LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Mobilapplikationer - en säkerhetsrisk för dataintrång

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Marcus Andersson
Daniel Jönsson

Handledare: Umberto Fiaccadori

Examinatorer: Anders Svensson
Björn Svensson

2018-01

Mobilapplikationer - en säkerhetsrisk för dataintrång

Författare: Marcus Andersson och Daniel Jönsson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Framlagd: Höstterminen 2017

Dokumenttyp: Kandidatuppsats

Antal sidor: 58

Nyckelord: säkerhetsrisk, mobila enheter, dataintrång, mobilapplikationer, säkerhetsmedvetenhet

Sammanfattning:
En majoritet av alla verksamheter tillåter att mobila enheter får användas i tjänsten, trots ökad effektivitet för verksamheten uppstår även ökade säkerhetsrisker för dataintrång. Genom intervjuer med ansvariga för IT-säkerheten på verksamheter vilka är stora nog att inneha en IT-avdelning kunde vi undersöka deras konkreta åtgärder för att säkerställa de mobila enheterna för att etablera deras säkerhetsmedvetenhet. I studien kommer vi fram till att säkerheten fokuseras kring den fysiska säkerheten av enheten samt säkra anslutningar till verksamhetsresurser. Vi finner att verksamheter är medvetna om säkerhetsrisker för de mobila enheterna men att det saknas säkerhetsåtgärder samt direktiv för de anställda när det kommer till den interna säkerheten på enheterna.

Figurer och tabeller

1 Introduktion

Förmågan att kommunicera över en telefon kan dateras tillbaka till Alexander Graham Bell för mer än ett sekel sedan. Det var inte förrän 1973 som Martin Cooper blev först med att göra det första mobilsamtalet och mobiltelefonen kom i bruk (PC Magazine, 2011). Sedan mobiltelefonens kommersiella framtåg har fler funktioner tagits fram än att ringa och en särskild populär funktion är möjligheten för användare att installera tredjepartsprogram. Tack vare att det går att installera mjukvara från en tredje part väljer många mobilanvändare att installera applikationer till sina mobiler.

Mobilapplikationer har blivit populärt att ladda ner, på Apple App Store finns det mer än 2 miljoner appar tillgängliga medan på Google Play Store börjar det närma sig 3 miljoner, till dessa appar har det skett miljarder av nedladdningar (App Store, 2017; Google Play, 2017). I takt med denna popularitet sker konstant forskning och utveckling inom Wireless Sensor Networks (WSN) samt mobilteknik (Koceski & Koceska, 2016). Detta möjliggör att mobiltelefoner kan bli integrerade med nya funktioner och nya typer av appar kan utvecklas. Precis innan millennieskiftet började mobiler bli integrerade med ett inbyggt Global Positioning System (GPS) (PCWorld, 2012). Med hjälp av så kallad Geotracking, där mobilen identifierar en individs nuvarande fysiska position genom att hämta platsdata från mobiltelefonen, kunde positionsbaserade applikationer börja användas.

1.1 Bakgrund

Mobilapplikationer begär ofta tillgång till känslig information på användarens mobil, som till exempel enhetens unika ID, platsdata, kontaktlista och bilder (Wang et al, 2017). Operativsystemet (OS) Android begär av apputvecklare att deklarera vilka funktioner och data applikationen kommer använda sig av, dock saknas det i nuläget förklaringar om syftet kring användningen (Wang et al, 2017). En app kan exempelvis använda platstillåtelse för olika syften som reklam och geotagging (Wang et al, 2017). Geotagging, där en geografisk position anknyts

till ett objekt som en video eller bild, har blivit ett problem i vissa fall. Då platsdata kan finnas inbäddad i en bild eller video går det att lokalisera källans ursprung. Detta har öppnat upp möjligheten för att kartlägga individers rörelser på en karta (New Scientist, 2010).

Lyne (2011) förklarar att i moderna mobila plattformar inkluderar de funktionalitet där det går att begränsa teknologi där applikationer kan isoleras från varandra: “Sandboxing”. Lyne (2011) förklarar vidare att säkerhetskontrollerna på mobiler har förändrats från det konventionella OS, istället för att ha tillgång till särskilda nycklar förlitar sig säkerheten mer på individers val av konfigurering. Inom val av konfigurering ingår vare sig en applikation behöver ha tillgång till användarens platsdata, SMS, e-post och annan information.

