HÖGSKOLAN I HALMSTAD

Affärssystemprogrammet 180hp

KANDIDATUPPSATS

Security Awareness for Mobility

En studie om företagsmobilitet och hanteringen av de säkerhetsrisker som följer

Kim Bildtmark och Robin Jädersand

Informatik 15hp

Halmstad 2015-05-25

© Copyright Kim Bildtmark & Robin Jädersand, 2015.
All rights reserved
Kandidatuppsats
Akademin för informationsteknologi
Högskolan i Halmstad

Förord

Vi vill tacka alla som på olika vis har varit delaktiga i denna studie. Utan det stöd som vi har fått hade denna uppsats inte varit möjlig att genomföra. Det har varit en intressant process med många nya erfarenheter och lärdomar.

Vi vill ge ett extra stort tack till våra handledare Magnus Bergquist, Ann Svensson och Ewa Zimmerman som har varit ett stort stöd under processen. Tack för allt arbete ni har lagt ner. Era tankar, resonemang och argumentationer har bidragit till att vi har kunnat fullfölja och slutföra denna studie.

Vi vill även tack övriga handledare; Esbjörn Ebbesson och Jesper Lund. De tillfällen vi haft med er har gett oss värdefulla synpunkter på arbetet.

Ett stort tack till de personer som agerat opponenter för oss. Ni har läst och fördjupat er i ett ämne som ni själva inte varit insatta i, tack för alla tips och råd.

Sist men inte minst vill vi tacka våra respondenter. Tack för att ni har medverkat i studien, våra möten med er har varit väldigt intressanta. Era funderingar och tankar har varit värdefulla och givande.

Kim Bildtmark Robin Jädersand

Abstrakt

Mobilitet är idag en viktig konkurrensfördel som möjliggör att företag kan arbeta mer flexibelt för att möta kunder och andra intressenters efterfrågan och behov. Företagsmobilitet handlar om friheten att kunna kommunicera vart du än befinner dig, med tillgång till rätt information vid rätt tidpunkt. Däremot skapar mobila lösningar nya säkerhetsrisker och hot för företaget och deras anställda, vilket skapar ett behov av Security Awareness. Denna uppsats undersöker hur företag bör bemöta säkerhetsrisker och hot för att säkerställa hanteringen av mobila lösningar. Undersökningen utfördes genom att ta del av dokumentation i form av IT-policys och genomföra intervjuer för att kunna besvara frågan, *”Hur kan verksamheter bemöta och öka medvetenheten kring de säkerhetsrisker som medföljer företagsmobilitet?”*. Undersökningen resulterade i rekommendationer för hur företag bör arbeta för att öka medvetenheten kring säkerhetsrisker och hot.

Nyckelord: Mobilitet, Säkerhetsrisker och Hot, Bemötande, Medvetenhet för Säkerhetsrisker

Abstract

Today mobility is an important competitive advantage that enables companies to work more flexible, in order to meet customer and other stakeholders needs and demands. Enterprise mobility is about having the freedom to be able to communicate wherever you are, and having access to the right information at the right time. However, mobile solutions create new security risks and threats for companies and their employees, thus creating a need for security awareness. This paper examines how companies should respond to security risks and threats to ensure the management of mobile solutions. A survey was conducted, by taking part of IT-policies. Also, an interview was conducted in order to answer the question *"How can businesses respond to and raise awareness of the security risks that come with business mobility?”*. The study resulted in practical recommendations for how companies should work to raise awareness of security risks and threats.

Keywords: Mobility, Security Risks and Threats, Response, Security Awareness

Innehållsförteckning

1 Inledning 1
1.1 Syfte 2
1.2 Avgränsningar 2
2 Litteratur 3
2.1 Mobilitet och användandet av mobila lösningar 3
2.2 Bring Your Own Device (BYOD) 4
2.3 Säkerhetsrisker och hot 4
2.4 IT-strategier och policys 5
2.5 Mobile Device Management (MDM) 7
2.5.1 Riskkällor 8
2.5.2 Tillgångar 8
2.5.3 Skadliga handlingar 8
3 Metod 9
3.1 Vetenskaplig ansats 9
3.2 Litteraturstudie 9
3.3 Urvalskriterier 10
3.3.1 Företag 10
3.3.2 Respondenter 11
3.4 Datainsamling 12
3.5 Analysmetod 13
3.6 Metoddiskussion 15
3.7 Etiska överväganden 16
4 Resultat 18
4.1 Strategier och policys 18
4.1.1 IT-policys 18
4.1.2 Mobila policys 19
4.1.3 Användarcentrerade policys 19
4.1.4 Företagens förhållningssätt till strategier och policys 20
4.1.5 Sammanfattning 22
4.2 Hanteringen av mobila lösningar 22
4.2.1 Betydelsen av mobila lösningar 22
4.2.2 Autentisering för åtkomst 23
4.2.3 Metoder för att säkerställa hanteringen av mobila lösningar 24
4.2.4 Sammanfattning 26
4.3 Säkerhetsrisker och hot 26
4.3.1 Upplevda säkerhetsrisker och hot 26
4.3.2 Privat- eller företagsägda enheter 27
4.3.3 Användaren som ett hot 28
4.3.4 Användarens eget ansvar 29
4.3.5 Sammanfattning 30
5 Analys 31
5.1 Bemöta säkerhetsrisker - ur ett policyperspektiv 31
5.2 Bemöta säkerhetsrisker - ur ett tekniskt perspektiv 32
5.3 Bemöta säkerhetsrisker - ur ett utbildningsperspektiv 34
5.4 Bemöta säkerhetsrisker - ur ett användarperspektiv 35
6 Diskussion 37
7 Slutsats 40
7.1 Rekommendationer 40

7.2 Vidare forskning **41**

Tabellförteckning

Tabell 1 - Respondenter **12**

1 Inledning

Marknadens ständigt ökande konkurrens leder till att företag idag måste arbeta mer flexibelt för att möta kunder och andra intressenters efterfrågan och behov. Under senare tid har mobilitet växt fram till att bli en affärskritisk faktor för att lyckas med att bedriva en mer flexibel verksamhet och möta kundernas behov (Harris & Patten, 2014). Enligt Basole (2007) har mobila företag blivit en allt vanligare organisationsform som resulterat i ett paradigmskifte. Företagsmobilitet handlar om friheten att kunna kommunicera var än du befinner dig, med tillgång till rätt information vid rätt tidpunkt (Harris & Patten, 2014). Anställda spenderar mer tid ute hos kund och allt mindre tid på sin arbetsplats. Detta kräver att anställda har tillgång till ständigt uppdaterad information som kan svara på kundens frågor, vilket har resulterat i att många privata mobila enheter används i arbetssyften. Detta har blivit ett fenomen som organisationer kallar för ”Bring Your Own Device”, något som i sin tur kan resultera i både fördelar och nackdelar. Under senare år har ny teknologi inom mobilitet inspirerat många företag till att använda sig av mobila lösningar (Sybase, 2011). Den mobila teknologin syftar i denna studie till mobila lösningar på en smartphone eller surfplatta. Dessa mobila enheter används för att få tillgång till en mängd olika tjänster, bland annat banktjänster och sociala medier. De används även i arbetsändamål för att kunna få tillträde till exempelvis information om lagerstatus från företagets affärssystem, eller kunna ta del av kundinformation från företagets CRM-system (Customer Relation Management) (Jain & Shanbhag, 2012).

Även om möjligheterna är många skapar de mobila lösningarna nya säkerhetsrisker för företag och deras anställda (Harris & Patten, 2014). Applikationer med information som lagras på smartphones och surfplattor är sämre skyddade från att obehöriga gör intrång jämfört med de flesta stationära och bärbara datorer (Ben-Asher, Ben-Oved, Kirschnik, Meyer, Móller & Sieger, 2011; Jain och Shanbhag, 2012). Säkerhetsintrång av detta slag kan resultera i att företag förlorar sina konkurrensfördelar eftersom att obehöriga kommer åt känslig information. Tidigare studier visar även att intrång kan resultera i att företag förlorar sina kunder och partners förtroende. Det kan samtidigt leda till att deras varumärke skadas samt att deras möjlighet att utföra vardagliga arbetsuppgifter försämras (Sybase, 2011).

För att hantera säkerhetsaspekten krävs nya och anpassade säkerhetsstrategier (Harris & Patten, 2014). IT-strategier, om de implementeras, bör tillhandahålla och upprätthålla ramverk för att kunna möta företagets syfte och mål (Dubey, 2010). Många företag väljer däremot att inte implementera heltäckande IT-strategier, på grund av kostnaden och komplexiteten för detta (Sybase, 2011). Företag står därför idag inför valet av att antingen använda sig av den mobila teknologin eller inte. För att kunna göra detta val måste företagen ha tillräckligt med kunskap och medvetenhet kring säkerhetsaspekten, även kallat *Security Awareness,* och hur arbetet bör gå tillväga för att bemöta säkerhetsriskerna (Bulgurcu, Cavusoglu & Benbasat, 2010; Harris & Patten, 2014). Befintlig forskning har fokuserat på hur säkerhetsrisker och hot bör hanteras rent tekniskt. Däremot saknas forskning som undersöker hur

medvetna företag och de anställda är kring säkerhetsrisker vid användande av mobila lösningar och hur medvetenheten kan ökas för att bemöta riskerna (Harris & Patten, 2014).

Vår frågeställning är således följande: *Hur kan verksamheter bemöta och öka medvetenheten kring de säkerhetsrisker som medföljer företagsmobilitet?*

1.1 Syfte

- Redogöra för hur företag och anställda använder och upplever sina mobila lösningar, vilka säkerhetsrisker de har identifierat och hur de arbetar för att säkerställa hanteringen av mobila lösningar.

- Ta fram rekommendationer för hur arbetet med säkerhetsrisker och hot för mobila lösningar bör se ut för att öka medvetenheten hos företag och anställda om de risker som medföljer användningen av mobila lösningar.

1.2 Avgränsningar

Avgränsningen i vår studie är till företag som använder sig av mobila lösningar utanför företagets arbetsplats, exempelvis ute hos kund.

2 Litteratur

2.1 Mobilitet och användandet av mobila lösningar

Mobilitet har kommit att bli en norm, där smartphones och surfplattor är de nya mobila informationssystemen som de flesta människor i världen använder (Middleton, Scheepers & Tuunainen, 2014). Men den mobila eran startade redan under slutet av 80-talet när den första nätverksbaserade persondatorn utvecklades. Sedan dess har utvecklingen fortlöpt och idag erhålls dataåtkomst genom en mängd olika mobila enheter. Alla dessa är sammanlänkade genom antingen privata, lokala eller globala nätverk. Kombinationen av de nya och kraftfulla enheterna som är anslutna till höghastighetsnät ger en kraftfull digital infrastruktur som öppnar upp för nya möjligheter (Sörensen, 2014). Utvecklingen har möjliggjort att de mobila enheterna stödjer fler funktioner än tidigare, vilket har ökat användningen för flera olika ändamål, till exempel inom kommunikation, informationssökning, underhållning och navigation. I motsats till starten av den mobila eran då mobil åtkomst skedde via webben och främst användes i affärssammanhang, har dagens konsumentvänliga och mångsidiga smartphones och surfplattor gjort det möjligt för alla människor att tillgodose dessa ändamål (Middleton et al., 2014).

Enligt Harris och Patten (2014) väljer även allt fler företag att omfamna och integrera den nya mobila tekniken, då dessa lösningar har blivit en allt mer affärskritisk aspekt för att kunna skapa sig konkurrensfördelar. Men detta har inte alltid varit en självklarhet. I början av 2000-talet, när företag först började utvärdera möjligheterna med den nya mobila tekniken, ansågs teknologin fortfarande vara i ett tidigt stadium och den misslyckade ofta att leverera den förväntade nyttan (Basole, 2007). Många ansåg att den mobila tekniken var alltför outvecklad för att kunna användas och ge fördelar i form av effektiviserade affärsprocesser. Fördelarna som sedan dess växt fram handlar framförallt om tillgång till rätt information vid rätt tidpunkt. Anställda som arbetar ute hos kund kan vara direkt uppkopplade till de resurser som företaget förfogar över genom att använda mobila enheter. Dessutom kan mobilitet ersätta traditionellt arbete, till exempel pappersbaserat arbete, och kan också reducera potentiella fel som kan uppstå vid förmedling av data och information via telefon tillbaka till kontoret. Det kan med andra ord leda till en högre grad av pålitlig data och integritet. De mobila lösningarna kan också innebära kostnadsbesparingar i och med att företag slipper investera i dyra och stationära IT-lösningar (Basole, 2007).

Mobilitet skapar många fördelar som företag kan ha nytta av, men det medför också nackdelar, framförallt gällande säkerhetsaspekten. I och med att mobilitet blivit en viktig del i företagens arbetsstruktur måste företagen samtidigt hantera de mobila säkerhetsriskerna. För att åstadkomma detta behövs kunskap om vilka risker som existerar (Sybase, 2011). Inom den mobila tekniken uppstår säkerhetsrisker huvudsakligen inom fyra områden:

- Risk för privat och arbetsrelaterad användning på en och samma enhet
- Stulen eller borttappad enhet
- Otillåten datatillgång
- Brister i hanteringen av enheter gentemot företagets policy

2.2 Bring Your Own Device (BYOD)

En anledning till att risker har ökat är det allt mer förekommande fenomenet Bring Your Own Device (BYOD). Med BYOD menas användande av en privat enhet i företagssyfte. Problemet är att privata enheter även används för vardagliga ändamål, vilket resulterar i att företag på så vis har begränsad möjlighet att kontrollera och övervaka användningen (Souppaya & Scarfone, 2013). Fenomenet skapar problem genom att anställda köper egna enheter och ber IT-avdelningen koppla upp dessa till företagets nätverk och funktioner. Detta skapar i sin tur nya säkerhetsproblem genom att de privata enheterna är mer mottagliga för virus och skadlig kod vilket utsätter företaget för en risk när enheten kopplas upp mot företagets nätverk. Detta är säkerhetsproblem som IT-avdelningen måste hantera och åtgärda. Traditionellt sett skedde support enbart på företagsägda enheter av IT-avdelningen. Detta berodde på att företagen endast hade budget till att ge en mindre del av personalen möjligheten till en mobil enhet att använda i företagssyfte. Företag förbjöd även användning av privata enheter i avseende att minimera dessa säkerhetsrisker (Lopez, 2010).

