modifikation av Bluetooth/IrDA-enheten ifråga oavsett syfte.

Bluetooth/IrDA användaransvar	Det är enhetens innehavares ansvar att följa denna policy. Bluetooth eller IrDA användare får endast använda Hårdvara, mjukvara eller lösningar som är godkända av företaget för åtkomst till företagets informations system. All annan hårdvara, mjukvara eller andra lösningar skall icke bli godkända för användande emot företagets systemlösningar. Bluetooth/IrDA-användare måste agera korrekt i sitt användande för att skydda information, nätverksåtkomsten, lösenord, krypteringsnycklar och Bluetooth/IrDA-utrustning. Bluetooth/IrDA-användare är skyldiga att rapportera någon form av missbruk, borttappande eller stöld av en Bluetooth/IrDA-enhet eller system omedelbart till informationssäkerhetsavdelningen.
Infraröd IrDA	En enhets infraröda stöd måste vara inaktiverat om stöd för Bluetoothuppkoppling finns på samma enhet. Bluetoothuppkoppling är att föredra framför IrDA om detta stöd finns. Om IrDA måste vara aktiverat måste parningen innefatta långa parningslösenord.

Datasäkerhet:

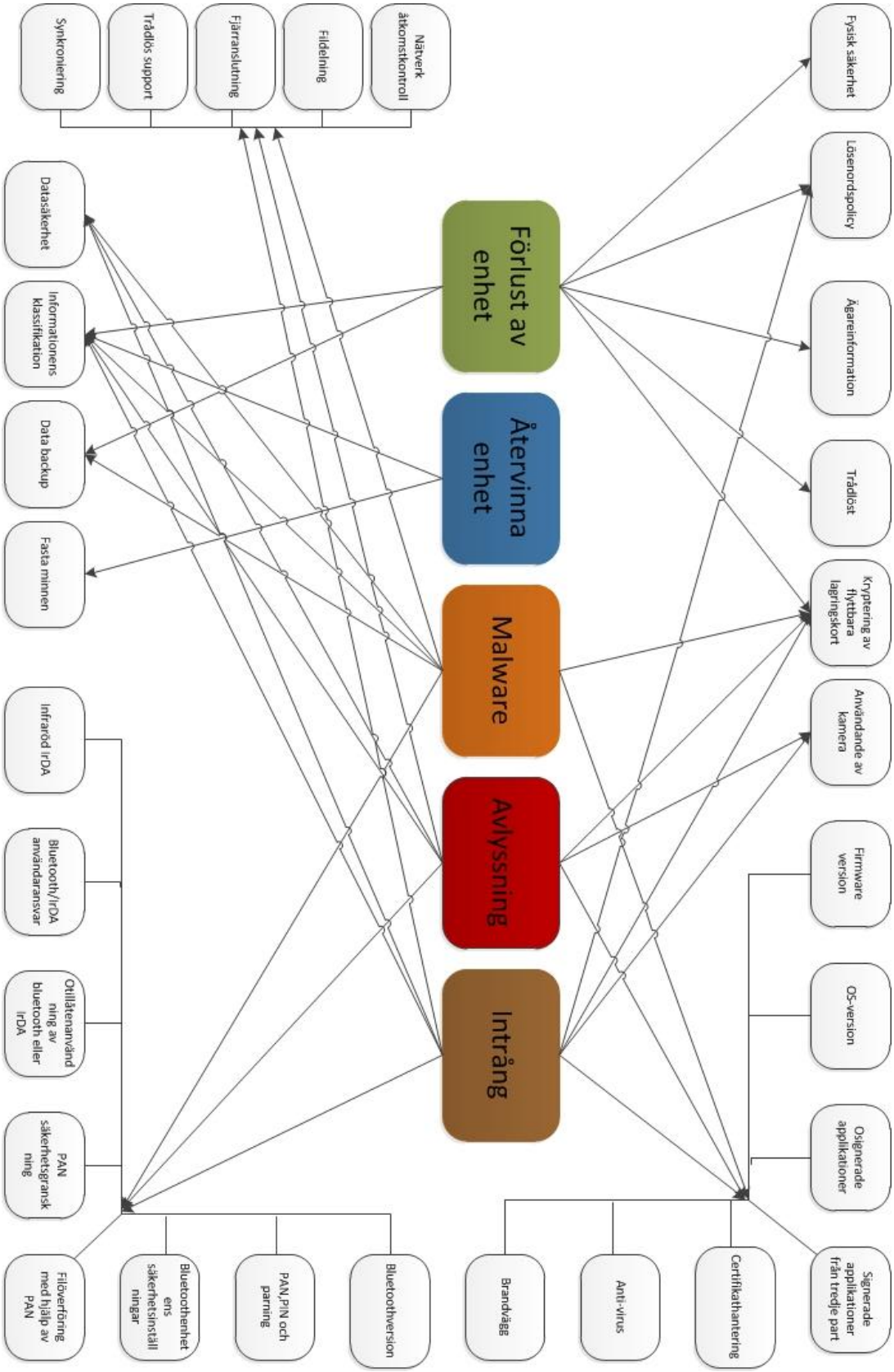
Policy:	Beskrivning:
Informations klassifikation	En handhållen enhet ska inte användas för att lagra lösenord, koder till dörrar, personnummer eller annan känslig information. Interna dokument ska inte lagras på enheten om det inte är absolut nödvändigt.
Datasäkerhet	Handhållna enheter som innehåller konfidentiell, personlig eller känslig information som tillhör företaget ska använda sig av kryptering eller likvärdig säkerhetsåtgärd för att skydda företagsinformationen.
Fasta minnen	Företagsinformation ska inte lagras på fasta minnen i enheterna, utan i minneskort så som SD- eller MMC-kort.
Kryptering av flyttbara lagringskort	Minneskort, som SD-kort, måste krypteras för att förhindra data förlust vid intrång.
Data backup	Backup måste göras regelbundet på den data som finns på handhållna enheter. Detta ska ske enligt företagets backup-policy, som ska specificera hur ofta backup ska göras.