Mobilanvändare har inget sätt att veta hur eller varför känslig information kommer nyttjas av en applikation samt saknar kontroll över på vilket sätt informationen kommer användas (Wang et al, 2017). Om mobilanvändare har mer insikt och kontroll över syftet med användningen av känslig information kan det till viss del minska att insamlad data missbrukas (Lin et al, 2012). Lin et al (2012) förklarar att det borde finnas möjlighet för användare att neka tillåtelse för geotagging men ändå tillåta kartsökningar med hjälp av platsdatan.

Mobiltillverkaren av BlackBerry har tagit de nämnda säkerhetsriskerna med mobilapplikationer på allvar och erbjuder mobiltelefoner där det finns två olika isolerade arbetsmiljöer på samma mobil, detta ska hålla isär arbetsdata från nöje- och speldatan (Lyne, 2011). Ägaren av en modern BlackBerry kan använda sig av en särskild app för ökad säkerhet, DTEK™ by BlackBerry® for Android™ (BlackBerry, 2017). Applikationen övervakar alla övriga applikationer på mobilen och skickar notifieringar till användaren om exempelvis en illasinnad app utan tillåtelse tar bilder eller videor, slår på mikrofonen, skickar meddelanden och försöker få åtkomst till användarens kontakter samt position (BlackBerry, 2017). Dessa olika metoder för att öka säkerheten kan ses som säkerhetsåtgärder vilka kan stödja säkerhetsmedvetenheten. BlackBerrys totala marknadsandel 2016 på mobiltelefonmarknaden var bara 0,0482 % (Business Insider, 2017).

Då moderna mobiltelefoner har nästintill samma kapacitet som en vanlig dator har verksamheter tillhandahållit mobilapplikationer till sina anställda för att stödja deras arbetsuppgifter (Hemdi & Deters, 2016). Många verksamheter stödjer konceptet av Bring Your Own Device (BYOD) vilket tillåter anställda att använda deras personliga enheter för arbetsrelaterade uppgifter (Hemdi & Deters, 2016). Utöver BYOD används även Choose Your Own Device (CYOD) och Use What You are Told (UWYT) (Brodin, 2016). För CYOD kan en anställd välja en enhet att utföra arbetsuppgifter på, dock äger verksamheten enheten och kan konfigurera och kontrollera den (Brodin, 2016). Vid UWYT bestämmer verksamheten vad den anställda ska använda sig av och har samma kontroll och äganderätt som nämndes för CYOD (Brodin, 2016).

Dhingra (2016) har studerat BYOD och uppger att det finns allvarliga säkerhetsrisker att upprätthålla dataintegriteten då verksamhetsdatan finns på ett allmänt nätverk och nås via en allmän åtkomstpunkt. För att förbättra säkerheten kan verksamheter använda sig av Virtual Private Network (VPN) när anslutningar utförs till företagets nätverk (Dhingra, 2016). Används VPN skapar det en säker förbindelse mellan källan och destinationen och tillhandahåller skydd för all data som färdas över nätverket (Dhingra, 2016).
Dhingra (2016) berättar att om de anställda använder CYOD eller UWYT förbättras säkerheten för verksamhetsdatan ytterligare då verksamheten kan implementera systemkonfigurationer efter säkerhetsbehov, kryptera data, utföra undersökningar på enheten samt övervaka dataanvändning för att upptäcka missbruk eller dataintrång. Används BYOD är verksamhetens kontroll över säkerheten låg och ansvaret för säkerheten läggs på den anställde (Dhingra, 2016). Anställda på en verksamhet med BYOD är ofta motvilliga till att implementera den gällande säkerhetspolicyn vilket ökar säkerhetsriskerna (Dhingra, 2016).

Tech Pro Research (TechPro, 2015) har utfört studier kring användningen av BYOD på verksamheter sedan 2013 och fann då att 44% av verksamheter tillät BYOD användning. Två år senare under 2015 undersöktes användningen av BYOD igen och då låg siffrorna på 60% varav 14% skulle införa BYOD inom de kommande 12 månaderna (TechPro, 2015).