Trots att företag har sina restriktioner och IT-policys gällande vilka mobila enheter som får användas, kvarstår problemet med privata enheter. Det finns många orsaker till att privata enheter används. En anledning kan vara att anställda tar med sina privata enheter i protest mot företagets totala förbud mot dessa. En annan anledning är att anställda vill ha tillgång till mobilitet på arbetstid även om företaget inte har resurser att erbjuda en företagsägd enhet. Även om företaget erbjuder en mobil enhet vill den anställde ha tillgång till sin privata enhet, vilket innebär två enheter i fickan, ett problem som många anställda upplever (Lopez, 2010). Den ökande användningen av smartphones och surfplattor i företag innebär att IT-avdelningen inte längre kan ignorera säkerhetsproblemen som BYOD kan resultera i. Ett företag kan antingen välja att använda en restriktiv policy, vilket ändå kan leda till säkerhetsöverträdelser, eller så omformas policys och strategier som tillåter IT-avdelningen att omfamna och förbättra användningen av privata enheter. BYOD har framkommit på grund av dåligt hanterade IT-policys, men idag kan det vara klokt och till och med bra för verksamheter att acceptera fenomenet (Lopez, 2010). Företag måste se fördelen och nyttan med BYOD eftersom det leder till ökad produktivitet och tillfredsställelse hos anställda, vilket i sin tur resulterar i högre inkomster och en bättre arbetsmiljö (Caldwell, Zettmann & Griffin, 2012).

2.3 Säkerhetsrisker och hot

Den ökande användningen av smartphones och surfplattor hos företag har ökat riskerna för att värdefull information läcker ut på grund av borttappade eller

missbrukade enheter (Rhee, Won, Jang, Chae & Park, 2012). Enligt Basole (2007) finns en mängd olika frågor som knyter an till säkerhet, vilket både Ben-Asher et al. (2011) och Sybase (2011) bekräftar genom att visa på vanligt förekommande risker med att använda sig av mobila lösningar. De risker som identifierats är till exempel: stulen eller borttappad mobil enhet, dataintrång, företagsanvändning av privat mobiltelefon (BYOD) och otillräckliga föreskrifter och policys kring användandet av mobila enheter. Harris och Patten (2014) ger andra exempel på risker och hot som företag kan tänkas utsättas för. Det kan till exempel vara virus på operativsystem genom användning av olika applikationer. Det kan också innebära risker i form av jailbreaking och rooting, vilket handlar om att mobila enheter öppnas upp av användare för att få tillgång till hela operativsystemet som i sin tur ökar risken för virus.

De flesta av dagens mobila enheter saknar funktioner som är tillförlitliga, till exempel säkra plattformsmoduler. Mobila enheter är utformade för att enkelt hitta, installera och använda tredjeparters applikationer. Detta resulterar i uppenbara risker, speciellt för mobila plattformar (till exempel Android OS) och applikationsbutiker (till exempel Google Play) som inte använder sig av säkerhetsåtgärder eller andra begränsningar vid publicering av nya tredjeparters applikationer (Souppaya & Scarfone, 2013).

En mer grundläggande säkerhetsrisk med mobilitet är att företag som integrerar sitt informationssystem med mobila enheter alltid möter en viss risk med trådlös kommunikation. Desto mer de mobila lösningarna stödjer affärsprocesser, desto mer ökar mängden av känslig information som skickas mellan mobila enheter. Allt som skickas trådlöst innebär en risk för att obehöriga får åtkomst (Androulidakis & Papapetros, 2008). Här kan en metod som heter packet sniffing utgöra ett hot, vilket handlar om att hacka och komma åt information som skickas trådlöst via nätverk (Rhee et al., 2012). Alla de nya säkerhetsriskerna som identifierats ställer samtidigt krav på företagens ”*Security Awareness”*. Begreppet security awareness handlar enligt Bulgurcu et al. (2010) om en individs kunskap och kännedom om företagets säkerhet och hantering kring information. Vidare menar Furnell (2008) att utmaningen för ett företag är att försäkra sig om att användare vet vilka risker som utgör ett hot och när användaren bör vara försiktig. För ett företag handlar det om att öka medvetenheten och kunskapen för situationer där användare är benägna att bortse från säkerhet och begå misstag. Nyckeln till en säker hantering är genom utbildning och medvetenhet för den mobila tekniken vilket är grundläggande för att ett företag ska kunna ha en gemensam förståelse och tänkande kring den IT-strategi och säkerhetsarbete som bedrivs (Furnell, 2008).

2.4 IT-strategier och policys

För att garantera att den nya tekniken fungerar på ett säkert sätt behöver företag utforma nya säkerhetsstrategier för användningen av mobila enheter i verksamheten (Harris & Patten, 2014). Många företag har infört mobila lösningar utan att

implementera heltäckande IT-strategier på grund av att det anses vara dyrt och komplicerat (Sybase, 2011). Syftet med en IT-strategi är att på bästa sätt tillhandahålla system som är effektiva, pålitliga och flexibla, och som möter dagens och framtida verksamheters behov och krav. IT-strategier bör tillhandahålla och upprätthålla ramverk för att kunna möta företagets syfte och mål (Dubey, 2010). Utan IT-strategier och policys, som kan ställa krav på användningen av mobila enheter, riskerar företag att olika säkerhetsrisker och hot förbises. Ett företags säkerhetsstrategi ska utgå från IT-principer som till exempel skyddar känslig information om företaget och kunder, att regler följs, och för att hålla en hög säkerhetsnivå gentemot marknadens standard. Säkerhetsstrategier handlar inte om tekniska val, utan bör istället spegla företagets mission, övergripande strategi, affärsmodell och bransch (Pearlson & Saunders, 2013).

De policys som upprättas bör därför omfatta mobilitet för att säkerställa företagets information. Dessa säkerhetspolicys bör också uppmuntra standardisering och integration, där best-practice ska följa företagets övriga IT-policys och gå hand i hand. Utifrån den utarbetade säkerhetspolicyn bör företaget utveckla underliggande och mer detaljerade policys för hur hanteringen av specifika områden ska gå tillväga, till exempel för Internet-användning och autentisering. Policys måste följa en viss balans mellan de säkerhetsåtgärder som ska följas gentemot produktivitet och användarupplevelse, så att åtgärderna inte hämmar användaren i dess arbete. En sådan åtgärd kan till exempel vara fingeravtryck för autentisering. Denna funktion ökar både säkerheten för åtkomst av data samt användarvänligheten (Gao, Hu, Cao & Li, 2014). När säkerhetspolicys tas fram är det därför viktigt att både användar- och IT-perspektivet beaktas. Användare måste vara tydliga med vad de vill att säkerhetsåtgärderna ska hantera och hur de ska stödja dem i sitt vardagliga arbete, medan IT-avdelningen har kunskapen om vilka möjligheter och begränsningar som finns för respektive säkerhetsproblem. För att säkerställa att säkerhetspolicys följs behöver användarna vara väl införstådda med de riktlinjer som finns (Pearlson & Saunders, 2013). Att säkerhetsrisker förbises, menar även Harris och Patten (2014), kan relateras till bristande medvetenhet och förståelse för riskerna.

Nyckeln till en säker användning ligger i att företag och de specifika användarna är medvetna om riskerna samt är noga med att använda sig av rätt säkerhetsfunktioner och strategier (Ben-Asher et al., 2011). En säkerhetsåtgärd kan till exempel vara att ett företag har möjlighet att komma åt data i sina anställdas mobila enheter var de än befinner sig, för att begränsa eller ta bort känslig data om företaget (Sybase, 2011). Företag måste integrera säkerhetstänkandet redan i utvecklingsfasen av mobila applikationer för att kunna skydda sig själva från potentiella risker och hot. Säkerhetstänkandet bör integreras och nå ut till användare genom olika kommunikationskanaler och relevant medvetenhet om säkerhet måste uppmuntras mer aktivt från företaget. Problemet med medvetenhet löser sig inte självt även om vi idag ser en ny generation av mer IT-intresserade användare ute hos företag (Furnell, 2008). Genom att integrera säkerhetstänkandet i ett tidigt skede kan företag minska kostnaderna av tidskrävande och dyra åtgärder i ett senare skede om en användare

begått ett misstag (Jain & Shanbhag, 2012). För att hantera säkerhetsrisker finns även olika system för IT-strategi som stödjer användning av mobila enheter i ett företag, dessa kallas för *Mobile Device Management Systems (MDM-system)* (Rhee et al., 2012).

2.5 Mobile Device Management (MDM)

Många företag applicerar idag MDM-system för att övervaka och kontrollera funktionalitet och användning av smartphones och surfplattor. På senare tid har det blivit allt vanligare att företagets konfidentiella och känsliga information läckts ut via mobila enheter, vilket har gjort att fler företag börjat använda sig av MDM-system för att kunna motverka detta. Systemen har som övergripande syfte att hantera och lösa säkerhetsproblem vid användning av mobila enheter, samt övervaka och kontrollera status och funktioner hos en mobil enhet, trådlöst, genom Over-the-Air (OTA) eller Wi-fi. För att en organisation ska kunna säkerställa att användningen av ett MDM-system ger önskad nytta bör organisationen se över fyra olika riktlinjer. Dessa är säkerhetspolicys, datakommunikation och lagring, användare och enhetsautentisering samt applikationer (Souppaya & Scarfone, 2013). Dessa fyra riktlinjer beskrivs mer detaljerat nedan.

- **Säkerhetspolicy** – Det ska finnas policys som beskriver: begränsning av användarnas tillgång till hård- och mjukvara, hantering av nätverksgränssnitt, hur övervakning av användningen ska se ut samt hur rapportering av regelbrott mot policyn ska utföras.

- **Datakommunikation och lagring** – Företaget ska stödja: en krypterad och säker datakommunikation och lagring, hur enheter ska rensas innan den används av ny användare, kunna rensa mobila enheter på distans om den blir borttappad eller stulen.

- **Användare och enhetsautentisering** – Det ska finnas krav på: verifiering av användaren innan åtkomst till företagets databas och information, återställning av bortglömda lösenord på distans, kunna spärra enheter som misstänks vara lämnade olåsta i en oskyddad miljö.

- **Applikationer** – Vilka applikationer och program som installeras på en enhet bör begränsas, men också varifrån de kan laddas ned. Även vilken behörighet användare tilldelas ska göras tydligt. Användare ska också kunna verifiera sig genom någon typ av digital signatur för användning av applikationer i den mobila enheten.

Enligt Rhee et al. (2012) bör programmerare och systemutvecklare även överväga samtliga hot och säkerhetsrisker som ett MDM-system ska kunna hantera, annars är risken stor att systemet inte kan tillhandahålla tillräckligt med säkerhet. Dessutom måste det finnas kunskap om potentiella risker, vilket också är kritiskt för att kunna utforma säkerhetsfunktioner i ett MDM. Det finns olika riskkällor, tillgångar och skadliga handlingar som möjliggör att en risk uppstår. Vid användning av ett MDM-system är det viktigt att identifiera förhållandet mellan dessa tre objekt, för att sedan kunna definiera vilken karaktär risken är av och vilken åtgärd som ska utföras för att

hantera den. Riskkällorna som Rhee et al. (2012) anser kan möjliggöra att risker uppstår förklaras nedan.

2.5.1 Riskkällor

Administratör – är den systemansvarige för MDM-systemet. Administratören måste ha tillräckligt med kunskap om systemet och hur det fungerar. Denna person är generellt sett välutbildad i systemet. Personen i fråga måste vara pålitlig med tanke på vilken behörighet och tillgång denne har till systemet, vilket samtidigt kan utgöra ett hot.

Användare – är den som använder den mobila enheten, MDM-systemet och företagets applikationer. I och med denna tillgång utgör användaren ett hot mot företaget. Generellt sett är en användare inte tillräckligt kompetent för att utgöra någon fara i form av att attackera systemet. Men en användare kan utgöra ett hot genom att försöka få tillgång till information som den inte har behörighet till.

Obehörig person – är oftast datahackare eller konkurrenter och deras virus. De är också experter på att attackera säkerhetssystemen. Dessa personer har ofta tillräckligt med resurser för att skada företaget och handlar avsiktligt. En obehörig person kan också vara upphittaren av en borttappad enhet. Denna person är ofta inte en expert och har inte tillräcklig kunskap för att utgöra ett hot.

Omgivningen – är hot som utgörs av naturen, till exempel jordbävning, översvämning, bränder och har stora möjligheter att skada systemet.

2.5.2 Tillgångar

Tillgångar utgörs av enheter som har ett subjektivt värde. Detta värde definieras som det kommersiella värdet men kan variera beroende på företag. Tillgångar kan till exempel vara en kunds privata information i en anställds mobila enhet och ha ett högt kommersiellt värde. Värdet på tillgången ska bestämma vilken nivå av säkerhet den ska ha och hur mycket resurser den ska delges. Värdet bestäms av fyra principer: confidentiality, integrity, availability och autenticity som tillsammans kallas för CIAA (Rhee et al., 2012).

2.5.3 Skadliga handlingar

Skadliga handlingar utgörs av en riskkälla på en tillgång. Dessa handlingar utnyttjar systemets sårbarhet, vilket till exempel kan vara dålig design och utveckling eller otillräckliga säkerhetspolicys och rutiner. Generellt sett finns det olika typer av skadliga handlingar så som packet sniffing, SQL injektioner (användaren kringgår inloggningssystem och manipulerar data), password dictionary attack (teknik för att ta fram rätt lösenord genom att slumpa alla ord i ett lexikon) samt olika typer av virus (Rhee et al., 2012).

3 Metod

3.1 Vetenskaplig ansats

Vår undersökning har haft för avsikt att skapa en djupare förståelse för hur säkerhetsrisker och hot vid användning av mobila lösningar bemöts i organisationer. Syftet har varit att redogöra för hur organisationer och anställda använder och upplever sina mobila lösningar, men syftet har också varit att ta fram rekommendationer för hur säkerhetsrisker bör bemötas. Vår frågeställning var således *Hur kan verksamheter bemöta och öka medvetenheten kring de säkerhetsrisker som medföljer företagsmobilitet?* För att få denna förståelse och kunna svara på vår frågeställning valde vi en kvalitativ ansats. En kvalitativ ansats har som mål att komma nära människor för att få en djupare förståelse för den data som samlas in. En kvalitativ ansats består av olika metoder som kan kopplas till intervjuer, observationer och analys av text. Genom att kombinera och analysera olika datakällor (litteratur, dokumentation och empiri), en så kallad datatriangulering, finns det möjlighet att belysa problemområdet ur ett helhetsperspektiv (Yin, 2013). Jämfört med en kvantitativ studie använde vi oss av ett mindre urval eftersom kvalitativa tillvägagångssätt tenderar att vara exponentiellt tidskrävande i alla steg som ska utföras (Denscombe, 2009). Exponentiellt tidskrävande handlar i kvalitativa studier om att det ofta tar längre tid att utföra framförallt datainsamling än vad en kvantitativ studie ofta gör. Därför har vi valt att hålla oss till ett mindre urval i denna undersökning. Samtidigt som vi har en kvalitativ ansats har undersökningen haft inslag av en normerande ansats, vilket vår frågeställning och syfte implicerar. En normativ undersökning söker ofta svar om hur något bör vara och hur det kan rättfärdigas (Badersten, 2006).

3.2 Litteraturstudie

Litteraturstudien har genomförts med hjälp av artikeldatabaserna IEEE Xplore, Emerald Insight och Google Scholar. Vi fokuserade till en början på att försöka hitta artiklar kring säkerhetsrisker och hot kopplat till mobilitet. De söktermer vi först använde var *mobility, security risks and threats, security concernss, mobile* devices. Till en början lästes allt som hade med huvudämnet samt sidoämnena att göra, men efterhand som vi fick mer kunskap begränsades de artiklar som valdes ut för att höja relevans och matcha vårt problemområde. Följande sökord användes därefter, i olika kombinationer: *mobility, mobile devices, business mobility, bring you own device (BYOD), security concerns, security awareness, IT-strategy, enterprise mobile management, mobile device management*.