Privat information på företagets enheter	Tre alternativ: 1: Anställda får inte lagra privat information på företagets enheter. 2: Anställda har fullt ansvar för den privata information som finns på företagets enheter. Företaget kan inte hållas ansvarigt för vad som händer med den informationen vid exempelvis stöld. 3: Anställda får lagra privat information på företagets enheter, men bör då använda sig av en sorts mobil ”plånbok” som låser den informationen med ytterligare ett lösenord. Detta lösenord ska inte vara samma som det som låser telefonen.

Företags nätverkssäkerhet:

Policy:	Beskrivning:
Nätverk; åtkomstkontroll	Alla enheter som vill ansluta till företagets nätverk måste först bli godkända av IT-avdelningen.
Fildelning	Ska vara avstängt ifrån början. Om fildelning ska förekomma måste en verifiering finnas som identifierar de involverade enheterna.
Fjärranslutning till företagets resurser	Alla som använder fjärranslutning till företagets resurser måste rätta sig efter följande procedurer: Distansarbete, Bortskaffande av information/media/utrustning.
Trådlös support	Trådlös åtkomst bör inte användas om det inte är nödvändigt, detta för att minska risken för spridning av malware. Åtkomst till publika, öppna och opålitliga trådlösa nätverk bör alltid vara avstängt om uppkoppling inte är av högsta nödvändighet. Begränsa åtkomstpunkter till endast företagets åtkomstpunkter, begränsa möjligheten att ansluta till publika nätverk utan kryptering och begränsa möjligheten att ansluta till WEP-skyddade trådlösa nätverk.
Synkronisering	Synkronisering mellan en PC och en handhållen enhet måste ske på ett säkert sätt genom att använda en sorts nyckel för sammankoppling i enlighet med företagets standarder och lösenordspolicy.

Bilaga 4 – Risker och koppling till Säkerhetspolicy enligt SANS



Bilaga 5 – Transkribering Företag A

Datum: 2012-04-25, Malmö

Nr:	Fråga:	Svar:	Kod:
0	Vilken är din roll på företaget?	Jag är HR-chef.	R
1	Och hur länge har du arbetat här?	Företaget bildades för ett år sedan, så det beror på vad du menar. Med de människorna som jobbar här inne har jag jobbat sedan 2000. Men bolaget är bara ett år gammalt, det är ett resultat av sammanslagningen av två bolag.	R
2	Hade du samma roll innan sammanslagningen?	Ja.	IR
3	Har ni några policys för hur era anställdas smarta mobiltelefoner får användas?	Inga what so ever.	R
4	Inga alls?	Nej, ingenting. Vi har en rätt så utvecklad IT-policy som gäller generellt, och man skulle kunna hårddra det och säga att allt som gäller datorerna gäller även mobilerna. I det kan man säga: inget upphovsrättsskyddat material, inga oegentligheter typ porr, våld och sådant där. Men det är den generella IT-policyn. Vi anser att den gäller telefonerna men det finns inte skrivit specifikt för dem eftersom att det är en så ny sak att ha smarta mobiltelefoner, det har exploderat liksom.	C,D,E
5	Får de anställda smarta mobiltelefoner av företaget, eller de har sina egna?	Nej, var och en har en jobbmobil, som de får nyttja och bruka. Den lämnas ju tillbaka om de slutar, det är företagets telefoner. Det är samma sak för datorer, och det är bland annat för att kunna kontrollera vad man har dem till.	B
6	Men det här med att inte surfa in på till exempel vissa sidor, det står skrivet i IT-policyn?	Ja det gör ju det, men egentligen bör det ju skrivas något specifikt för mobiltelefoner för det skiljer sig ganska mycket åt.	C,D,E
7	Den policyn är något de nyanställda får läsa när de kommer hit?	Absolut, det är det första de får, första dagen, bland annat den policyn.	R