1.1.1 Tidigare forskning - mobilapplikationer

Lin et al (2012) utförde en studie rörande användarnas förväntningar kring applikationers nyttjande av känslig information. Studien fann att användarnas förväntningar skilde sig mot de verkliga anledningarna varför deras information samlats in (Lin et al, 2012). Lin et al (2014) utförde en djupgående analys på 400 populära tredjepartsbibliotek och kartlade syftet med apparnas begäran av tillgång till särskilda enhetsfunktioner och känslig data. Studien fann att syftena varierar allt mellan riktad reklam, olika analysmetoder, sälja datan vidare osv, dessa syften blir inte förklarade för användaren om hur deras information kommer användas (Lin et al, 2014). Om applikationerna förklarade syftet till användningen av funktioner och känslig data skulle detta påverka användarnas konfigurering av applikationers behörighet att begränsas (Lin et al, 2014).

1.2 Problemområde

BYOD blir allt mer populärt på verksamheter med tiden enligt Tech Pro Research (2015) och som tidigare nämnt (kap 1.1) kan nyttjandet av BYOD öka säkerhetsriskerna. Eftersom BYOD ägs helt av den anställda kan bara verksamheter hänvisa till att särskilda säkerhetspolicyer ska följas. Då anställda ofta är motvilliga till att implementera den gällande säkerhetspolicyn (kap 1.1) blir verksamhetens kontroll över säkerheten låg.

Om en slutanvändare ger tillstånd till att en enhetsfunktion får användas ges ingen förklaring till syftet med användningen av applikationen (kap 1.1). Med bristande säkerhet på BYOD/CYOD/UWYT ser vi en hotbild när mobilapplikationer kan få tillgång till olika enhetsfunktioner där eventuell verksamhetsdata kan finnas eller användas för att få tillgång till verksamhetens data. Denna hotbild gäller vare sig det är medveten eller automatiserad datainsamling av applikationen då ett dataintrång kan ske.

Med statistiken från Tech Pro Research (TechPro, 2015) i kombination med att applikationer ofta begär tillgång till känslig data (kap 1.1) ställer vi oss frågan om varför BYOD kan fortsätta vara

så populärt när det tycks finnas brister när det kommer till säkerhetsaspekter. Denna bakgrund leder fram till vår forskningsfråga om till vilken utsträckning denna säkerhetsproblematik är känd på verksamheter.

1.3 Forskningsfråga

Hur medvetna är IT-chefer och övriga IT-ansvariga om säkerhetsproblematiken med BYOD/CYOD/UWYT?

1.4 Syfte

Vi vill reda ut verksamheters medvetenhet om säkerhetsriskerna med att mobila enheter får användas på verksamheter då fördelarna tycks vara mer belysta än nackdelarna. Vi önskar även mer specifikt analysera hur verksamheter arbetar med att säkerställa den interna säkerheten för de anställdas enheter för det är där vi ser en allvarlig hotbild för dataintrång.

1.5 Avgränsning

BYOD/CYOD/UWYT innefattar olika enheter som bärbara datorer, surfplattor och smartphones. Vi väljer att avgränsa oss mot enheter där konfigurering av applikationers behörighet baseras på användarens godkännande med ett knapptryck. Enheter som surfplattor och smartphones har den nämnda konfigureringen och illustrerar därför en viss säkerhetsproblematik till att applikationer får åtkomst till känslig data.

Med medvetenhet syftas inte på vilka implikationer som kan ske utan om den konkreta medvetenheten där faktiska åtgärder finns.

2 Litteraturgenomgång

I detta kapitel bearbetas litteratur som ligger till grund för studiens forskningsfråga. Detta resulterar till en teoretisk sammanfattning vilken intervjufrågorna kommer vara utarbetad från och utgöra grunden för den empiriska studien. Till en början presenteras läsaren för vanligt förekommande begrepp vilket ska öka läsförståelsen för studien. Efter detta förklaras olika aspekter som relaterar till problemområdet vilket ska förse läsaren med en ökad insyn i studien.