Vi har fokuserat på artiklar där företagsmobilitet har berört användning och säkerhetsrisker för att begränsa oss, och samtidigt för att få fram den mest relevanta informationen för vår studie. Vidare har sökningarna inriktat sig på befintliga metoder och tillvägagångssätt för att hantera de säkerhetsrisker och hot som vi genom befintlig forskning har kunnat identifiera inom mobilitet. I de fall där sökningarna

resulterat i relevanta artiklar för vår studie har vi även läst igenom referenslistorna i syfte att hitta ytterligare användbara artiklar inom området. Detta har gjorts både för att kunna styrka och bestrida den forskning vi redan har funnit. Artiklarna som vi använt oss av i litteraturstudien har legat till grund för vår empiriska undersökning och våra intervjufrågor.

Genom vår litteraturstudie upptäckte vi framförallt att tidigare forskning fokuserar på tekniska lösningar som finns för att upprätthålla en säker användning av mobila lösningar. Det som saknas är forskning som visar på hur företag ska arbeta med den mänskliga faktorn. Detta kan med andra ord beskrivas som företaget och de anställdas medvetenhet kring säkerhetsriskerna och hur de ska arbeta med sina mobila lösningar för att upprätthålla en säker användning.

3.3 Urvalskriterier

För att kunna undersöka vår frågeställning gjordes urval för att komma åt rätt information. Det första urvalet vi gjorde var att begränsa oss till tre företag i undersökningen. För att få en helhetsbild valde vi sedan att intervjua två olika roller i vardera företag, en IT-ansvarig som motsvarade den strategiska nivån och som ansvarade för företagets IT-policys. Den andra rollen vi valde att intervjua var anställda på operativ nivå som representerade användarna av företagets mobila lösningar. Förutom en empirisk undersökning i form av intervjuer ville vi också ta del av företagens dokumentation gällande IT-policys. I och med att vi valde att genomföra två intervjuer på vardera företag samt analysera deras policys ansåg vi att tre företag var tillräckligt för att kunna undersöka vårt problemområde. Med andra ord genomförde vi sex intervjuer samt analyserade företagens olika IT-policys. De företag som medverkat i undersökningen var alla tillverkande företag i olika branscher. De verkar inom sjukvård, industriell kommunikation och storkök- och restaurangutrustning. Företagen valdes enbart utefter kriterierna att de har mobila lösningar som används på operativ nivå ute hos kund samt att företagen använder sig av IT-policys och har någon ansvarig för detta.

3.3.1 Företag

De företag som medverkar i denna undersökning har valts ut utefter tidigare nämnda kriterier. Dessa kriterier var att de måste använda sig av en eller flera mobila lösningar. De mobila lösningarna var också tvungna att användas av säljare eller tekniker eftersom vi ville jämföra hur strategisk- och operativnivå ser på säkerhetsriskerna. Vidare hade vi som kriterier att företagen skulle ha en IT-policy för att kunna se hur företagen vill att hanteringen av mobila lösningar ska se ut samt hur deras policys är utformade. I två av sex intervjuer deltog fler än en respondent. Anledningen till detta var att företagen ansåg att de behövde fler personer som deltog för att kunna svara på våra intervjufrågor som de mottagit inför intervjun. Därför har fler än sex respondenter deltagit i undersökningen (se *Tabell 1 – Respondenter* s. 13). Av anonymitetsskäl har vi valt att använda fiktiva namn på både företag och

respondenter samt att inte nämna företagets exakta storlek då vi anser att det kan avslöja företagets identitet.

Voondo är ett företag som bedriver både tillverkning och erhåller tjänster inom medicinsk utrustning. Voondo har över 250 anställda och i Sverige har de sitt kontor beläget i Halmstad.

Mire är ett tillverkande företag inom teknik och industriell kommunikation. De har över 250 anställda och deras produktion sker på flera platser i världen men huvudkontoret finns beläget i Halmstad.

Kando är ett tillverkande företag inom storköksutrustning. Deras produktion och kontor finns beläget i Halmstad och de har 10-50 anställda.

3.3.2 Respondenter

För att få ett bredare perspektiv på säkerhetsriskerna valde vi att intervjua olika roller i företaget, både anställda på operativ- och strategisk nivå. Ett kriterium för studien var därför att företagen hade säljare eller tekniker ute hos kund som kunde representera den operativa nivån. Anledningen till detta var att vi till en början upplevde att säljare och tekniker framförallt är de personer som använder mobila lösningar i sitt dagliga arbete. Tillsammans med dessa två roller valde vi att även intervjua företagets IT-ansvarig, som motsvarade den strategiska nivån (se *Tabell 1 – Respondenter* s. 13). Företagen skulle även använda sig av mobila enheter i form av smartphones eller surfplattor. Syftet med intervjuerna var att öka informationsvärdet, och därför var det viktigt att deltagarna medvetet valdes ut baserat på deras relevans för studien (Holme & Solvang, 1997).

När vi bestämde urvalet av respondenter använde vi ett subjektivt urval. Vi "handplockade" personer hos de företag som uppfyllt våra kriterier för studien. Vi hörde med andra ord av oss till företagen och informerade om vår undersökning och vilka personer vi letade efter. Med företagets hjälp fick vi kontakt med de personer som var relevanta att intervjua och som uppfyllde våra kriterier. Fördelen med ett subjektivt urval är att det tillåter forskaren att närma sig människor eller företeelser som forskaren på goda grunder kan anta vara avgörande för undersökningen. Denscombe (2009) beskriver ett subjektivt urval som processen där forskaren väljer ut personer med ett speciellt syfte i åtanke, och detta syfte återspeglar de utvalda människornas kvaliteter och relevans för studien.

Tabell 1 – Respondenter

Företag	Namn	Befattning
Voondo	Thomas	IT-ansvarig
	Nils	IS-ansvarig
	Sven	Processägare
	Richard	Tekniker
Mire	Mattias	IT-chef
	Niklas	Säljare
Kando	Peter	VD och IT-ansvarig
	Olle	Serviceledare och koordinator
	Gustav	Tekniker

3.4 Datainsamling

För vår undersökning studerades olika källor, samtliga kopplade till säkerhet kring mobila lösningar. Det var också genom att studera källor med likartade preferenser som hjälpte oss att fastslå vårt unika problemområde (Denscombe, 2009).

För att få svar på vår frågeställning och uppnå syftet med vår undersökning valde vi att använda oss av intervjuer som insamlingsmetod. Enligt Kvale och Brinkmann (2014) söker forskningsintervjun kvalitativ kunskap och syftar inte till kvantifiering. Syftet med en kvalitativ, intervju-baserad metod är att klargöra och kunna beskriva deltagarnas upplevelser och erfarenheter kring det område som utforskas (Schultze & Avital, 2011; Kvale & Brinkman, 2014). När det gäller intervjuer och de frågor som ska ställas, måste också graden av standardisering och strukturering beaktas - hur mycket är tolkningsbart för respondenten själv och hur mycket "svarsutrymme" finns i frågorna. En intervju som är helt standardiserad och strukturerad har frågor som är bestämda i förväg och som ställs i en viss ordning utan utrymme till förklaring (Patel & Davidson, 2003). Eftersom vi har valt en kvalitativ ansats för vår undersökning ville vi därför lämna utrymme i våra intervjufrågor till respondenterna att utveckla sina svar men samtidigt använda en viss struktur för att kunna fokusera på vårt identifierade problemområde. Enligt Patel och Davidson (2003) är en intervju som är helt utan struktur och standardisering således det motsatta. Intervjuaren skapar sig då sina frågor och den ordning de ställs i under intervjuns gång och anpassar sig efter situationen och vad som är lämpligt för respondenten för tillfället.

För att komma åt rätt information valde vi därför att använda oss av semi-strukturerade intervjuer. Denna struktur på intervjuer möjliggjorde att vi kunde utgå från förutbestämda frågor samtidigt som den gav utrymme till att deltagare fick chans att vara mer öppna i sina svar och på så vis kunde utveckla sina idéer och tankar. Semi-strukturerade intervjuer möjliggjorde även att vi fick chans att ställa följdfrågor på de svar vi fick, vilket resulterade i att mer kvalitativ data samlades in (Kvale &

Brinkmann, 2014; Myers & Newman 2007). För att komplettera våra följdfrågor använde vi oss av Kvale och Brinkmanns teori (2014) med sonderande frågor. Det betyder att vi uppmanade deltagare till att svara mer detaljrikt och ge exempel, för att vi som intervjuare enklare skulle förstå. Efter varje genomförd intervju såg vi över den information vi tagit del av för att se om vi behövde omforma vårt material och våra frågeställningar till nästkommande intervju.

Våra intervjufrågor (se bilaga 1) togs fram baserat på tidigare skriven litteratur som vi valt att inkludera i vår litteraturstudie. Intervjufrågorna hade för avsikt att skapa klarhet i hur anställda tänker och ser på säkerhetsaspekten kring de mobila lösningar som används. Frågorna delades därför in i tre olika teman: hantering av mobila lösningar, säkerhetsrisker och hot, samt strategier och policys. Detta gjorde vi för att underlätta för respondenterna då vi fick en röd tråd genom hela intervjun. Respondenterna fick också en bättre överblick över de frågor vi tänkt ställa. Varje tema bestod sedan av fem till sex olika frågor som representerade temat och de delar som vi ansåg vara väsentliga att få svar på kopplat till vår frågeställning. Intervjumaterialet mailades till sist ut till respondenterna i god tid innan intervjuerna för att de skulle vara väl införstådda i ämnet och känna sig förberedda.

Intervjuerna genomfördes på plats hos företagen, med undantag från en intervju som genomfördes via telefon. Till vardera intervju hade vi avsatt minst en timme vilket i efterhand också visade sig rimligt. En av intervjuerna genomfördes på telefon på grund av att respondenten arbetade som tekniker och alltid befann sig ute på fält. Denna intervju varade endast 30 minuter och blev en aning abstrakt. Detta kan bero på att en telefonintervju tenderar till att enbart hålla sig till intervjumaterialet och inte uppmuntrar till detaljrika och utvecklande svar (Jacobsen, 1993). De andra fem intervjuerna genomfördes på plats hos företagen vilket möjliggjorde en mer öppen intervjudiskussion i och med att vi hade direkt kontakt med respondenterna. Två av dessa intervjuer genomfördes med fler än en respondent. Jacobsen (1993) menar att den intervjuperson som kontaktats kanske inte vill ställa upp ensam utan vill ha stöd från någon annan, vilket kan bero på att det krävs en viss typ av kunskap som respondenten själv inte besitter. Detta var i vårt fall anledningen till att företagen ställde upp med två respektive tre personer vid dessa tillfällen, att kunskapen fanns hos fler än en person.

3.5 Analysmetod

Vår analys har utgått från fem grundläggande steg för hur analysarbete bör gå tillväga. Steg ett var att vi började med att strukturera vår insamlade data genom transkribering. Därefter genomfördes bearbetning av data genom att leta efter samband, återkommande teman och begrepp från transkriberingen. Sedan genomfördes kodning och analys av data, vilket är steg tre. Den analyserade datan presenterades sedan i vårt resultat som till sist möjliggjorde att vi kunde genomföra steg fem, att validera och jämföra data i analys och diskussionskapitlet (Denscombe, 2009).

Inför analysarbetet pekade vår litteraturstudie på att kunskapen är relativt obegränsad för vilka olika säkerhetsrisker det finns för företagsmobilitet. Vi märkte samtidigt att de rådde brist på kunskap för hur företag ska arbeta, för att bli mer medvetna om vilka konsekvenser ett visst användande av mobila lösningar kan få. För att kunna undersöka och analysera detta ansåg vi att en litteraturstudie behövde ligga som grund och därför passade en deduktiv analysmetod, eftersom teorin då hjälper oss att få fram vad som är relevant från empirin för undersökningen. En deduktiv ansats är enligt Elo och Kyngäs (2008) användbar när tidigare teorier ska användas och testas i nya situationer och områden.

Innan vi genomförde transkriberingen läste vi igenom insamlad data flertalet gånger för att skapa oss en god förståelse. Vår teoretiska utgångspunkt har varit bemötande och medvetenhet av och kring säkerhetsrisker. Vi valde att se på resultatet från empirin och dokumentationen och utföra vår analys utifrån dessa begrepp eftersom vi anser att bemötande och medvetenhet har varit det centrala för att besvara vår frågeställning. Under tiden som processen med att transkribera det insamlade materialet noterade vi även uppenbara mönster och tema utifrån vår teoretiska utgångspunkt. Dessa noteringar följde med in i analysen och fungerade som ett extra stöd för oss under vår analys av vår insamlade data. För att identifiera och sortera data använde vi oss av färgpennor och anteckningar där vi arbetade med utskrivna exemplar av vår transkribering. Vi ansåg att detta tillvägagångssätt gav oss en bättre översikt av innehållet för att kunna koda data än på en dator. När det transkriberade materialet hade sammanställts påbörjade vi kodningen och sammankopplade de noterade mönstren mellan de olika intervjuerna. Dessa mönster hade på olika vis samband och samlades under de perspektiv vi redan fått fram från litteraturstudien. Efter att vi hade fått en god överblick kunde arbetet fortsätta och innehållsanalysen påbörjades.

För att kunna undersöka vår frågeställning valde vi sedan att utföra en innehållsanalys av empirin för att kunna ta fram det som var relevant för undersökningen. Det slutliga valet av metod blev en deduktiv innehållsanalys där vi tog fram fyra relevanta perspektiv utifrån litteraturstudien och den insamlade data, vilket är en form av öppen kodning. De fyra perspektiven var utifrån ett policy-, tekniskt-, användar- och utbildningsperspektiv. Med hjälp av dessa perspektiv analyserades empirin genom en kvalitativ innehållsanalys för att resultera i kunskap och förståelse kring området. En kvalitativ innehållsanalys används för att analysera text, verbal och visuell kommunikation och fokuserar på karaktäristiska drag i innehållet för att ta fram relevanta perspektiv (Elo & Kyngäs, 2008; Hsieh & Shannon, 2005).

Perspektiven låg sedan till grund för jämförelse med vår egen tolkning av den empiri och dokumentation som vi hade tagit del av. Syftet har varit att kunna identifiera och förstå respondenternas egna upplevelser, idéer och åsikter kring säkerhetsriskerna vid användningen av mobila lösningar. För att kunna se hur företagen förhöll sig till den

kunskap vi erhållit av tidigare forskning kring säkerhetsaspekter analyserades även deras dokumentation i form av IT-policys. Avsikten med att analysera företagens dokumentation var för att få en bild över vilka strategier företagen har kring hur användningen av mobila lösningar bör gå tillväga, utifrån ett säkerhetsperspektiv. Detta gjorde vi också för att identifiera eventuella mönster och samband mellan tidigare forskning och företagens dokumentation. Denna analys gav oss en förståelse för vad de deltagande företagen fokuserade på, samt själva anser vara viktiga gällande säkerhetsaspekten. För att sedan se om företagen och personalen följde sina egna säkerhetsstrategier jämfördes även deras policys med empirin.