8	Har ni någonsin reflekterat kring säkerheten kring mobiltelefoner?	Nej, det är det jag menar, det har vi inte alls tänkt på. Eller rättare sagt, vår IT-chef håller på att tänka på det nu, men det är ingenting som alls har varit uppe till diskussion innan. Och IT-policyn är säkert något standardformulär som vi hittat någonstans.	R
9	Policies om vem folk får ringa till, har ni det?	Vi har fastpris-abonnemang, så folk får använda sina mobiler privat hur mycket de vill, så länge de inte ringer utomlands. Det gäller i Sverige och Danmark, vi har en del kunder i Danmark också.	IR
10	Är ni medvetna om de hot som finns för smarta mobiltelefoner?	Delvis, men inte jättemycket.	R
11	Vad händer om en anställd tappar bort sin telefon, eller om den blir stulen?	Idag har vi egentligen ingen åtgärd, det vi borde haft är egentligen att tvinga folk att ha någon form av programvara installerad för att kunna radera den fjärrstyrt. Vissa har det, vi som är intresserade av det har det.	A
12	Ja har man iPhone så är det ju ganska ”basic”?	Precis, men alla är definitivt inte medvetna om att det går, så det är en sådan grej som borde finnas med i en policy.	A
13	Men polisanmälan, det är inget krav heller?	Det beror på, det var en person som blev rånad på sin mobil ute på stan och då polisanmäler man händelsen ju. Men jag har aldrig varit med om att någon gjort av med sin telefon.	A
14	Om en telefon inte längre brukas eller används av anställd, som kanske har slutat på företaget, vad händer med telefonen då?	Den lämnas in till oss. Nu har vi precis gått över till den typen av riktiga företagsmobiler som vi har idag så det är ännu ingen som har lämnat in någon än. Men de kommer säkert att cirkulera, om det inte är så att det är någon jättegammal pjäs. Så de kommer säkert att lämnas till någon nyanställd.	B

15	Har ni då några krav på att de ska radera innehållet innan de lämnar in den?	Ja, alltså det går också tillbaka till den generella IT-policyn. Kravet där är att lämna över den icke-raderad. Dom får inte själva radera företagets material, det materialet äger vi. Alla har ju någon form av privata saker i sin dator, och det raderar man själv, men det som är jobbrelaterat vill vi kunna kontrollera och vara hundra på att vi har kvar. Detsamma gäller i princip för mobilen. Men jag kan tillägga det, och det kanske vi kommer till, vi använder inte våra mobiler i arbetet till någonting annat än att ringa och maila med och då finns ju det på Exchange-servern.	B
16	Men ofta är det ju så att i en smartphone är mailen alltid tillgänglig?	Absolut.	IR
17	Så om man tappar bort den finns det alltid en risk att företagsinformationen hamnar i fel händer?	Det är helt rätt, men det är en helt annan sak och det kanske vi kommer till också, men om någon skulle tappa bort sin mobil så finns det liksom inget som vi behöver, utan det mesta finns ju redan på våra servrar.	A
18	Sen kommer vi in på det här med hur ni skyddar er mot malware, intrång och avlyssning?	Ingenting.	C,D,E
19	Ni har inga anti-virusprogram eller liknande?	Inte ett smack, förutom det som eventuellt finns inbyggt i en iPhone.	C,D,E
20	Det gäller ju mest android-telefoner, har ni några sådana?	”Tjej-telefoner” har vi inte, vi har bara iPhones. Det finns några enstaka Android-telefoner faktiskt, men policyn är att alla nyanställda får en iPhone, och vi har bytt ut nästan alla precis.	R
21	Kör ni PC eller Mac på datorsidan?	Jag skäms och säga att vi kör PC, vi har ett par Mac men det är de som håller på med design och sånt, resten kör PC. Där har vi naturligtvis en helt annan utbyggnad av brandväggar och anti-virus.	IR
22	Man kan ju skydda sin telefon rent fysiskt genom att låsa skärmen och så, har ni något i er IT-policy som säger att man ska göra det på datorn?	Nej det har vi nog inte, tror jag, men vi borde haft det och vi borde haft det på våra telefoner också.	A,E

23	Att ni måste ha någon form av kod?	Ja, det ska definitivt in i den policyn som ska finnas. Jag tror att många har det, jag själv har det definitivt och det är definitivt något som man ska ha. Det är ju det minsta man kan göra.	A,E
24	Säkerhetspolicyn som ni har för era mobila enheter är i så fall den som gäller för datorerna?	Ja, precis.	R
25	Har ni hört talas om till exempel avlyssning?	Nja, man kan ju resonera såhär: Man måste jämföra kostnaden för att skydda information, eller data i vårt fall, jämfört med kostnaden för att bli av med den. Vi har liksom ingenting som skulle vara så farlig om det kom ut. Vi har ingen produktutveckling, som Microsoft till exempel, inga patent, så vi har inga sådana grejer utan det är ju vidareutveckling av kunders system.	D
26	Hur många anställda är ni här?	Vi är 65 st. totalt på våra två kontor. Och kommentaren till mobilerna är att vi använder dem bara till att ringa och skicka sms med, vi har inga applikationer som vi själva använder, vi har ingen typ av dokument som skulle vara lönt att ha på telefonen.	R
27	Ni har heller inga restriktioner för vad som får installeras då?	Nej, så är det ju, vi har inga restriktioner för vilka applikationer som får installeras, men å andra sidan har ju Apple rätt så hårda restriktioner själva så man kan ju inte lägga in precis vad som helst.	C,D,E
28	Det är ju det som är fördelen med iPhone jämfört med Android-telefoner, på Android kan ju folk lägga in lite vad som helst, som kanske verkar trovärdigt men som är fulla med spyware och liknande.	Precis, det är ju det som är bra med Apple. Men det är lite så vi har resonerat med våra datorer också, vi har egentligen inget som skulle vara en jättekatastrof att bli av med, vad jag kan komma på på rak arm.	IR
29	Det finns ju en hel del risker med att använda bank-applikationer och liknande om man blir utsatt för avlyssning, till exempel.	Ja, men det är nog mest privatpersoner som använder det, jag har svårt att se företag använde dem.	IR