2.1 Förklaringar av vanligt förekommande begrepp

2.1.1 Säkerhetsrisk

En säkerhetsrisk är möjligheten för att drabbas av skada eller förlust (Alberts & Dorofee, 2003). Alberts & Dorofee (2003) ser en risk som oönskade negativa konsekvenser av en händelse vari antingen individer eller ett naturligt skick på ett ting kan vara orsaken för det inverkade. Ledningen för en verksamhet utför ofta en risk- och hotanalys vilket är ett tillvägagångssätt där ett säkerhetsbeslut avgörs baserat på värdet på objektet i fråga, omfattningen på hotet av objektet samt kostnaden för att reducera hotet (Gollmann, 2011). Arlitsch & Edelman (2014) förklarar att hoten ökar som ett resultat av ‘Internet of Things’ (IoT) där förhållandet blir mer sammanflätat mellan den virtuella samt fysiska världen i människors vardag. Detta medför att ett dataintrång kan bli mer omfattande än tidigare på grund av att mer personlig information finns tillgänglig i samband med IoT (Arlitsch & Edelman, 2014).

2.1.2 Säkerhetsmedvetenhet

Att vara säkerhetsmedveten på en verksamhet handlar om att kontinuerligt utbilda och träna sina anställda om de senaste utvecklingarna inom informationssäkerhet (Dahbur m.fl, 2017). Dahbur m.fl (2017) förespråkar att verksamheter överväger följande element när säkerhetsmedvetenhet ska eftersträvas:

- **Personer:** Rätt anställd ska vara positionerad i sin rätta roll och ansvara för de rätta ansvarsområdena. Anställda måste också vara utbildade samt tränade för att förbättra deras kunskap, skickligheter och attityd med hänsyn till säkerhet.
- **Teknologi:** Teknologi måste vara modern samt användarvänlig då anställda måste vara tränad inom tekniken baserat på deras roller och ansvarsområden. Teknologin borde även vara konfigurerad ordentligt för att implementera funktionaliteten och säkerhetsfunktionerna.
- **Processer och procedurer:** Processer måste bli designade och implementerade för att reglera hur teknologin används av de anställda baserat på deras roller och ansvarsområden. Procedurer måste bli definierade och implementerade enligt de riktlinjer av *bästa metoder* (best-practices) för att främja processernas effektivitet.
- **Policyer:** Policyer måste vara tydligt definierade, använda lämpligt språk där alla anställda kan förstå innebörden, för att uppnå verksamhetens säkerhetsmål. Ledningsstöd måste engageras i tillämpningen av policyer för att säkerställa att de efterföljs samt dess effektivitet.

Allam m.fl (2014) förklarar att när ökad medvetenhet finns influeras beteendet, dvs vad folk gör, vilket ska minska säkerhetsrisken genom att fokuset läggs på individen och inte enheten som ska skyddas. I kombination med att mobilteknik förbättras med tiden kommer användare samt ledning finna olika nya metoder att utföra arbetsuppgifter på (Allam m.fl, 2014). Detta kan innebära att metoderna som nyttjas kan gå över existerande säkerhetsbarriärer om inte verksamheten applicerar en gränsmodell för medvetenhet (Allan m.fl, 2014). Gränsmodellen är till för att forma policyer, procedurer och kontroller där en kontinuerlig bedömning görs för att förbättra samt bibehålla medvetenheten av informationssäkerheten i den gällande verksamheten (Allam m.fl, 2014). Faktorer som borde forma policyer, procedurer och kontroller relateras till vad ledningen önskar utföras på de mobila enheterna, produktivitetsnivån, ansträngningsnivåer av de anställda att utföra arbetsuppgifter och graden av arbetsbelastning (Figur 1) (Allam m.fl, 2014).

Figur 1: Modell för utformning av policyer och procedurer (Allan m.fl, 2014)

Om anställda använder mobila enheter ofta och blir påverkade av tids- och arbetskrävande säkerhetsinstanser måste detta balanseras med exempelvis produktivitetsnivån, arbetsbördan och vad ledningen begär av de anställda (Allan m.fl, 2014). För att säkerhets- medvetenheten ska kontinuerligt bibehållas och förbättras måste återkoppling ske från alla medverkande parter annars implementeras bara ‘traditionell säkerhet’ som fördärvas när maximerad effektivitet önskas av alla (Allan m.fl, 2014).