3.6 Metoddiskussion

Till vår undersökning valde vi att genomföra semistrukturerade intervjuer där vi gav mycket utrymme för intervjupersonen att svara. Risken med semistrukturerade intervjuer är att intervjuerna är öppna och flexibla och att det är lätt att glida ifrån ämnet. Frågorna kan även tolkas på olika sätt av intervjupersonen (Kvale & Brinkmann, 2014). För att försöka förhindra detta förklarade vi alltid vårt syfte innan vi påbörjade intervjun, så att respondenten förstod vad vi valt att fokusera på i vår undersökning. Våra intervjuer kunde i vissa fall glida ifrån ämnet vilket berodde på vilken respondent som intervjuades och dennes personliga intresse och kunskap för vissa frågor. Men i och med att vi hade vår intervjuguide kunde vi enkelt gå tillbaka och fånga in respondenten ifall vi ansåg att intervjun gled ifrån ämnet.

Intervjumaterialet som vi sedan tagit fram inför intervjuerna, alltså vår intervjuguide, såg likadan ut för intervjuer på både strategisk- och operativ nivå. Intervjuguiden som var uppdelad i teman med respektive frågor visade sig i efterhand ha både för- och nackdelar. Det som talade för detta tillvägagångssätt, att ha likadana frågor till de båda rollerna, var att vi hade samma underlag att utgå från vid analysarbetet. Detta underlättade vårt arbete med att se likheter och skillnader i svaren som gavs eftersom vi var intresserade av att se ifall användare arbetar som IT-ansvarig förespråkar när det kommer till ett säkert användande av mobila lösningar. Nackdelarna med intervjuguiden var att den operativa nivån visade sig ha svårt att svara på frågor gällande temat strategier och policys. Det vi hade kunnat göra annorlunda hade varit att ha fler frågor på respektive rolls huvudtema. Till IT-ansvarig hade vi kunnat ha fler frågor gällande strategier och policys och till användare kunnat ha fler frågor gällande hantering av mobila lösningar.

Vi genomförde som tidigare nämnt två intervjuer med fler än en respondent. Enligt Jacobsen (1993) kan en intervju med flera personer ofta vara svårt att hantera av olika anledningar. En anledning kan vara att det blir obalans mellan respondenternas deltagande och svar. I vårt fall stämmer detta överens då framförallt en person i vardera av dessa gruppintervjuer stod för majoriteten av svaren medan de andra respondenterna gav mer kompletterande svar och samtycken. Även om teorin menar att det finns problem med att genomföra intervjuer med flera respondenter samtidigt anser vi att detta inte var någon nackdel för vår undersökning, snarare tvärtom. Efter

att ha genomfört både telefonintervju och intervjuer på plats hos företagen med både en och flera respondenter anser vi att gruppintervjuerna varit mest givande då respondenterna kompletterade varandra på ett bra sätt.

En kritik till vår arbetsprocess i sin helhet var att vi till en början endast kontaktade fyra företag. Vi fick svar från tre företag omgående att de var intresserade. Misstaget vi gjorde var att vi förlitade oss på dessa tre och inte hade några företag i reserv ifall något av de intresserade skulle falla bort. Detta var princip vad som hände då ett av de tre företagen meddelade att de inte kunde ställa upp på grund av tidsbrist. Detta resulterade i att vi hamnade i en situation där vi saknade ett företag och tiden för att hitta ett nytt var knapp för att lyckas hålla vår tidsram. Vi hade däremot tur och fick kontakt med ett företag snabbt efter att det andra hade fallit bort. Det hela resulterade i att tidsramen för att genomföra intervjuer försenades ett par veckor. Det företag vi fick tag på saknade däremot policys, vilket vi förstod först när vi var på plats hos företaget och skulle genomföra intervjuerna. Orsaken till detta var brist i kommunikationen mellan oss och VD:n. I det e-postmeddelande som skickades ut till företaget med information om vår undersökning, inkluderande vår intervjuguide, förklarade vi att företaget måste ha policys för att vara relevant för undersökningen. Missförståndet kan ha berott på att vi var otydliga och inte frågade en extra gång när vi talades vid inför intervjun. Efter att ha analyserat och erhållit vårt resultat har denna aspekt inte påverkat våra chanser att besvara vår frågeställning. Det har istället bidragit till ett intressant perspektiv som skiljt sig från de andra företagen.

Till sist anser vi att trovärdigheten av vårt resultat kan styrkas både av den tidigare litteratur vi valt att utgå ifrån i litteraturstudien. Litteraturens relevans kan härledas genom att vi använt oss av tre olika databaser samt använt källor som refererats ett flertal gånger. Tillförlitligheten av vår undersökning kan även styrkas av vår transkribering från den empiri vi tagit del av från respondenterna.

3.7 Etiska överväganden

För all samhällsforskning som utförs finns ett antal etiska principer som en forskare är skyldig att förhålla sig till. Dessa etiska principer gäller i samband med datainsamling, analys och publicering av en undersökning (Denscombe, 2009). Vi har i vår undersökning diskuterat med respondenterna huruvida de vill vara anonyma eller inte. Detta är något som all samhällsforskning måste ta hänsyn till, vilket även kallas för individskyddskravet (Vetenskapsrådet, 2002). Individskyddskravet handlar om att respektera deltagares rättigheter, intressen och värna om deras värdighet. Ett av företagen ville att deras policy skulle vara anonym vilket innebar att vi valde att hålla alla företagens policys anonyma i vårt arbete. För att kunna göra jämförelser mellan intervjuerna och dokumentation resulterade anonymiteten av policys också i att vi valde att hålla respondenterna och företagen anonyma. Inför varje intervju förklarade vi det övergripande syftet med studien för respondenten och hur insamlad data skulle komma att användas och presenteras.

Individskyddskravet är utgångspunkten för forskningsetiska överväganden och konkretiseras i fyra allmänna huvudkrav. Dessa är informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet, vilka var och en innehåller ett antal regler som forskare ska följa för att kunna utföra ett korrekt etiskt förhållningssätt (Vetenskapsrådet, 2002). Dessa fyra huvudkrav har legat till grund för hela vår undersökning.

Informationskravet handlar om att forskaren ska informera respondenterna om den aktuella forskningsuppgiftens syfte. Informationen ska omfatta alla de delar i undersökningen som kan tänkas påverka deras vilja att delta. Inför varje intervju informerade vi respondenterna om varför intervjun genomförs, vad den kommer att handla om och hur lång tid den kommer att ta.

Samtyckeskravet handlar om att respondenterna har rätt till att själva bestämma över sin medverkan. Vi informerade om att deltagandet är frivilligt och att om det är någon som motsätter sig att uppgifter om denne används i studien kommer vi inte att göra detta. Alla intervjupersoner hade våra kontaktuppgifter, ifall de hade frågor kring undersökningen. Inför varje intervju frågade vi om respondenterna samtyckte till att intervjun spelades in. Detta gjorde vi för att förenkla vår insamling av korrekt data.

Konfidentialitetskravet handlar om att uppgifter om respondenterna ska förvaras på ett sådant sätt att obehöriga inte kan ta del av dem. Alla uppgifter om respondenterna har i denna undersökning hanterats på ett sådant sätt att ingen annan haft möjlighet att ta del av dem. Vi informerade också intervjupersonerna om att verksamhetens och respondenternas identitet kommer att skyddas genom att de behandlas anonymt i undersökningen. På detta sätt ska det inte gå att förstå vilka företagen och respondenterna är, detta för att obehöriga inte ska kunna ta del av uppgifter som kan vara känsliga.

Nyttjandekravet handlar om att uppgifter insamlade till undersökningen endast får användas för forskningsändamål. Informationen kommer inte lämnas till tredje part eller användas i annat syfte än till vår undersökning för att vi vill respektera och skydda de personer som bidrar till vår studie (Vetenskapsrådet, 2002).

4 Resultat

Nedan presenteras resultatet från vår innehållsanalys av empiriinsamlingen. Under strategier och policys har vi däremot valt att dela upp temat i underrubriker. Citaten som presenteras är hämtade från de transkriberingar som gjordes efter empiriinsamlingen. Företagen och namnen som används är fiktiva för att upprätthålla anonymitet (se *Tabell 1 – Respondenter* s. 13*)*. Stundtals kan kategorier och teman gå in i varandra då en del svar kan appliceras på flera ställen. Vardera kategori innehåller i sin tur både empiri från anställda på operativ (säljare eller tekniker) och strategisk nivå (IT-ansvarig). De skillnader som identifierats mellan strategisk och operativ nivå kommer att presenteras där de är aktuella. Kategorin strategier och policys inkluderar utöver empiri från respondenter även dokumentation i form av företagens IT-policys. Strukturen inom varje kategori följer samma mönster.

4.1 Strategier och policys

Genom att undersöka företagens dokumentation kring policys och IT-standards vill vi först och främst ge en bild av hur företagen tänker kring säkerhet samt vilka riktlinjer de framhäver. Under detta tema tydliggörs även vad företagen tycker att en användare får och inte får göra när det handlar om ett säkert användande av deras mobila lösningar.

4.1.1 IT-policys

Företagens IT-policy handlar om att ge vägledning och stöd för olika IT-beslut inom respektive företag. Policys och tillvägagångssätt som ingår i en IT-policy ska avspegla ett säkert och accepterat användande av de IT-resurser, exempelvis de system och mobila lösningar som företaget förfogar över. Mer specifikt syftar företagens IT-policy åt att: skydda människor och information, ställa regler på förväntat beteende av användare, systemadministratörer, ledning och IT-personal, samt minska de totala IT-riskerna.

I vår undersökning var det ett av företagen, Kando, som inte hade någon uttalad IT-policy. Anledningen till detta var att de inte ansåg sig behöva en policy på grund av deras storlek. Kando har 10-50 anställda och menade att ifall det uppstår IT-relaterade problem hanteras dessa utifrån de resurser som finns tillgängliga och inte utefter styrande policys. De andra två företagen, Voondo och Mire, är något större företag och har båda omfattande IT-policys. I dessa policys beskrivs en högre nivå av rekommendationer för IT-verksamheten och hur den ska bedrivas. Därefter har båda företagen ytterligare IT-policys som mer detaljerat beskriver specifika områden inom IT-verksamheten. Ett av dessa områden handlar om IT-säkerhet och hur företaget bör bedrivas ut ett säkerhetsperspektiv.

Mire har ett dokument som de kallar för ”IT Security Policy”. Denna policy syftar till att säkerställa konfidentialitet, integritet och tillgänglighet av data och resurser med

hjälp av effektiva och etablerade IT-säkerhetsprocesser och rutiner. Det gäller all utrustning som är ansluten, permanent eller ibland till Mire-koncernens nätverk. Alla anställda på Mire förväntas följa denna policy vid alla tillfällen, där alla överträdelser ska rapporteras till IT-chefen. Policyn ska ses som ett levande dokument och uppdateras när ny teknik och tillvägagångssätt fastställs.

Voondo kallar sitt andra dokument för IT-standards. Detta dokument innehåller särskilda riktlinjer och krav för specifika situationer och resurser. Inledningsvis presenteras en klassificeringsmodell som beskriver riskhantering av företagets informationssystem. Modellen behandlar tre perspektiv av information: konfidentialitet, integritet och tillgänglighet. Därefter innehåller dokumentet exempelvis hantering av lösenord, licenser och mobila enheter samt olika säkerhetsstandards.

4.1.2 Mobila policys

En mobil policy fokuserar enbart på hanteringen av mobila lösningar och hur användningen av den mobila enheten ska ske för att motverka säkerhetsrisker. Av de tre företagen som deltagit i undersökningen var det enbart Voondo som har en IT-policy som inkluderar en säkerhetsstandard för mobila lösningar. Mire håller i nuläget på att ta fram en mobil policy specifikt för sina mobila enheter, men har ingen för tillfället. Kando, som vi tidigare nämnt, har i dagsläget ingen framtagen IT-policy och därmed heller ingen policy för mobila enheter.

Voondo förklarar att mobila enheter måste hanteras så att företagens information ska kunna säkerställas vid både lagring och överföring, även om fysisk kontroll av enheten skulle förloras. Företagets information måste krypteras både vid lagring och under överföring via användandet av mobila enheter. Endast företagsägda enheter kan ansluta till företagets nätverk utan att extra lager av säkerhetsinställningar tillämpas. Voondo använder olika verktyg inom Mobile Device Management (MDM) som möjliggör en säker och effektiv process för att hantera de mobila enheterna. Vidare lyfter dokumentet fram mer tekniska aspekter i form av inställningar på respektive enhet:

- Inaktivera platstjänster om de inte används för affärsändamål
- Blockera automatisk anslutning till öppna nätverk
- Användande av lösenord för åtkomst till företagsinformation
- Kontinuerligt byte av lösenord
- Autolås av enheten efter fem minuter i vänteläge
- Om konfidentiell eller hemlig information överförs eller lagras med hjälp av den mobila enheten rekommenderas ett lösenord på minst åtta tecken

4.1.3 Användarcentrerade policys

Vi valde att rubricera detta tema för användarcentrerade policys efter att ett av företagen, Voondo, har tagit fram en policy som är riktad specifikt mot användaren.

Dokumentet kallar de för ”End User Acceptable Use Policy” och innehåller vad användaren får och inte får göra vid nyttjande av informationssystem, Internet och e-post. Policyn gäller för alla anställda och icke anställda med tillgång till Voondos IT-resurser.

Exempel på restriktioner som policyn innehåller:

- Det är förbjudet att koppla upp sig mot företagets nätverk med en enhet som inte uppfyller företagets rekommendationer av konfidentialitet och integritet
- Användare får inte ladda ner eller installera programvara utan godkännande från IT-avdelningen – kan exempelvis leda till virus
- Användare får inte lämna företagsägd enhet obevakad i offentlig miljö
- Användare får inte skicka, förvara eller vidarebefordra material som kan anses pornografisk, sexistisk, diskriminerande eller inskränka på patent, copyrights eller varumärke via e-post. Vid användning av Internet gäller samma sak, användare får inte logga in på, ladda ned eller lagra något av ovanstående material

För att säkerställa att dessa restriktioner följs beskriver även policyn att företaget har rätt att övervaka all hantering av företagsägda enheter. Övervakningen sker för att kunna bedöma ifall en anställd har brutit mot policyn. Exempelvis har Voondo rätt att övervaka vilka hemsidor som anställda besöker.

I jämförelse med Voondo har som tidigare nämnt Mire ett dokument (IT Security Policy) som innehåller restriktioner för hur företaget ska bedriva ett säkert IT-användande. Det intressanta i detta dokument är att Mire har valt att kombinera vilka säkerhetskrav företaget måste uppfylla och vad användaren själv måste tänka på. Dokumentet innehåller tio övergripande punkter som vardera innehåller restriktioner som både företaget och användaren måste uppfylla för att uppnå en acceptabel säkerhetsnivå, exempelvis för hantering av Internet och e-post. Att kombinera vad företaget och användaren bör tänka på, i en och samma policy, kan i detta fall uppfattas otydlig för vad den enskilde användaren bör ta hänsyn till. Till skillnad från Voondos användarpolicy som omfattar två A4-sidor och enbart handlar om vad användaren ska tänka på, omfattar Mires policy 11 A4-sidor och är en kombination av företag- och användarrestriktioner.