30	Är det något mer du känner att du vill tillägga?	Nej jag tror inte det, det är väl mer att konstatera att den här marknaden är rätt så ny för oss.	R
31	Men ni har ändå funderat på det?	Absolut, jag pratade nyss med vår IT-ansvarige och han hade haft en diskussion med vår andra IT-ansvarige bland annat om att just inte tillåta smarta mobiltelefoner i vårt riktiga nät här inne. De flesta kopplar ju upp sig med mobilen på vårt trådlösa nätverk för att kunna sitta på muggen och surfa, det är ju på den nivån, och så gör vi ju förvisso en del applikationsutveckling till våra kunder. Men man har ju inte hur många licenser som helst till brandväggen, och helt plötsligt har vi dubbelt så många mobila enheter i samma nät. Så sådana grejer hade de diskuterat, att det inte ska tillåtas eller att man har ett halv-publikt nät med restriktioner. Sen hade de nog diskuterat just det här med knapplås, att det borde man nog införa, och någon trådlös ”remote wiping”. Sen hade de nog mest diskuterat IT-policyn, att utveckla den vidare och hur långt man ska gå. Men IT-folk och IT-chefer är ju rätt glada för att inte lyfta för många fingrar, och de vill inte sitta och lägga tid på sådant här hela tiden. Så det är det jag menar, vad kostar det att skydda och vad kostar det att bli av med data. Vi har ju pratat om det härinne, vad hade hänt om vår konkurrent fått min mobiltelefon? Förmodligen ingenting.	R

Bilaga 6 – Transkribering Företag B

Datum: 2012-04-26, Lund

Nr:	Fråga:	Svar:	Kod:
0	Vilken titel har du i företaget?	Jag är IT-Chef.	R
1	Hur länge har du jobbat på företaget?	IT- Chef titeln har jag haft i två år ungefär. Innan dess var jag IT-ansvarig i några år, ensam på min avdelning. Innan dess var jag supporttekniker och totalt har jag väl varit här i nästan 7 år.	R
2	Gick du direkt hit från din utbildning?	Ja.	IR
3	Du läste möjligtvis inte Systemvetenskap?	Nej.	IR
4	Vad läste du för någonting?	Jag läste i Kristianstad. Först läste jag ett KY-program sen började jag plugga på högskolan. Satte ihop ett eget program faktiskt. Sen fick jag jobberbjudandet här.	IR
5	Har ni några policys för hur era anställdas smarta mobiltelefoner får användas?	Ja det har vi! Vi har en mobiltelefonpolicy och den har väl varit informell innan, mer att man bara sagt hur det ska vara. Men nu sen vi skaffade iPhones för ungefär ett år sedan, är den nedskriven och väldigt formell.	R
6	Vad innefattar denna policy?	Den innefattar när man ska ringa, hur man ska ringa, vad man ska tänka på, att man ska skydda sin telefon.	R

7	Så den innefattar säkerhetstänk?	Ja och nej. Vi synkar dem med exchange-server och då ”pushar” vi ut en del inställningar genom det. Man måste ha låskod på den, vi kan ”remotwipa” dem (fjärrstyrt radera enheten), vi kan kolla positionerna på dem, inte för att vi gjort det någon gång men vi kan och vi kan kräva lösenkodbyten osv. så det är inget användarna ser egentligen, de bara tänker att så är det så det sköts helt via servern trådlöst. Microsoft släppte precis en helt ny produkt som heter system ”Center configuration manager 2012” som utökar detta och tillåter att man gör fler saker trådlöst till mobilerna. Man kan pusha ut program till dem, man kan välja vilka program som installeras osv. Men vi anser att iPhone är en så pass säker plattform att folk får installera precis vilka program de vill. Vi ser ingen säkerhetsrisk i det.	A
8	Har alla iPhone på företaget?	Alla har iPhone. Eller alla har som behöver ha en mobiltelefon.	R
9	Och det får de när de börjar jobba på företaget eller?	Ja. Vi tog ett beslut för ungefär ett år sedan, alla hade Androidtelefoner innan och innan dess hade vi gamla Windows mobile. iPhone är ju lite dyrare men vi tog ett beslut att vi skulle köra på dessa eftersom vi antog att det skulle minska supporten ganska mycket vilket det utan tvekan har gjort. iPhone sköter sig själv. Det är i princip ingen anställd som hör av sig beträffande problem. Det är i så fall om de badat med telefonen eller tappat den eller att den blivit stulen annars ingen support.	R
10	Så om man kommer som nyanställd hit till företaget så får man en iPhone, man får inte använda sin egen telefon i arbetet?	Man får lov att mailsynkronisera sin egen telefon men då blir man också ”ägd” av oss! När man sätter upp den här synken får man våra policys på telefonen, man måste ha pinkod, och följer man inte dem så får man inte synka. Och vi har möjlighet till ”remote wipe” så själva grundförutsättningen för att få synka mobilerna är att våra policys fungerar på telefonerna.	R

11	Men har ni mycket information i företaget som hade varit direkt skadligt om det hade kommit i fel händer?	Det är ju aldrig bra när man har informationsläkage. Det finns väl mer eller mindre känslig information. Men ja och nej, det hade skadats sen hur stor grej det hade blivit av det är ju en annan fråga. Vi sitter ju inte på försvarshemligheter direkt. Så den information som är känslig finns inte i mail och det är i princip mail vi synkar med mobilen. Det hade varit illa men det hade inte varit ohanterbart. Men vi är inte direkt oroliga för det heller i och med att där måste finnas en låskod, vi kan ”remote wipa” mobilerna, vi har rätt så bra koll på den informationen.	A,C,D,E
12	Då kommer vi lite automatiskt till nästa fråga, är ni medvetna om de olika hoten som finns till smarta mobiltelefoner?	Alltså vi har gjort det väldigt lätt för oss i och med att vi har iPhones då dessa är säkra i grund och botten. Sen finns de vissa som synkar från Android, det handlar om en eller två personer, och där är det ju kanske lite mer riskfyllt. Men man håller ju en allmän koll på säkerhetssituationer så att säga och kommer det något som riktar in sig på just stöld av synkroniseringsuppgifter eller spionage på mail och så vidare, då kanske man får spärra Androidenheterna. Eller om det kommer en säkerhetslucka till iPhone, då får man se till att de antingen blir uppdaterade eller att man stänger av synken så länge. Man gör ju en riskbedömning löpande på den informationen som finns på marknaden. Vi resonerar lite så att är det något stort och brett virus som kommer och söker allting, är vi kanske ett mål. Men vi känner oss inte som ett mål för någon som gör ett ”Custom made” virus, alltså ett anpassat virus bara för oss. Vi är ett för litet företag för det som folk inte riktigt bryr sig om på det sättet och vi har inget man direkt kan översätta till värde i form av pengar osv. Så vi känner oss inte alls som en måltavla mer än om det är generella virus.	A,C,D,E

13	Om en anställd tappar bort sin telefon eller om den blir stulen, vad gör ni då?	Då utför vi en ”remote wipe” först och främst. Så en ”remote wipe” initieras men det är ju inte alltid de fungerar eftersom om de är stulna så tar de ofta ut simkorten och då har vi inte kontakt med telefonen längre. Men sen polisanmäler vi det och sen köper vi en ny telefon. Det är inte mer än så.	A
14	Men det har hänt att den blivit stulen?	Det har hänt, ganska nyligen också faktiskt.	IR
15	Hur hanterar ni en telefon som använts av en anställd som sedan slutar, eller hur hanterar ni en telefon om den är gammal och uttjänt?	De lämnar in telefonerna till oss, och just nu ligger alla våra gamla telefoner där nere i en kartong, vi har inte gjort oss av med dem än, men skickar vi in dem på reparation eller något liknande så återställer vi dem alltid fullt innan vi skickar in dem. Och det är samma, skulle vi slänga dem eller sälja dem vidare till någon återvinning så skulle vi ”wipa” dem innan. Vi gör det en gång telefonernas egna gränssnitt faller. Vi känner att skulle en annan part ha intresset att återställa informationen, kanske det går rent teoretiskt sett, då får de göra det. Allt ligger på en rimlig nivå, allt är tidskrävande. Bara att återställa 60 telefoner tar tid och ännu mer tid hade det tagit att återställa dem fem gånger för att göra det på ett säkert sätt och det har man inte tid med.	B
16	Hur skyddar ni era smarta mobiltelefoner mot Malware och Spyware?	Vi har iOS på dem! Det är det enklaste och bästa. Nya Windows mobile, eller Windows phone som den heter nu, hade också varit tillämpbar eftersom den också är väldigt bra, den har en väldigt bra säkerhetsmodell.	C,D,E
17	Hur skyddade ni er när ni hade Android?	Vi gjorde ingenting.	C,D,E
18	Ni hade inga virusskydd?	Vi hade inga virusskydd. Och det var väl den stora anledningen till varför vi gick ifrån Android också.	C,D,E

19	Märkte ni av att där var en säkerhetsrisk rent allmänt eller det var bara ett rykte?	Lite märkte vi. Vi märke nog mer av den dåliga prestandan i dem. Installerar man program så kunde det fungera lite dåligt. Man fick återställa dem relativt ofta vilket innebar att vi fick börja om från början ganska ofta. Det funkade generellt ganska dåligt. Det märkte vi av. Säkerhetsrisker, inte vad vi vet! Men samtidigt så var det en stor del av poängen varför vi gick ifrån Android. Men under ett par år så var Android prisvärda och de hade en aktiv synk som en del telefoner inte löste.	R
20	Vår nästa fråga är om ni skyddar dem mot avlyssning och intrång men det är väl kanske samma sak där?	Ja FRA kan man nog aldrig skydda sig emot! Men annars inga speciella skydd.	D,E
21	Har ni någon utbildning till nyanställda om hur de ska hantera telefonen med till exempel de synkningarna du nämnt eller man kör bara på direkt?	Man får ett A4 papper med policyn som man får läsa.	R
22	Ni kontrollerar inte alls den mjukvaran som installeras av anställda på telefonerna. De får ha vilka applikationer de vill?	Ja. Den kontrollen gör Apple till oss. Det är väl där Google och Android är lite sämre. Jag kan sakna Android och dess funktioner lite då de har en del användbara funktioner. Att låsa upp iPhone telefoner bidrar ju till att man kan komma åt fler användbara funktioner men bidrar också i sin tur till att säkerheten i dem försvinner. Jag tror Google måste börja justera sin modell vad gäller säkerheten.	C,D,E
23	Men kontentan är att ni har en policy för mobiltelefoner som är på cirka en A4 sida?	Ja. (Respondenten frågar om vi vill se policyn och plockar fram den) Policyn berättar bland annat att man som anställd ska vara försiktig med att ringa utomlands och man ska ha skal på dem för att skydda dem mot fysiska skador. Detta har bidragit till att väldigt få displayglas har gått sönder. Vi har utgått ifrån en befintlig policymall så det är inget märkvärdigt med den på något sätt.	R