4.1.4 Företagens förhållningssätt till strategier och policys

Ett tema som framkom under analysen var företagens förhållningssätt till strategier och policys. Under intervjuerna diskuterades hur policys tas fram och utformas i företagen och hur de sedan säkerställer att användarna följer dessa.

Som vi tidigare nämnt var det enbart Voondo som hade en utarbetad policy som omfattade den mobila hanteringen. Både IT-nivå och operativ nivå bekräftade under intervjuerna att så var fallet.

Thomas, IT-ansvarig: ”*Ja, vi har mobila policys. Vi har både på användarnivå – hur man bör använda en device men också från ett tekniskt perspektiv, till vilka plattformar vi stödjer och hur vi stödjer dem. Så ja, vi har policys för allt.”*

Richard, Tekniker: ”*Ja det har vi, men det var väldigt länge sen man tittade på dem, det var väl typ i samma veva som man blev anställd som man också blev tillsagd att läsa igenom dem. Men jag vet att vi hade en mindre genomgång angående användningen av våra datorer, men jag menar det var ju inte så mycket angående alla säkerhetsrisker som finns idag flera år senare.”*

Richard, i egenskap av tekniker, bekräftar här att Voondo har mobila policys och att han tagit del av både dessa och fått en mindre genomgång kring användningen av sin dator. Det intressanta är däremot att han påpekar att det var länge sedan han läste igenom deras policys, vilket visar på att Voondo lämnar över ansvaret till användaren att själv uppdatera sig när nya policys introduceras eller uppdateras. Att det inte säkerställs från företaget, att användare ska ha läst igenom policys, är något som Thomas bekräftar.

Thomas, IT-ansvarig: ”*Man kan aldrig tvinga folk att läsa igenom dem, även fastän de är enkla att läsa och förstå.”*

Däremot säger Thomas att företaget borde säkerställa att användare läser igenom uppdaterade policys, vilket han själv säger att han borde bli bättre på. Till skillnad från Voondo arbetar Mire med att säkerställa att deras policys efterföljs, att anställda läser och följer riktlinjerna i den skrivna policyn.

Mattias, IT-chef: *”Varje anställd ska skriva på ett avtal där det står att man är skyldig att följa företagets policys och att de har läst och förstått innehållet i dessa. Sen är det ju upp till användaren att de ser till att policyn följs.”*

Detta visar att både Voondo och Mire har samma syn kring vem som har huvudansvaret för att deras policys efterföljs. De säger båda att ansvaret till största del ligger hos användaren även om företaget skulle arbeta med att säkerställa och kommunicera innehållet i sina policys. Även om arbetet med att säkerställa policys kan vara svårt och att företag lägger stort ansvar på användaren ska det inte avskräcka företag från att ha en utarbetad IT-policys. Mire som i nuläget inte har en specifik mobil policy arbetar för tillfället med att ta fram en sådan. Mattias beskriver att det finns god förbättringspotential gällande säkerheten för mobila lösningar och att en mobil policy kan öka förståelsen kring det mobila användandet.

I kontrast till Voondo och Mire har däremot inte Kando några policys beträffande IT-verksamheten. Peter som är VD och inofficiell IT-ansvarig beskriver att företaget befinner sig någonstans i gränslandet mellan ett företag som har behov av policys och

ett som inte har det. Detta baserar han på företagets storlek och att de idag inte har något behov av policy eftersom de inte tycker sig hantera någon affärskritisk data.

> Peter, VD: ”*Vi jobbar mot offentlig sektor med offentliga upphandlingar. Alla vet vad alla tar betalt hela tiden. Jag kan få tag på min danska konkurrent och hans prislista när jag vill. Så därför är det redan så transparent att det känns som det där med affärshemligheter nästan inte finns längre.”*

Utifrån respondenternas uttalanden verkar både bransch och storlek ha en betydelse för om ett företag har behov av policys eller inte. En orsak till att inte ha policy kan enligt resultatet också vara att ett företag inte uppfattar sig ha någon känslig data.

4.1.5 Sammanfattning

Resultaten som har presenterats under detta tema, strategier och policys, har behandlat företagens IT-policys samt respondenternas tankar och åsikter kring dessa dokument. Företagens IT-policy handlar om att ge vägledning och stöd för olika IT-beslut inom respektive företag. Resultatet visade att två av tre företag har policys, varav ett företag har en separat policy för användaren. Av de tre företagen var det endast Voondo som har en policy som inkluderar hanteringen av mobila lösningar. Beroende på bransch och storlek pekar resultatet på att företag har olika behov av policys. Detta handlar i sin tur om vilken affärskritisk data ett visst företag bedömer sig ha. Men för Voondo och Mire som båda har policys framhävs också betydelsen av att anställda läser och följer policyn. Om inte företaget lyckas förmedla informationen i policyn är risken att företaget förlorar en del av syftet med den. Både Voondo och Mire framhäver till sist vilket ansvar användaren har i att en policy efterföljs, att ansvaret inte enbart vilar på företaget. Intresset för att ta till sig innehållet i policys måste finnas hos den enskilda individen. Samtidigt har företagen en betydande roll i att se till så att detta intresse motiveras genom att utforma policys utifrån ett användarperspektiv.

4.2 Hanteringen av mobila lösningar

För att kunna få en förståelse för medvetenheten kring säkerhetsrisker och hot hos företagets anställda krävs en förståelse för hur arbetet med de mobila lösningarna ser ut i verkligheten. Detta tema gav respondenterna möjlighet att uttrycka vilka användningsområden som finns men också vilken betydelse de mobila lösningarna har för deras arbete. De uttryckte sig också kring autentisering och vilka åtgärder som företaget valt att ha för åtkomst till den mobila lösningen. Till sist presenteras resultatet kring hur hanteringen av deras lösningar säkerställs.

4.2.1 Betydelsen av mobila lösningar

I de tre företag som intervjuats används framförallt smartphones som den primära mobila lösningen. Ett av företagen använder för sina tekniker också en PDA-lösning

(Personal Digital Assistent) för det dagliga arbetet ute hos kund, vilket är en portabel handdator. De tre företagen har med olika typer av erfarenheter visat på vilken betydelse den specifika mobila lösningen har för dem.

> Mattias, IT-chef: *”Jag sitter ju extremt mycket i externa möten, då blir ju mobilen min förlängda arm, speciellt om jag inte använder mig av min laptop.”*

> Richard, Tekniker: ”*Jag är ute hos kunder hela dagarna och sitter därför aldrig på kontoret eller väldigt sällan i alla fall. Så man kan ju verkligen säga att allt mitt arbete sker mobilt. När jag använder mig av min laptop så använder jag alltid min iPhone som ett externt wi-fi för att få Internetuppkoppling.”*

> Gustav, Tekniker: ”*Jag skriver mina arbetsorder via mobilen. Varje dag blir vi ju tilldelade olika jobb och kan då vi via den mobila lösningen skriva direkt i ordern exempelvis vad vi har gjort, vilka delar vi har använt och hur mycket tid vi har gjort ute hos kunden. Och allt detta gör vi via vår mobil som är en iPhone 6.”*

Användningsområden för den mobila lösningen visar ovan att de varierar hos de olika företagen. De områden som beskrevs var, utöver att kommunicera, följande: hämta, skriva och skicka order, e-posthantering, rapporthantering, kundhantering via CRM-system, använda mobiltelefonen som ett externt wi-fi (hotspot). Oavsett användningsområde framställer alla respondenter en mobil lösning som ett nödvändigt verktyg för att klara av och hantera en arbetsdag. En mobil lösning har ofta som syfte, förutom att öka tillgängligheten, att effektivisera arbetsprocesser vilket är något som Gustav påpekar.

> Gustav, Tekniker: *”Ja, den har ju tagit bort mycket av efterarbetet som måste göras efter att ordern har blivit påskriven. Med den nya mobila lösningen så finns ordern redan i systemet, innan så var man tvungen att renskriva den i systemet när den väl blivit inlämnad av oss servicetekniker i pappersformat.”*

4.2.2 Autentisering för åtkomst

För att uppnå en säker användning av en mobil enhet är en säker autentisering en avgörande faktor för att säkerställa användningen. Respondenterna fick i undersökningen förklara hur autentiseringen av deras mobila lösning såg ut.

> Niklas, Säljare: *”VPN-tjänsten som vi använder har ju en call-back funktion, alltså en tvåstegs-inloggning, där jag får ett sms med en kod som jag sedan matar in. Så först matar jag in mitt användarnamn och lösenord och då får jag ett sms tillbaka med en kod, och sen så anger jag den koden och är inne i systemet. Samma som banken.”*

> Nils, IS-ansvarig: *”En av våra mobila lösningar är den som går igång i Europa och som kräver ett lösenord så fort den varit inaktiv under en viss tid.”*

Respondenterna ovan bekräftar att autentiseringen är en viktig säkerhetsåtgärd som både Voondo och Mire valt att fokusera på i sina lösningar. Kando använder sig av en webblösning där tekniker måste logga in med användarnamn och lösenord varje gång de ska få åtkomst till systemet. Medan Nils på Voondo påpekar en lösning som är säker vad gäller autentisering, förklarar samtidigt Thomas en annan av företagets mobila lösningar.

> Thomas, IT-ansvarig: *"En tekniker har endast en inloggning till devicen men inte något till systemen. Med andra ord behöver de inte logga in i system när de väl slagit in lösenordet på telefonen, vilket hade kunnat vart en grej för att lägga på extra säkerhet."*

Det intressanta med detta är att Voondo har olika krav på autentisering för olika mobila lösningar. Den lösning som Nils pratar om är en ny lösning som ska köras igång inom en snar framtid, där de då har valt att fokusera mer på säkerheten vad gäller åtkomst av data. Richard som är tekniker på Voondo säger i sin tur att företaget vill att en tekniker ska logga in och ut från systemet, men i verkligheten är en tekniker i princip alltid inloggad för att få snabb åtkomst till systemet eftersom autentisering anses besvärligt och tidskrävande. Detta bekräftar Jörgen.

> Jörgen, IS-ansvarig: *"Våra tekniker hatar lösenord. Däremot blir det bättre på mobiltelefonerna som har stöd för fingeravtryck vilket fungerar med den lösningen som vi använder. Och det kommer vi att köra med framöver."*

Eftersom tekniker och säljare ofta behöver ha snabb åtkomst till information samtidigt som företaget kräver en säker autentisering skapar detta ett problem. En lösning kan vara det Jörgen beskriver ovan, att ett smidigare alternativ med fingeravtryck används istället för lösenord.

4.2.3 Metoder för att säkerställa hanteringen av mobila lösningar

För att skapa en säker autentisering och hantering använder sig både Voondo och Mire av MDM-system. Enligt Thomas på Voondo måste användare få stöd i hanteringen av enheter, det får inte enbart vara policys som säger vad som får och inte får göras, det har man provat i alla år och det fungerar inte. Han säger att det krävs ett interaktivt stöd, vilket ett MDM-system kan användas som. Voondo använder sig av ett MDM-system som heter Airwatch medan Mire använder en light-version av MDM-systemet MobileIron. Vidare berättar Thomas att både MobileIron och Airwatch är två topplattformar i branschen. Han förklarar att det är få skillnader dem emellan och att båda är ett bra val.

> Thomas, IT-ansvarig: *"Airwatch är ett manageringssystem. Det man gör är att man installerar en agent på en device som tar över säkerhetsfunktioner i devicen. Detta gör att du kan styra den på i princip vilken parameter du vill: inloggning, kryptering, segmentering, vad du får göra/inte göra, stänga av/på enheten,*

kamera, batteritid, kolla jailbreak, spåra och wipa (rensa). Allt du kan tänka dig av ett MDM-system."

Mattias, IT-chef: *"Idag har vi en enklare variant av MobileIron som ställer krav på bland annat pinkod och efter fem misslyckade försök att logga in så wipas telefonen och koden blir krypterad. Vi har alltså inte applicerat MobileIron fullt ut och har därför inte haft stor kontroll utan det har bara varit kring kraven på lösenorden."*

Det respondenterna antyder är att oavsett om företaget valt att använda sig av MDM-systemets funktionalitet fullt ut eller inte, skapas fördelar i form av säkerhetsåtgärder. Däremot säger Mattias att desto mer funktionalitet av ett MDM-system du väljer att använda desto större kontroll får du. Han förklarar sedan att Mire just nu håller på att ta fram mobila policys för att få större kontroll på sina enheter. I arbetet med att ta fram dessa har de använt sig av MobileIron som ett ramverk i form av vilka delar som policyn ska omfatta. Ett MDM-system kan med andra ord fungera som ett stöd för både den fysiska hanteringen av den mobila enheten, men också för utformningen av en mobil policy.

Mattias, IT-chef: *"Tanken med det nya MDM-systemet är vi ska kunna styra hanteringen av de mobila enheterna med lite fastare hand i och med att det kommer att finnas en separat företagsdel i mobilen. Detta betyder att så fort man ska göra någonting arbetsrelaterat så går man in i företagsläget i mobilen. Så man kan säga att det kommer finnas två olika miljöer i mobilen, en för arbete och en för privat. Fördelen och moroten för detta arbetssätt är att användarna får en bättre tillgång till våra interna system via mobilen."*

Även om ett MDM-system kan hjälpa ett företag att hantera de mobila enheterna så förklarar Mattias på Mire att det i slutändan inte är enheten i sig som innebär den största risken. Han berättar att det istället är användaren som utgör den största risken och detta kan enbart åtgärdas genom att användaren får säkerhetsutbildning för att öka medvetenheten kring den mobila lösningen och säkerhetsriskerna.

Mattias, IT-chef: *"Det väsentliga är ju att se till så att alla vet hur arbetet och hanteringen av den mobila lösningen ska gå till för att användningen ska ske säkert."*

Thomas fortsätter på samma spår men tolkar det på ett annat sätt och förklarar att det handlar om att lära användaren vilken data som är viktig att skydda och att den utbildningen inte genomförs idag. Som det ser ut idag, förklarar Thomas, att det inte går att lägga ansvaret hos användaren att veta vilken data som är affärskritisk och att den utbildningen skulle behöva göras.

4.2.4 Sammanfattning

Resultaten som har presenterats under detta tema, hanteringen av mobila lösningar, tyder på att mobila enheter har stor betydelse för det dagliga arbetet oberoende av vilken roll respondenterna haft i denna undersökning. En mobil enhet kan enligt respondenterna effektivisera arbetet och öka tillgängligheten hos en användare. Två av tre företag använder sedan ett MDM-system för att säkerställa hanteringen av sina mobila lösningar. Att enbart fokusera på ett MDM-system garanterar inte att säkerhetsrisker motverkas eftersom att användare själva inte har förståelse för vilka säkerhetsrisker och hot som finns. Respondenterna beskriver att utbildning krävs för att de ska nå den kunskap och förståelse som företagen vill åt.