24	Det var de frågorna vi hade. Du har ingenting att tillägga?	Nej! Vi har gjort det väldigt enkelt för oss. Vi har en fördel då vi är ett IT-företag och vi har därmed en ganska hög medvetenhet. Skulle inte jag ha implementerat en mobiltelefonpolicy, så hade folk kommit till mig och sagt till att en sådan borde vi ha vilket jag kan föreställa mig inte är lika prioriterat i andra företag.	R
	Tack för intervjun och för att du tog dig tid att besvara våra frågor.	Tack själva.	IR

Bilaga 7 – Transkribering Företag C

Datum: 2012-04-26, Lund

Nr:	Fråga:	Svar:	Kod:
0.	Vad har du för titel på företaget?	Jag är platschef och har även ett IT-ansvar.	R
1.	Hur länge har du arbetat på företaget?	Två år har jag varit här.	R
2.	Har ni några policys för hur era anställdas smarta mobiltelefoner får användas?	Ja, det har vi.	R
3.	Är det då säkerhetsmässigt eller är det hur mycket de anställda får ringa, eller är det både och kanske?	Det är både och.	R
4.	Hur ser den här policyn ut?	I korta drag kan man väl säga att den inte får användas för piratkopiering, pornografi, extrempolitik och sabotage. Och det är samma som vår vanliga IT-policy, att som anställd får man inte förekomma i forum som har med detta att göra, och det är precis samma policy som vi har för mobiltelefoni eller smarta mobiltelefoner. Man kan också säga att det skiljer sig lite ifrån datorpolicyn som säger att man inte får lov att installera privata program på din dator, även om du får lov att ta hem den får du inte lov att installera dina privata spel eller vad du nu har för något. När det gäller smartphonen har vi en policy som säger att du får lov att göra det. Vi har tänkt såhär att telefonen är så uppenbar, den har du i fickan och du får lov att använda telefonen privat. Vi har begränsning hur man får ringa men det är ett jätteavtal som gör att det selar egentligen ingen roll om du ringer ett samtal eller 400, det kostar lika mycket. Därför får du lov att använda den privat. Det gäller även om man surfar på telefonen, och det är därför jag känner att då bör policyn även omfatta det som vi gör med en dator när det gäller just dem där sakerna.	C,D,E

5.	Får dem anställda en telefon eller får dem ha med sig sin egen telefon, hur ser det ut när man kommer som nyanställd till er?	Man får en telefon. Det finns även anställda här som har sina egna när de kommer. Då låter vi dem ha det. Det handlar mest om att jag vill att de ska använda de mobilavtal som vi har och kommer dem med en telefon som är bunden till ett avtal privat, då blir det svårt. Kommer dem med en telefon som vi bara kan byta sim-kort är det okej med mig.	R
6.	Är ni medvetna om de olika hot och risker som smarta mobiltelefoner kan bli utsatta för?	Alltså nä. Det vore kaxigt att svara ja på det. Vi är naturligtvis inte det till fullo, det är vi inte. Visa delar vet vi om och vad jag har skrivit i policyn är att vi, i en smartphone inte ska lägga företagsinformation, vi ska inte lägga word-dokument som är relaterat till våra kunder, hemlig information.	A,B,C,D,E
7.	Det står i policyn att man inte ska göra det alltså?	Ja, det gör det. Samtidigt är det så att de flest har sin mail i smartphone. Det innebär ju att i princip ligger det redan då information på telefonen. Det är jättesvårt att leva upp till den policyn. Vi har sagt att virusskydd är inget vi kräver att ha i smartphone. Jag har aldrig hört talas om att det finns något virus till smartphone men jag vet att det finns virusskydd. Jag kan nog säga att det är en omognad från vår sida när det gäller säkerhetspolicyn.	C,D,E
8.	Är det iPhones de anställda får eller får de välja själv vilken telefon de vill ha?	Man får välja själv. Jag ser gärna en spridning därför att vi jobbar med webbutveckling och desto fler olika varianter vi har i huset desto bättre.	R
9.	Om en anställd tappar bort sin telefon eller den blir stulen, vad gör ni? Har ni några åtgärder för det?	Ja vi har åtgärder. Vi spärrar telefonen om vi kan det. Där är ju problemet att det hänger på leverantören. Har man något nummer för den. Vi kan ju spärra telefonabonnemanget, men vi kan väl egentligen aldrig spärra själva telefonen.	A
10.	Jag tänkte på sånt som ”Remote wipe” som man kan göra med iPhones exempelvis.	Det finns inget i vår policy om det.	A

11.	Om en telefon inte brukas längre. Om en anställd slutar t.ex. eller om en telefon blir väldigt sliten och ni ska göra er av med telefonen på något vis. Har ni några regler kring det, att ni exempelvis rensar telefonen.	Nej, det har vi egentligen inte. Vi följer samma regler som vi har med datorerna. Vi fabriksåterställer dem. Men, vi lämnar nästan aldrig över en telefon. Det ska vara om man slutar tidigt och då finns det en värdig telefon som man kan få, men annars är den så sliten och omodern så att vanligtvis slänger vi bort dem.	B
12.	Hur skyddar ni er mot malware, avlyssning, intrång och spyware och sådant? Ni har inget antivirusprogram?	Nej, vi har inget antivirusprogram.	C,D,E
13.	Har ni någon fysiskt skydd för telefonen som exempelvis kodlås?	Nej. Den säkerheten vi har för telefonen finns inne i vårt nät med inloggning osv.	A,E
14.	Det var nog det hela. Inget du känner du vill tillägga?	Nej, inte direkt. Det är väl egentligen bara att jag upplever det som en ganska svår bransch att se vad som gäller med säkerhet. När det gäller själva datoranvändningen, laptops och sådana saker, det har man hygglig koll på vad som kan hända och hur vi ska göra när saker och ting händer. Man glömmer väldigt gärna bort själva smartphonen. Det är ju en dator. Det har tidigare varit en telefon med sms, sen kunde man visa färg och sen kunde man surfa lite. Nu kan man ju göra precis vad som helst med den. Jag kan känna att vi här på företaget inte har hängt med där i vår policy och säkerhetstänk där utan det gjordes en omprövning av vår policy förra hösten, precis efter sommaren. Först då förde jag in smartphone i IT-policyn. Det är först nu som smartphone nämns i IT-policyn. Innan har det bara varit ad-hoc, var försiktig nu, slarva inte bort den, inget snusk.	R

15.	I er IT-policy, har ni något där om exempelvis en dator skulle bli stulen eller borttappad?	Vi har inget sådant i policyn. I policyn har vi sagt att utrustnigen ska användas på ett ansvarsfullt sätt. Det betyder: den ska inte lämnas i bilen, inte ta med den på stranden och dem bitarna. Men sen har vi en aktivitetsplan. Hur ska vi göra när olika saker händer. Där är vi fortaranade på vad som händer om hela nätet går ner eller om det börjar brinna osv. Jag är på den nivån fortfarande. Det är också en process vi håller på med. Så därför så har jag ingen aktivitet när en dator blir stulen. För i praktiken är det så att, jaha den var stulen, vi får väl polisanmäla den då. Vi får låsa kontot på den så den inte kan komma in på vårt nät men vi har inget annat. Vi har inget som kan spåra den, vi har ingen stöldmärkning på den, vi har inte kommit dit än.	R
16	Känner ni att ni har information på era telefoner som i fel händer kan göra skada för företaget?	Ja den risken finns. I och med e-posten exempelvis. Det kan ju ligga offerter som kan skada upphandlingar. Absolut, den risken finns.	A,B,C,D,E

Bilaga 8 – Transkribering företag D

Datum: 2012-05-03, Lund

Nr.	Fråga:	Svar:	Kod:
0.	Vilken titel har du på företaget?	Jag är teknisk kundansvarig.	R
1.	Hur länge har du arbetat här?	Jag har arbetat här i snart fem år, men jag har inte arbetat med detta hela tiden. Jag har suttit som teknisk kundansvarig i lite mer än ett år.	R
2.	Har ni några policys för hur era anställdas smarta mobiltelefoner får användas?	Ja.	R
3.	Hur ser den ut? Är det en specifik säkerhetspolicy eller är det en policy hur de anställda får ringa?	Nja, menar du policys som låser telefonen, hur den ska användas?	IR
4.	Ja precis, hur den ska användas för att minska olika säkerhetsrisker?	Ja vi har policys som går på varje telefon. Vi har ju vissa krav då som telefonen helt enkelt måste klara av. Exempelvis måste den klara ”Remote wipe” och den måste klara av att ha företagslås på sig	A,B,E
5.	Företagslås?	Ja, det innebär att telefonen låser sig, du måste slå in din pinkod igen efter tio minuter om du inte använt telefonen.	R
6.	Ja okej, då är jag med. Får de anställda ha sina egen telefoner på arbetet? Om man kommer som nyanställd hos er, får man en telefon då eller får man använda sig egen?	Ja, de flesta får telefon, men vi har inget som säger att man inte kan ha sin egen telefon. Många har ju även en egen telefon. Det som gäller är att telefonen stödjer den policyn som vi skjuter ut.	R
7.	Är ni medvetna om de olika hot som finns riktade mot smarta mobiltelefoner?	Ja, det är vi. Och det börjar bli allt mer. Den enda policyn vi har nu går på via Exchange. Vi har inget extra ”Management Device” som vi skjuter på mobilerna än så länge. Det är något vi håller på att kolla på och det ligger ganska högt upp på prioriteringslistan.	A,B,C,D,E
8.	Har ni några åtgärder som vidtas om en anställds telefon blir stulen eller tappas bort?	Ja, då är det ”Remote wipe” som gäller. Då blåses hela telefonen. Det kan varje användare göra via sin Outlook webaccess. Då blåses den och låses den.	A
9.	Följer där någon polisanmälan då, eller det står kanske inte skrivit?	Det vet jag inte faktiskt inte.	R