4.3 Säkerhetsrisker och hot

Under tredje och sista temat presenterar vi här resultatet kring de säkerhetsrisker och hot som företagen upplever med sina mobila lösningar, samt hur de betraktar sig vara påverkade av dessa risker. Frågorna som ställdes under detta tema kretsade också kring användandet av privata- och företagsägda enheter där Bring Your Own Device-fenomenet diskuterades. Till sist gav respondenterna sin egen syn på vilket hot användaren själv utgör och samtidigt vilket ansvar användaren har för en säker hantering av den mobila lösningen.

4.3.1 Upplevda säkerhetsrisker och hot

Under intervjuerna framkom det till en början att inget av de tre företagen ansåg sig uppleva några större risker och hot med sina mobila lösningar. Inget av företagen hade råkat ut för säkerhetsrisker som resulterat i betydande konsekvenser.

> Thomas, IT-ansvarig: ”*De incidenter som är säkerhetsrelaterade och kända, det kan ju hända att det finns sådana som vi inte vet om naturligtvis, men de som är kända är ju vanligast mail, någon form av virus men då är det ju alltid på desktop sidan.”*

> Mattias, IT-chef: ”*Det finns två typer av företag, de som blivit hackade och de som blivit hackade men inte vet om det. Så det är ju klart att någonting har vi säkert fått och blivit påverkade av, för det finns så ohyggligt mycket skit därute, men vi har ju inte råkat ut för någon större incident där vi har identifierat någon farlig kod. Däremot vi har ju sett att vi har fått en del infekterade enheter och då har vi satt dem i karantän.”*

Vidare förklarar Mattias att det är e-posten som oftast är en bidragande orsak till att enheter blivit infekterade och fått virus, något som Niklas instämmer om men som han också tror kan innebära fler risker.

> Niklas, Säljare: *”Rent generellt är det väl e-posten som innebär den största risken av det man hört med packet-sniffing och allt annat, speciellt eftersom det är det*

verktyget som vi använder dagligen. Vi skickar både priser, offerter, kontaktinfo, strategidokument med mera. Så det är väl ett jättehål då om det nu verkligen är så att konkurrenter eller andra kan ta del av den informationen."

Av ovanstående citat visar det sig att e-posten verkar utgöra det största hotet på företagets enheter. Mattias fortsätter sitt resonemang och berättar att hans största oro är att någon råkar öppna upp ett e-postmeddelande innehållande en trojan eller phishing-attack (även kallat nätfiske eller lösenordsfiske) när en användare sitter "in-house" och är uppkopplad till det egna nätverket. Han förklarar också att de hot som kan resultera i skadlig data gäller på de system och verktyg som är mest exponerade och öppna för hot, till exempel CRM-system och e-post.

4.3.2 Privat- eller företagsägda enheter

Ett annat hot som Mattias lyfter fram är om någon ansluter sig till företagets nätverk via sin privata mobila enhet, som inte är företagsägd och på så vis inte är säkrad. Detta leder oss in på BYOD, där företagen hade tydlig uppfattning om vilka enheter som får användas i arbetet.

Peter, VD: "*Jag vill ju inte att man ska plocka med sin egen privata telefon och få upplagt sin jobbmail och sin mobila växel på den. Där säger jag stopp. Jag vill kunna ta den ur handen och säga att nu tar jag hand om den för den är min. Det är företaget som äger telefonerna och den data som är på den."*

Thomas, IT-ansvarig: *"Grundprincipen är att om du ska ha företagets data på enheten så ska det antingen vara en företagsägd produkt eller att vi gör bedömningen att våra tekniska lösningar kan skydda produkten på samma sätt så att det inte spelar någon roll."*

Mattias, IT-chef: *"Vi köper in mobilerna till våra anställda, så det är inte deras egna, men de senaste 5-6 åren så har fler och fler gått till att bara använda företagsmobilerna i både privata- och företagssyften. Enheterna har glidit över till att bli en multiplattform."*

Citaten ovan visar att företagen verkar vara eniga om att enheter som används i företagssyfte måste vara företagsägda för att kunna säkerställa den information som behandlas. Däremot har inte företagen någon regel som motsätter privat användande av den företagsägda enheten. Detta är istället något som verkar vanligt då flera av respondenterna använder sin företagsägda enhet även till privat ändamål. Anledningen till detta är att de vill slippa gå runt med två enheter, men framförallt för att kunna vara tillgängliga även efter arbetstid. I Voondo och Mires fall är enheterna styrda av MDM-system för att säkerställa användningen, men att säkerställa enheterna till hundra procent verkar omöjligt.

4.3.3 Användaren som ett hot

Även om ett MDM-system används och säkerställer enheten finns det fortfarande en risk i form av användaren. Den mänskliga faktorn är något som alla tre företag har poängterat vara den mest bidragande orsaken till att säkerhetsrisker kan uppstå vid användning av en mobil lösning.

> Thomas, IT-ansvarig: *”När jag tänker efter så hade vi ett virus i Tyskland alldeles nyss där de hade en sådan ransomware som krypterade alla filer. Och det viruset kom via ett mail där en användare öppnade mailet, förmodligen i god tro.”*

> Gustav, Tekniker: ”*Jag tror att Peter (VD:n) är väldigt duktig och har bra koll på säkerhetsrisker, vilket gör att man lägger ifrån sig ansvaret för detta på honom och litar på att han ska lösa olika problem ifall de skulle uppstå. Jag tror att det krävs att något inträffar mig, annars kommer inte jag gå runt och tänka på detta.”*

I Voondos fall berättar Thomas att användaren var anledningen till att ett virus drabbade företagets enheter. Han säger också att det förmodligen var i god tro som användaren öppnade e-postmeddelandet men antyder att detta hade kunnat hindras om användaren hade haft större medvetenhet och förståelse för de risker och hot som finns via e-post. Detta är något som även Gustav antyder i citatet ovan. Han pekar på att användare lägger ifrån sig ansvaret på de som ansvarar för lösningen i företaget och att det krävs att något inträffar för att användare ska bli mer medvetna kring riskerna. Mattias på Mire berättar även att det kan vara svårt att nå ut till användarna och förmedla all information som krävs för att hantera säkerhetsrisker. Däremot har alla anställda på Mire fått gå igenom en säkerhetsutbildning för att öka användarnas medvetenhet för hanteringen av IT-resurser. Enligt Mattias handlar det i det stora hela om att se till så att alla vet hur hanteringen ska gå till. Thomas på Voondo instämmer om att utbildning för användare är en viktig del av säkerhetsarbetet, men han tror också att det finns andra saker som Voondo hellre lägger sina resurser på när det kommer till utbildning. Istället förklarar Thomas hur arbetet med att öka användarens medvetenhet för säkerhetsrisker skulle kunna se ut.

> Thomas, IT-ansvarig: *”Man skulle kunna göra en ”annons-kampanj” en gång om året, där man gick ut till anställda via e-post eller intranät och säga: Tänk på att…! Att man inkluderar ett tydligt exempel på något som har hänt hos ett företag på grund av att någon, exempelvis, glömt att stänga av sin dator. Alltså för att göra folk påminda, att man får en aha-upplevelse, det hade varit bra att göra lite oftare. En väldigt enkel grej egentligen, någon måste bara göra det.”*

> Mattias, IT-chef: *”Det kan vara nödvändigt att man samlar dem som är mindre IT-intresserade och går igenom säkerhetsbiten bara med dem eftersom alla inte har lika stor möjlighet att tänka säkerhet. Det är samtidigt viktigt att se till så att anställda inte hittar på sina egna varianter på säkerhetsfunktioner.”*

Respondenterna beskriver att användare behöver hjälp på vägen för att nå medvetenhet kring säkert användande. Mattias tror att användare överlag är väldigt svåra att hantera eftersom det alltid finns användare som letar genvägar när de inte samtycker med företagets tillvägagångssätt. Därför är det viktigt att ha utbildningar för att se till att användare med lägre medvetenhet kring säkerhet får en förståelse för vilka konsekvenser deras handlande kan medföra. Samtidigt tror inte Mattias att användare kan bli fullt medvetna även om utbildningar genomförs. Han upplever att det är latheten och smidigheten som är de största hoten mot att användare inte blir medvetna om alla säkerhetsrisker som finns. En användare strävar efter att hanteringen ska vara så enkel som möjlig och är därför inte intresserad av att ha komplexa anpassningar på sin enhet bara för att hanteringen ska bli säkrare. Detta är något som fler respondenter bekräftar när de säger att säkerheten inte får överspela användarvänligheten.

> Sven, Business-ansvarig: *”Det gäller att hitta den här kompromissen mellan bra säkerhet och användarvänlighet.”*

> Niklas, Säljare*: ”Mire skulle säkert vara villiga att investera i verktyg för att kryptera till exempel e-post om det finns verktyg som gör att hanteringen blir smidig, vi lever ju trots allt i en omvärld där vi måste kunna kommunicera på ett enkelt sätt.”*

Vidare förklarar Thomas på Voondo att användaren måste få hjälp per automatik av olika system för att säkra upp användandet.

> Thomas, IT-ansvarig: *”Jag tror att det handlar om sunt förnuft, vad skulle man själv vilja ha för stöd? När man till exempel sitter där i sin bankapplikation och ska logga in och det kommer upp ett popup-meddelande med information: tänk på att…! Det är bra information.”*

4.3.4 Användarens eget ansvar

Att företag tar sitt ansvar och säkrar upp enheter med hjälp av olika stöd som policys och MDM-system, är en del i arbetet med att säkra upp användandet. Men detta måste balanseras med användarens eget ansvar att vara medveten kring säkerhetsriskerna.

> Mattias, IT-chef: *”Det är upp till de anställda att själva ta ansvar och ha koll på att till exempel kontrollpunkterna i våra policys efterföljs. Det kan till exempel vara att antivirusprogrammet ska vara uppdaterat. I det stora hela är det upp till användarna att tänka säkert eftersom det idag finns så många olika plattformar att hämta information från.”*

> Niklas, Säljare: *”Jag har haft ett naturligt intresse för tekniken och hur det ska användas. Det handlar om eget lärande, snarare än att någon annan ger dig*

information. Det här är ju ändå vårt viktigaste eller andra viktigaste verktyg i det dagliga arbetet, smartphonen. Och kan man inte den så kan man inte sitt jobb."

Användare har enligt respondenterna ett stort ansvar i att själva vara medvetna om de säkerhetsrisker och hot som finns men också hantera sin enhet med ett sunt förnuft. Detta är något som i många fall kan vara ett problem då Mattias beskriver att vi fortfarande befinner oss i ett förlegat tänkande kring mobila lösningar och säkerhet, där det fortfarande finns användare som inte förstår allvaret och därför måste bli upplysta.

Mattias, IT-chef: *"Vi har faktiskt tänkt hålla en workshop där vi ska visa hur en attack kan se ut. Man väljer ut en person i publiken för att visa hur lätt det är att ta sig in i en mobil för att bland annat se lösenord. Det handlar ju om att användarna inte har en aning om vilka risker som finns förrän de själva har råkat ut för det. En attack på arbetet kan innebära att även privat information läcker ut, till exempel lösenord till banken, vilket gör att man känner sig attackerad personligen. Detta kan i sin tur öka medvetenheten och underlätta själva förståelsen för vad riskerna kan innebära."*

Thomas på Voondo fortsätter och ger ett annat exempel på hur användare kan förstå allvaret med säkerhetsrisker. Han förklarar hur de nya låssystemen till hemmet fungerar. Systemen bygger på ett kodlås istället för en nyckel vilket möjliggör att du kan ge ut en engångskod till sotaren och fastän du inte är hemma kan sotaren komma in. Men hur får sotaren koden? Om du skickar den via e-post eller sms på telefonen, kan du vara säker på att koden inte har fångats upp av en tredje part som i sin tur gör inbrott i ditt hem? Att ge konkreta exempel som en användare enklare kan ta till sig och sedan förklara hur detta kan se ut på arbetsplatsen, kan vara ett bra tillvägagångssätt för att öka medvetenheten kring riskerna. Det här betyder samtidigt att användaren själv måste ta sitt ansvar och förstå vilka risker som mobila enheter kan utsättas för. Samtidigt behöver användarna stöd av företaget för att uppnå den medvetenhet som krävs. Användarna måste få konkreta exempel på sådana saker som gör att de kan dra paralleller till sitt privatliv och saker som händer i vardagen.

4.3.5 Sammanfattning

Resultaten som har presenterats under detta tema, säkerhetsrisker och hot, har kretsat kring användandet av privata- och företagsägda enheter. Respondenterna har också gett sin syn på hur de själva upplever att säkerhetsrisker och hot för mobila lösningar kan motverkas. Resultatet har visat att både användarna har lika stort ansvar som företaget i att motverka riskerna. Slutligen har respondenterna, framförallt på strategisk nivå, ansett att de säkerhetsrisker som uppstår oftast beror på bristande medvetenhet och förståelse hos användaren. För att öka medvetenhet och förståelse pekar flera av respondenterna på att det krävs konkreta exempel på vilka konsekvenserna kan bli av ett visst handlingssätt.

5 Analys

Vårt problemområde kretsar kring företag och de anställdas brist på kunskap och medvetenhet gällande säkerhetsrisker för mobila lösningar. Frågeställningen har därför fokuserat på hur företag kan bemöta dessa säkerhetsrisker. I vår analys har sedan den teoretiska utgångspunkten varit att fokusera på olika bemötanden eftersom det har varit centralt i hela vår undersökning. Analysen av vårt resultat är därför uppbyggd utifrån olika perspektiv på hur säkerhetsrisker kan bemötas för att öka medvetenheten och kunskapen. Vi har valt att rubricera dem enligt följande: bemöta säkerhetsrisker - ur ett policy-, tekniskt, utbildnings-, och användarperspektiv.

5.1 Bemöta säkerhetsrisker - ur ett policyperspektiv

Av de tre företag som intervjuats använder sig två av omfattande policys. Det tredje företaget beskrev att de inte behöver någon policy på grund av företagets storlek och att de bedömer att de inte har någon affärskritisk data. Enligt Sybase (2011) inför många företag mobila lösningar utan att implementera heltäckande IT-policys på grund av att det anses dyrt och komplicerat. Pearlson och Saunders (2013) menar även att företag utan IT-strategier och policys som ställer krav på användandet av mobila enheter riskerar att förbise olika säkerhetsrisker och hot. Oavsett om ett företag är mindre till storlek eller själva inte bedömer att de har någon affärskritisk data, kan det vara bra att implementera någon form av policy ifall det skulle inträffa något säkerhetsrelaterat problem. Genom att ha en policy kan företag få vägledning och stöd som kan skydda människor och information. En policy bör hantera frågan hur företag ska förhålla sig till BYOD-fenomenet. Enligt Caldwell et al. (2012) måste företag se fördelen och nyttan med BYOD eftersom det leder till ökad produktivitet och tillfredsställelse hos anställda. Resultatet pekar däremot mot motsatsen. Företagen i denna studie verkar eniga om att mobila enheter måste vara företagsägda för att kunna säkerställa informationen som behandlas. Däremot hade företagen ingen regel som motsätter privat användande av den företagsägda enheten. Enligt resultatet framställer användarna att deras dagliga användning, både för arbete och privat bruk, inte hämmas av att enheten är företagsägd och säkerställd.

För att garantera att den nya tekniken fungerar på ett säkert sätt behöver företag utforma nya säkerhetsstrategier och policys för användandet av mobila enheter i verksamheten, oavsett om de är företagsägda eller privata (Harris & Patten, 2014). Endast Voondo har en policy som fokuserar på hanteringen av de mobila lösningarna i företaget. Däremot håller Mire på att ta fram en mobil policy, eftersom de bedömer att en sådan är nödvändig för att öka förståelsen kring det mobila användandet. Enligt Pearlson och Saunders (2013) bör företag utveckla underliggande och mer detaljerade policys för hur hanteringen av specifika områden ska gå tillväga, till exempel för Internet-användning och autentisering. Detta är något som både Voondo och Mires policy redan innehåller. I Voondos fall har de även utformat en policy som enbart riktar sig till användaren (End User Acceptable Use Policy). Denna policy omfattar

två A4 sidor och är enkel för användaren att läsa och förstå då den tydligt beskriver vad användaren får och inte får göra vid användning av företagets IT-resurser.

Resultatet av empirin visade att företagen har policys men att de inte arbetar aktivt med att säkerställa att de efterföljs. Företagen uppmanar anställda till att läsa igenom policys men berättar att de aldrig tvingar anställda att läsa dem. Anställda kan läsa igenom policyn men det betyder inte att de har förstått innehållet. Pearlson och Saunders (2013) menar på att för att kunna säkerställa att säkerhetspolicys följs behöver användarna vara väl införstådda med de riktlinjer som finns. Idag sker heller ingen återkoppling av uppdaterade policys. Mattias på Mire säger att de idag skickar ut uppdaterade versioner till alla anställda men därifrån sker ingen kontroll på att dessa har blivit accepterade och införstådda. För att policyn ska accepteras menar Pearlson och Saunders (2013) att det är viktigt att användare är med och tar fram policyn tillsammans med IT-ansvariga. Användare måste vara tydliga med vad de vill att säkerhetspolicyn ska innehålla och hur den ska stödja dem i sitt vardagliga arbete, medan IT-avdelningen har kunskapen om vilka möjligheter och begränsningar som finns för respektive säkerhetsrisk.

Ur ett policyperspektiv kan säkerhetsrisker och hot bemötas genom att företaget använder policys som är användarcentrerade. Genom att utforma policys tillsammans med användare som får ge feedback på innehållet, samtidigt som företagets egna restriktioner inte inkluderas, kan en användarcentrerad policy erhållas. Om inte företaget lyckas förmedla informationen i sin policy är risken att företaget förlorar en del av dess syfte. Därför har företag en betydande roll i att se till så att intresset för att ta till sig innehållet i policyn motiveras genom att utgå från ett användarperspektiv i framtagandet av en mobil policy.

5.2 Bemöta säkerhetsrisker - ur ett tekniskt perspektiv

För att säkerställa hanteringen av mobila enheter använder två av tre företag i undersökningen sig av MDM-system. Enligt Thomas på Voondo måste användare få stöd i hanteringen av enheter, det får inte enbart vara policys som säger vad som får och inte får göras. Istället förklarar han att det krävs ett interaktivt stöd, vilket ett MDM-system kan användas som. Ett MDM-system har som övergripande syfte att hantera och lösa säkerhetsproblem vid användandet av mobila enheter, samt trådlöst övervaka och kontrollera status och funktioner hos en mobil enhet (Souppaya & Scarfone, 2013). Enligt resultatet kan systemet ta över säkerhetsfunktioner på en enhet. Företag får då möjlighet att styra enheten på i princip vilken parameter de vill: inloggning, kryptering, segmentering, vad en användare får göra/inte göra, stänga av/på enheten, kamera, batteritid, se över jailbreaking, spåra och rensa. Ett exempel på säkerhetsåtgärd i ett MDM-system är att du kan rensa enheten trådlöst om en användare tappar bort enheten eller slår in fel lösenord ett visst antal gånger och därmed låser enheten. Souppaya och Scarfone (2013) menar att systemet ska stödja rensning av mobila enheter på distans om den blir borttappad eller stulen, vilket ingår

i en av riktlinjerna (datakommunikation och lagring) för att kunna säkerställa att användningen av ett MDM-system ger önskad nytta.

En annan riktlinje är användare och enhetsautentisering. Den handlar framförallt om krav på verifiering, innan åtkomst till företagets databas och information (Souppaya & Scarfone, 2013). Respondenterna bekräftade i resultatet att autentiseringen är en viktig säkerhetsåtgärd och en åtgärd som alla tre företag har valt att fokusera på i sina lösningar. Företagen har däremot olika krav på lösenord. Det mest förekommande var en enkel pinkod för att logga in på enheten. För att komma åt mer känslig information, till exempel till företagens egna system, krävs en tvåstegsinloggning hos ett av företagen. Voondo har dessutom olika krav på lösenord för olika lösningar. En tekniker i Sverige har endast en inloggning till enheten, men inget till systemet. De globala lösningarna som körs i flera länder har däremot ett större fokus på autentisering där lösningen kräver ett lösenord så fort den varit inaktiv under en viss tid. Tekniker och säljare vill ha snabb åtkomst till sina enheter och system vilket är ett hinder för komplexa och tidskrävande krav på lösenord. Resultatet visar att säkerheten inte får överspela användarvänligheten, därför krävs det enkla och effektiva säkerhetslösningar som användaren accepterar. Ett alternativ som respondenterna lyfter fram kan vara att använda sig av fingeravtryck istället för lösenord, eller en kombination av de båda. Att använda sig av fingeravtryck som autentiseringsmetod är enligt Gao et al. (2014) en metod som ökar både säkerheten och användarvänligheten på mobila enheter.

Som tidigare nämnts används ett MDM-system för att övervaka, kontrollera men också stödja en användare vid hantering av en enhet (Rhee et al., 2012). En funktionalitet som Voondo framställer som potentiellt användbar för att guida och öka medvetenheten för säkerhetsrisker hos en användare är pop-up meddelanden. Tanken med pop-up meddelanden går att likna med hur vissa bankapplikationer fungerar. När en användare till exempel ska överföra pengar på sin bank kommer det upp ett pop-up meddelande med information, exempelvis: ”Tänk på att kontrollera att du har skrivit in rätt kontonummer!”. En säkerhetsåtgärd av denna sort, om den används vid hantering av andra system, skulle kunna uppmärksamma användaren för de moment i hanteringen av en enhet som är mer riskfyllda. I e-posten, som i resultatet anses vara det mest utsatta verktyget för företagen, hade denna funktionalitet exempelvis kunnat varna användaren från att öppna oidentifierade e-postmeddelanden som kan innehålla ett potentiellt virus.

Säkerhetsrisker och hot kan ur ett tekniskt perspektiv bemötas med hjälp av ett MDM-system. Förutom att använda systemet till att säkra upp och styra enheter kan företag stödja användaren i hanteringen och öka medvetenheten för de risker som finns. MDM-system bör användas för att möjliggöra en säker men också smidig autentisering, till exempel genom fingeravtryck. Det skulle även kunna användas för att öka förståelsen för olika risker genom att använda interaktiv funktionalitet likt pop-up meddelanden.

5.3 Bemöta säkerhetsrisker - ur ett utbildningsperspektiv

Även om ett MDM-system används och säkerställer enheten framhäver respondenterna att det fortfarande finns en risk. Enligt de tre företagen anses användaren vara den mest bidragande orsaken till att säkerhetsrisker kan uppstå vid användning av en mobil lösning. Att säkerhetsrisker förbises kan enligt Harris och Patten (2014) relateras till bristande medvetenhet och förståelse för riskerna. I resultatet beskriver respondenterna att det är svårt att nå ut till användarna och förmedla den information som krävs för att hantera säkerhetsrisker. Att företaget genomför säkerhetsutbildningar med användarna för hur hanteringen ska gå till kan öka medvetenheten och förståelsen för vilka risker som finns. Resultatet visar att utbildning för användare är en väsentlig del av säkerhetsarbetet. Detta styrks av Furnell (2008) som anser att nyckeln till en säker hantering är genom utbildning. Att användare får kunskap och kännedom om företagets säkerhet och hantering är enligt Bulgurcu et. al (2010) grundläggande för att ett företag ska kunna ha en gemensam medvetenhet och förståelse för de risker som finns. Användare har enligt respondenterna olika förutsättningar att uppnå ett säkert användande av mobila enheter. Detta grundar sig ofta i hur intresserade en användare är av tekniken och de lösningar som används. Därför är det viktigt att hålla utbildningar för att se till att användare med lägre medvetenhet och kunskap kring säkerhet får en förståelse för vilka konsekvenser deras handlande kan innebära.

För att integrera säkerhetstänkandet och nå ut till användare bör företag aktivt använda olika kommunikationskanaler som uppmuntrar till relevant medvetenhet kring säkerhet (Furnell, 2008). Utbildning kan se ut på olika vis men det viktiga är att ha konkreta exempel som användaren kan relatera till, för att enklare ta till sig informationen. Användarna har oftast inte en aning om vilka risker som finns förrän de själva har råkat ut för det, därför är det viktigt att kunna ge information där användarna kan dra paralleller med privatlivet. I resultatet kom det fram olika exempel på hur utbildning skulle kunna se ut. Ett förslag var att hålla en workshop för de anställda där företaget visar hur en attack eller ett intrång på en mobil enhet kan se ut. Tanken med en workshop är att tydligt visa vilka konsekvenser en säkerhetsrisk kan tänkas ha och hur enkelt det är att utsättas för den. I samband med denna typ av presentation bör användaren även lära sig hur de kan förebygga en risk men också hur den hanteras när den väl inträffat. Ett annat exempel på utbildning är att genomföra så kallade annons-kampanjer. Dessa kan utgöras av företaget själva, att de skickar ut information via till exempel e-post. Enligt respondenterna kan en sådan kampanj via e-post bestå av information om en relevant händelse som inträffat på ett annat företag. Tanken med en annons-kampanj av detta slag är att ge användare en insikt och förståelse för vad en osäker hantering kan resultera i.

Säkerhetsrisker och hot kan ur ett utbildningsperspektiv bemötas genom att lära användaren hur en säker hantering uppnås och vilken data som är viktig att skydda. Nyckeln till ett säkert användande ligger i att företaget och de specifika användarna

är medvetna om de risker som finns samt är noga med att använda sig av rätt säkerhetsfunktioner (Ben-Asher et al., 2011). Respondenterna förklarar att företag måste arbeta mer aktivt med utbildning och använda sig av flera kommunikationskanaler. Detta för att kunna försäkra sig om att informationen når fram och att användaren får förståelse och medvetenhet för de risker som finns.

5.4 Bemöta säkerhetsrisker - ur ett användarperspektiv

Även om utbildningar genomförs visar resultatet att användare inte kan bli fullt medvetna kring säkerhetsrisker och hot. Att företag tar sitt ansvar och säkrar upp enheter med hjälp av utbildning och olika stöd som policys och MDM-system, är en del i arbetet med att säkra upp användandet. Men detta måste balanseras med användarens eget ansvar och intresse av att vara medveten kring säkerhetsriskerna. Användare är de som använder den mobila enheten, MDM-systemet och företagets applikationer. I och med tillgång till företagets information menar Rhee et. al (2012) att användaren utgör ett hot mot företaget. En användare kan utgöra ett hot genom att försöka få tillgång till information som den inte har behörighet till, men även genom en oansvarsfull hantering av den mobila enheten.

En av respondenterna beskriver att vi fortfarande befinner oss i ett förlegat tänkande kring mobila enheter och säkerhet. Enligt Ben Asher et. al (2011) är applikationer med information som lagras på smartphones och surfplattor sämre skyddade jämfört med de flesta stationära och bärbara datorer. Detta kan vara en av anledningarna till att användare inte förstår allvaret kring vilka konsekvenser en osäker hantering av mobila enheter kan innebära. En annan anledning kan enligt respondenterna vara att användare inte är tillräckligt intresserade av den mobila tekniken vilket också kan relateras till bristande kunskap. Den mobila enheten är ett av säljarens eller teknikerns viktigaste verktyg i det dagliga arbetet och har de inte kunskap om hur den ska hanteras innebär det en risk. Enligt Bulgurcu et al. (2010) måste anställda ha tillräckligt med kunskap kring användningen för att kunna bemöta säkerhetsriskerna.

Resultatet visade att företagen har delade meningar kring hur stort ansvar ett företag bör lägga på användaren. Mire förklarar att det handlar om eget lärande hos användaren, snarare än att företaget ger information om säkerhetsrisker. Enligt Mire bör de anställda själva ta ansvar och ha koll på de säkerhetsrisker som kan uppstå i det vardagliga arbetet. I Kandos fall finns det meningsskiljaktigheter mellan strategisk- och operativ nivå. Samtidigt som en tekniker lägger ifrån sig ansvaret och förlitar sig på att VD:n löser säkerhetsproblem, förklarar VD:n att han har förtroende för tekniker och att de hanterar enheterna korrekt.

Ur ett användarperspektiv pekar alla tre företagen på att säkerhetsrisker och hot kan bemötas genom att användaren själv tar ansvar för att skapa eget intresse och medvetenhet för de risker som finns med mobila enheter. Enligt företagen bör användaren samtidigt utgå från sunt förnuft för att hantera enheten korrekt. Däremot säger Voondo att företag inte kan lägga ansvaret på användaren fullt ut. För att uppnå

en säker hantering måste företaget stödja användaren på flera olika sätt. För att åstadkomma en säker hantering och inte enbart förlita sig på användarens sunda förnuft måste företag använda sig av utbildning, policys och MDM-system för att säkerställa hanteringen av mobila enheter.

6 Diskussion

Teorin beskriver att mobilitet har växt fram till att bli en affärskritisk faktor för att lyckas med att bedriva en mer flexibel verksamhet. Även om möjligheterna är många skapar de mobila lösningarna nya säkerhetsrisker för företaget och deras anställda. Befintlig forskning har fokuserat på hur säkerhetsrisker och hot ska hanteras rent tekniskt, men inte hur företag ska arbeta för att öka medvetenheten för riskerna inom verksamheten. Därför har vår undersökning fokuserat på hur företag bör bemöta säkerhetsrisker vid användning av mobila lösningar.