10.	Okej, men så länge det finns ”Remote wipe” är det lugnt från er sida så att säga?	Ja, precis.	R
11.	Har ni mycket känslig information på telefonerna som i fel händer kan skapa problem för företaget?	Ja, i och med att många synkar sin mail och den innehåller ofta information som kan vara företagshemlig.	R
12.	Hur hanterar ni då enheter som inte brukas längre? Om en anställd slutar eller om en telefon blir för gammal, vad händer med den telefonen då?	De har vi ingen policy för. Om det är företagets telefon lämnas givetvis telefonen tillbaka. Men det finns dem som har sin privata telefon och synkar.	B
13.	Om en anställd som har sin egen telefon slutar, måste han då rensa sin telefon på företagsinformation, eller det finns ingen skriven regel för det?	Nej, där finns inget upplagt vad jag känner till i alla fall. Men hans konto låses så han kan inte hämta ner ny information eller liknande.	R
14.	Hur skyddar ni era smarta mobiltelefoner mot malware, avlyssning och intrång.	Det blir samma svar som jag sa innan. Vi har inget sådant än så länge.	C,D,E
15.	Inget antivirusprogram?	Nej, inget sådant på mobilerna än så länge. Det är något som vi håller på att kika på. Det kommer i stort sett komma när som helst.	C,D,E
16.	Det ni har rent generellt är att telefonerna måste ha möjlighet att göra ”Remote wipe” och ha företagslås.	Ja, det stämmer.	R
17.	Annars är det fritt blås? De får lov att ladda ner vad dem vill på telefonerna?	Ja.	C,D,E
18.	Hur många anställda är ni?	Om vi snackar Sverige är vi runt 5000 anställda. I hela världen är vi runt 40 000 anställda. Men i exempelvis England kör dem bara BlackBerry och dem kör ett helt annat system.	R
19.	Vad är det för telefoner man får lov att välja på när man kommer till er?	Om man ska ha en telefon från oss så har vi ett specifikt urval. Det vi har nu är iPhone 3Gs, Nokia Lumia och HTC Wildfire S.	R
20.	Då får ni även med Android där!?	Ja precis. Där är vi lite osäkra på hur vida vi ska använda oss utav Android. Det kan bli så att vi endast ska använda oss utav Windows-phone och iOS framöver.	R
21.	Det var nog i stort sett allt. Har du något du vill tillägga?	Nej, inte vad jag kan komma på.	IR
22.	Då tackar jag så mycket!	Tack!	IR

Referenslista

Al-Zarouni M (2007): Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics. In: Proceedings of the 5th Australian Digital Forensics Conference

Check Point (2005): *Taxis Hailed as Black Hole for Lost Cell Phones and PDAs, as Confidential Data Gets Taken for a Ride.* http://www.checkpoint.com/press/pointsec/2005/01-24a.html (besökt 2012-04-12)

Europa (2006): *Definition av små och medelstora företag (SMF).* http://europa.eu/legislation_summaries/other/n26001_sv.htm (besökt 2012-05-17)

Gartner (2012): *Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth.* http://www.gartner.com/it/page.jsp?id=1924314 (besökt 2012-04-12)

Harrington J L (2005): *Network Security - A Practical Approach.* [e-bok] Okänd Ort: Morgan Kaufmann. Tillgänglig via: Lunds Universitets Bibliotek Summon, http://lu.summon.serialssolutions.com.ludwig.lub.lu.se/search?s.q=network+security+a+practical+approach&spellcheck=true (besökt 2012-04-16)

Hypponen M (2006): Malware Goes Mobile. *Scientific American.* November 2006, sid 70-77

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

Jansen W, Scarfone K (2008): *Guidelines on Cell Phone and PDA Security.* Special Publication 800-124, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf (besökt 2012-04-12)

Juniper (2012): *2011 Mobile Threats Report.* http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf (besökt 2012-04-16)

Meyer U, Wetzel S (2004): *On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Inteoperating GSM/UMTS Networks.* http://www.cs.stevens.edu/~swetzel/publications/gsm.pdf (besökt 2012-04-16)

Microsoft (2003): *Defining Malware: FAQ.* http://technet.microsoft.com/en-us/library/dd632948.aspx (besökt 2012-04-11)

Nationalencyklopedin (2012): *Datormobil.* http://www.ne.se/lang/datormobil?i_h_word=smartphone (besökt 2012-04-11)

Osborne M (2006): *How to Cheat at Managing Information Security.* [e-bok] Rockland: Syngress Publishing. Tillgänglig via: Lunds Universitets Bibliotek Summon,

http://lu.summon.serialssolutions.com/search?s.q=how+to+cheat+at+managing+information+security&spellcheck=true (besökt 2012-04-16)

Ponemon Institute (2011): *Smartphone Security, Survey of U.S. consumers.* Independently Conducted by Ponemon Institute. http://aa-download.avg.com/filedir/other/Smartphone.pdf (besökt 2012-04-11)

Post- och telestyrelsen (årtal saknas): *Integritet och säkerhet vid mobilsurf*. http://www.pts.se/sv/Telefoni/Mobil-telefoni/Mobilsurf/Integritet-och-sakerhet-vid-mobilsurf/ (besökt 2012-04-13)

SANS (2008): *Security Policy for the use of handheld devices in corporate environments.* http://www.sans.org/reading_room/whitepapers/pda/security-policy-handheld-devices-corporate-environments_32823 (besökt 2012-04-17)

US-CERT (2010): *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices.* http://www.us-cert.gov/reading_room/TIP10-105-01.pdf (besökt 2012-04-11)

Yi-Bing L, Meng-Hsun T (2007): Eavesdropping Through Mobile Phone. *IEEE Transactions on Vehicular Technology.* Vol: 56, No: 6, sid 3596-3600