Av det resultat vi tagit del av tyder vår undersökning på att det är svårt att öka medvetenheten och förståelsen hos användare. Vi har utifrån undersökningen identifierat och tolkat att företag kan utgå från fyra olika perspektiv för att bemöta säkerhetsriskerna och säkerställa hanteringen. Dessa är ur ett policy-, tekniskt-, utbildning- och användarperspektiv. Utifrån ett policyperspektiv har undersökningen visat att utformningen av policys ofta sker på användarens bekostnad. Policys är i många fall omfattande och svårbegripliga, istället för kortfattade och lättförståeliga. Enligt Pearlson och Saunders (2013) måste användare vara väl införstådda med de riktlinjer som finns för att kunna säkerställa att policyn följs. En förutsättning är då att policys är enkla att förstå och att de uppmuntrar användare till att läsa innehållet genom att vara kortfattade och tydliga. I undersökningen har det visat sig att det företaget och användarnas restriktioner kombineras i samma dokument istället för att tydligt separera dessa genom att ha varsin policy för vardera part. Genom att separera dessa två kan en mer användarcentrerad policy tas fram. Detta kan i sin tur motivera användare till att läsa en policy och göra det enklare för dem att förstå och ta till sig innehållet. För att uppnå en säker hantering av mobila enheter kan företag även särskilja på sina användningsområden och skapa en specifik policy för mobila enheter, en så kallad mobil policy. I den mobila policyn kan företaget vara tydligt med hur de ställer sig till privata och företagsägda enheter och vilka restriktioner som ska gälla. Vårt resultat pekar i detta fall på att företag ska prioritera den enhet som är enklast att säkerställa. Företag rekommenderas också att använda företagsägda enheter i sin verksamhet, som får lov att nyttjas för privat bruk. Företagsägda enheter kan vara enklare att säkerställa än en privat BYOD-enhet. I vår undersökning har det även framkommit att företag ser på affärskritisk data på olika sätt och att behovet av policys därför är olika. Oavsett om företag anser sig ha affärskritisk data eller inte anser vi att det ska finnas policys. Ifall en säkerhetsrisk inträffar kan en policy agera som ett stöd och visa svart på vitt vilka restriktioner och åtgärder som gäller. Enligt Pearlson och Saunders (2013) ställer policys krav på användningen av mobila enheter och kan därför användas som ett stöd när en risk inträffat. En användare kan också använda en policy som en förebyggande guide för hur hanteringen ska ske.

Utifrån ett tekniskt perspektiv har vår undersökning visat att säkerhetsrisker kan bemötas genom att använda ett MDM-system, vilket styrks av tidigare forskning (Rhee et al., 2012; Souppaya & Scarfone, 2013). Resultatet pekar på att desto mer

funktionalitet ett företag använder från ett MDM-system, desto mer kontroll och styrning kan de uppnå. Däremot kan funktionalitet ställa till problem genom att undertrycka användarvänligheten. Användarvänlighet och säkerhet måste balanseras och ett bra exempel på detta kan vara att använda sig av fingeravtryck i kombination med eller istället för lösenord, för att göra autentiseringen både smidigare och säkrare. För att öka medvetenheten hos användarna för säkerhetsrisker anser vi att MDM-system ska kunna erhålla interaktiv funktionalitet som är användarfokuserad. Att använda pop-up meddelanden för att guida användaren till ett säkert användande är ett exempel på ett interaktivt stöd som ett MDM-system skulle kunna erhålla och stödja. Resultatet tyder också på att företag skulle behöva använda säkerhetsfunktionalitet som är både användarvänlig och interaktiv för att öka medvetenheten och kunskapen hos en användare och samtidigt för att kunna säkra hanteringen av de mobila lösningarna. Samtidigt som säkerhetsåtgärder kan styra och guida användaren kan dem också uppmuntra till egen reflektion och observation kring hanteringen.

När det kommer till utbildningsperspektivet antyder resultatet att utbildning är centralt för att förstå säkerhetsrisker och hur de ska bemötas, vilket även Furnell (2008) menar. Anledningen till varför utbildning anses centralt är för att användaren är den mest bidragande orsaken till att säkerhetsrisker uppstår, enligt respondenterna. Därför är det viktigt att företag prioritera säkerhetsutbildningar som kan öka medvetenheten hos de anställda för olika typer av risker. Enligt respondenterna prioriteras utbildning om säkerhet sällan, istället lägger företag resurser på utbildningar inom andra områden. Resultatet pekar också på att det är svårt att nå ut med information kring säkerhetsrisker. Att använda sig av flera olika kommunikationskanaler kan vara en lösning för att öka chansen att nå ut till användarna, vilket både resultatet och litteraturen styrker. För att informationen i utbildningen ska vara tydlig, oavsett kommunikationskanal, pekar resultatet på att konkreta exempel som användaren kan relatera till behöver användas. E-posten har i undersökningen identifierats som den mest förekommande riskkällan och är även ett verktyg som en användare hanterar både privat och i arbetet. Därför kan e-posten vara lämplig att använda i utbildningssyfte för att demonstrera hur en säkerhetsrisk kan inträffa och vilka konsekvenser det kan innebära. Att ge användare ett exempel på en risk som kan inträffa både i arbetet och privat kan resultera i en större insikt och förståelse för en säker hantering. Exempel på utbildningsformer är att hålla workshops där användaren aktivt deltar. Fler exempel kan vara att genomföra annons-kampanjer eller bjuda in gästföreläsare som är experter inom området.

Något som resultatet till skillnad från litteraturen visade var att även om utbildningar genomförs kan inte användare bli fullt medvetna kring säkerhetsrisker och hot. För att bemöta riskerna fullt ut krävs det samtidigt att användaren tar sitt eget ansvar och hanterar sin mobila enhet på ett säkert sätt. Det måste finnas en accepterad balans mellan företaget och användarnas ansvar i hur hanteringen ska säkerställas. Risken kan annars bli att någon av parterna känner att de behöver ta ett större ansvar, vilket

kan skada förtroendet för den andre. Eftersom användare ofta är motståndare till komplexa säkerhetsfunktioner som hämmar användarvänligheten kan det vara värdefullt för företag att ta användarperspektivet på allvar. Resultatet i vår undersökning pekar på att företag lägger stort ansvar på användaren och förlitar sig på att användningen sker med sunt förnuft, vilket kan resultera i att användare gör misstag och känslig information läcker ut. Att användare ska använda sitt sunda förnuft kan skapa problem för företag eftersom användare har olika förutsättningar vad gäller hantering av mobila enheter. Detta kan i sin tur handla om intresse och tidigare erfarenheter. Därför kan det vara värdefullt om företag funderar kring sitt ansvar för att stödja och motivera användaren till att uppnå ett säkert användande. Detta skulle kunna åstadkommas genom att följa de tre tidigare nämnda perspektiven: policy-, tekniskt- och utbildningsperspektiv.

7 Slutsats

Vår undersökning har visat att det är svårt att öka medvetenheten och förståelsen kring säkerhetsaspekten hos användare. Den har också visat att företag lägger stort ansvar på att användarna själva har kunskap om hur en säker hantering av den mobila lösningen går till. Grundtanken var att i slutsatsen presentera rekommendationer som går att generalisera samt applicera på alla företag. Detta visade sig vara svårare än vi tänkt eftersom företag, enligt vår undersökning, bemöter säkerhetsrisker på olika sätt beroende på storlek och bransch. Våra rekommendationer kan istället ses som en lista på olika typer av bemötanden av säkerhetsrisker, applicerbara utifrån företagets resurser och behov. Frågan vi ställdes oss i inledningen var: *Hur kan verksamheter bemöta och öka medvetenheten kring de säkerhetsrisker som medföljer företagsmobilitet?* För att bemöta säkerhetsriskerna anser vi att företag bör utgå från fyra olika perspektiv. Dessa är utifrån ett policy-, tekniskt-, utbildnings- och användarperspektiv.

7.1 Rekommendationer

Ur de fyra perspektiven har vi tagit fram konkreta rekommendationer som företag kan använda sig av för att kunna bemöta säkerhetsrisker vid användning av mobila lösningar. Dessa presenteras nedan.

Policyperspektiv - *handlar om hur säkerhetsrisker kan bemötas med hjälp av policys*

- Utforma en separat mobil policy
- Användarcentrerade policys – skilj på företaget och användarens restriktioner
- Utforma policys med hjälp av användare – ska vara enkla att läsa och förstå
- Policys som förespråkar företagsägda enheter

Tekniskt perspektiv – *handlar om hur säkerhetsrisker kan bemötas med hjälp av tekniska lösningar*

- Använda ett MDM-system
- Ju mer funktionalitet av ett MDM-system, desto säkrare hantering
- Använda MDM-system interaktivt för att öka medvetenhet
- Användarvänliga lösningar, exempelvis för autentisering

Utbildningsperspektiv – *handlar om hur säkerhetsrisker kan bemötas med hjälp av utbildning av användare*

- Använda olika kommunikationskanaler
- Använda tydliga exempel som användaren kan relatera till
- Använda utbildningsformer där användaren känner sig delaktig

Användarperspektiv – *handlar om hur säkerhetsrisker kan bemötas genom att fokusera på användaren*

- Ha medvetenhet om att användare har olika intresse och förkunskaper kring tekniken och säkerhetsaspekten
- Företag kan inte utgå från att mobila enheter hanteras utifrån ett sunt förnuft
- Uppnå en balans mellan företaget och användarens ansvar vad gäller en säker hantering

7.2 Vidare forskning

För fortsatt forskning föreslår vi två områden. Det vore av intresse utifrån ett tekniskt perspektiv att undersöka hur ett MDM-system skulle kunna göras mer interaktivt för att stödja användaren i sin hantering av en mobil enhet. Vi föreslår detta eftersom ett MDM-system har en central roll i att säkra upp mobila enheter och att de skulle behöva mer interaktiv funktionalitet som kan guida en användare till en säker hantering. Det skulle också vara intressant att se om det finns andra tekniska säkerhetslösningar som lämpar sig bättre för att öka medvetenheten för riskerna.

Det andra området som vi föreslår är utifrån ett utbildningsperspektiv. För att öka medvetenheten och förståelsen för säkerhetsrisker har vi i vårt resultat sett att det är lämpligt att använda olika kommunikationskanaler för utbildning. Därför vore det av intresse att undersöka vilka kommunikationskanaler som användaren själv anser vara effektivast för att ta till sig information kring risker och hot.

Referenslista

Androulidakis, I., & Papapetros, D. (2008, November). Survey Findings towards Awareness of Mobile Phones' Security Issues. In *Recent Advances in Data Networks, Communications, Computers, Proceedings of 7th WSEAS International Conference on Data Networks, Communications, Computers (DNCOCO'08)* (pp. 130-135).

Basole, R. C. (2007, July). The emergence of the mobile enterprise: A value-driven perspective. In *Management of Mobile Business, 2007. ICMB 2007. International Conference on the* (pp. 41-41). IEEE.

Badersten, B. (2006). *Normativ metod – Att studera det önskvärda.* Lund: Studentlitteratur AB.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011, August). On the need for different security methods on mobile phones. *In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). In *Competition Forum* (Vol. 10, No. 2, p. 117). American Society for Competitiveness.

Denscombe, M. (2009). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna*. Lund: Studentlitteratur AB.

Dubey, S. S. (2010). *IT strategy and management*. PHI Learning Pvt. Ltd..

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing*, *62*(1), 107-115.

Furnell, S. (2008). End-user security culture: a lesson that will never be learnt?. *Computer Fraud & Security*, 2008(4), 6-9.

Gao, M., Hu, X., Cao, B., & Li, D. (2014). Fingerprint sensors in mobile devices. *In Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on* (pp. 1437-1440). IEEE.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*(1), 97-114.

Holme, I. M., Solvang, B. K., & Nilsson, B. (1997). *Forskningsmetodik: om kvalitativa och kvantitativa metoder*. Studentlitteratur.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, 15(9), 1277-1288.

Krag Jacobsen, J.(1993). *Intervju: Konsten att lyssna och fråga*. Lund: Studentlitteratur AB.

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, 14(5), 0028-33.

Kvale, S. och Brinkmann, S.(2014). *Den kvalitativa forskningsintervjun*. Lund: Studentlitteratur AB.

Middleton, C., Scheepers, R., & Tuunainen, V. K. (2014). When mobile is the norm: researching mobile information systems and mobility as post-adoption phenomena. *European Journal of Information Systems*, *23*(5), 503-512.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Patel, R., & Davidson, B. (2003). *Forskningsmetodikens grunder. Att planera, genomföra och rapportera en undersökning*. Lund: Studentlitteratur.

Pearlson, K. E., & Saunders, C. S. (2013). *Strategic management of information systems*. Hoboken: Wiley.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, 6(2), 353-358.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, 21(1), 1-16.

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication*, *800*, 124.

Sørensen, C. (2014). Enterprise Mobility. *Computing Handbook. CRC Press, Boca Raton*.

Vetenskapsrådet, I. (2002). Forskningsetiska principer-inom humanistisk-samhällsvetenskaplig forskning.

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.

Internetkällor

Lopez, M. (2010). *IT best practices: Mobile policies and processes for employee-owned smartphones*. Från http://ca.blackberry.com/content/dam/blackBerry/pdf/whitePaper/northAmerica/english/IT_Best_Practices-_Mobile_Policies_and_Processes_for_Employee-owned_Smartphones.pdf - Hämtad 2014-10-16

Sybase (2011). *Mobility Advantage: Why Secure Your Mobile Devices?*, Hämtad: 2014-10-15, från http://www.contax.com/marketing/whysecurity.pdf

Bilaga 1 - Intervjumaterial

Hantering av mobila lösningar

- Vilka mobila lösningar använder ni i ert dagliga arbete?
- Till vilka system/moduler är den mobila lösningen kopplad till?
- På vilket sätt används den mobila lösningen? Vilka användningsområden? Är det ute hos kund och/eller på kontoret?
- Hur sker autentiseringen?
- Vilken betydelse har de mobila lösningarna för ert arbete?

Säkerhetsrisker och hot

- Är det din privata surfplatta/smartphone eller företagets som används i det dagliga arbetet?
- Känner ni till Bring Your Own Device (BYOD)? Upplever ni att det här fenomenet kan skapa problem i ert företag? Och i sådana fall, vilka är de?
- Vilka säkerhetsrisker upplever du att den mobila lösningen utsätts för?
- Har du/ni drabbats av någon dataförlust/intrång kopplat till era mobila lösningar?
- Kan du/ni se några brister och/eller potentiella förbättringsförslag vad gäller de mobila lösningar som ni använder?
- Finns det några ytterligare säkerhetsrisker som ni upplever som vi ännu inte diskuterat? Några risker som ni anser att mobila lösningar utsätts för?

Strategier och policys

- Har ni några säkerhetspolicys gällande mobila lösningar? Och i så fall vilka?
- Har ni satt upp egna policys och strategier eller har ni följt något ramverk? Exempelvis MDM (Mobile Device Management)?
- Vilken typ av operativsystem har enheten? Windows, Android eller iOS?
- Vart lagras datan som den mobila lösningen använder?
- Hur har användarna lärt sig att använda de mobila lösningarna? Vet de vilka risker som finns?
- Hur säkerställer ni att era säkerhetspolicys och strategier följs? Arbetar ni aktivt med att följa upp användandet?

Kim Bildtmark

Robin Jädersand

HÖGSKOLAN
I HALMSTAD

Besöksadress: Kristian IV:s väg 3
Postadress: Box 823, 301 18 Halmstad
Telefon: 035-16 71 00
E-mail: registrator@hh.se
www.hh.se