En god säkerhetsmedvetenhet kan hjälpa till att förebygga, eller åtminstone mildra, de olika säkerhetsriskerna (Dahbur m.fl, 2017; Allam m.fl, 2014). Den kan även öka förståelsen om olika säkerhetstillämpningar samt stödja benägenheten för slutanvändare till att följa de (LeVeque, 2006). LeVeque (2006) förklarar att oavsett mängden av tekniska säkerhetstillämpningar eller säkerhetsmanicker kan de inte övervinna motståndet av slutanvändare som är ovilliga till att samarbeta eller är outbildade.

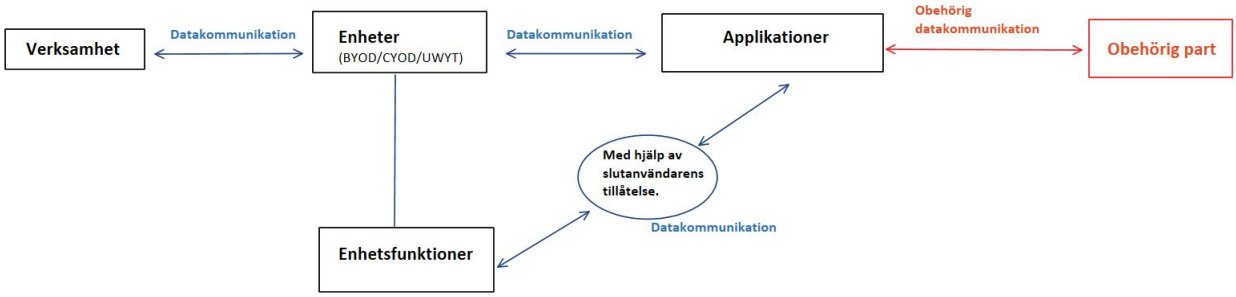
2.1.3 Slutanvändare

"The person, or persons, who operate or interact directly with the product." (IEEE, 1998, s. 3). Förutom att en slutanvändare är den person som avses använda en produkt, skiljer sig denna person från de personer som var involverade i utvecklingen eller marknadsföringen av produkten i fråga (Ordbok 2).

2.2 Problematik i informationsflödet

En verksamhet som använder sig av portabla enheter (BYOD/CYOD/UWYT) tillåter en datakommunikation mellan enheterna och verksamheten med dess olika typer av system. På enheterna finns olika enhetsfunktioner, kamera, mikrofon, GPS osv, vilka en slutanvändare behöver besluta vare sig en applikation kan få tillåtelse till. När tillstånd har getts för en applikation kan en datakommunikation existera mellan enheten och applikationen. En applikation som laddas ner från Apple App Store eller Google Play Store begär ofta tillgång till ett flertal enhetsfunktioner (Wang et al, 2017). Förutom självklara enhetsfunktioner, exempelvis att en navigationsapp behöver tillgång till en slutanvändares GPS, begärs ofta tillgång till andra enhetsfunktioner som inte är lika självklara till huvudsyftet med applikationen. Lin et al (2014) som studerat anledningarna varför applikationer begär tillgång till olika enhetsfunktioner har kommit fram till att det rör sig bland annat om riktad reklam, analysera datan och att sälja datan vidare. Om en applikation har tillåtelse till en enhetsfunktion och det saknas säkerhetsåtgärder för att skydda verksamhetens data existerar en säkerhetsproblematik. Säkerhetsproblematiken existerar fastän det finns en 'säker' anslutning mellan enheten och verksamheten då om en tillåtelse exempelvis getts till en enhetsfunktion kan datainsamling påbörjas (Leavitt, 2013). En mikrofon kan spela in en ljudfil under ett affärsmöte. Ges tillåtelse till GPS kan det vara av intresse för en obehörig part om många högt uppsatta chefer visar platsdata hos ett annat företags huvudkontor. Har en applikation tillåtelse till enhetens kamera kan eventuella bilder som tagits kommuniceras till en obehörig part.
De olika enhetsfunktioner kan därför åsidosätta 'säkra' anslutningar om ingen relevant

säkerhetsåtgärd tillämpas som exempelvis ett mjukvaruprogram som kontrollerar övriga mjukvaruprogram och att isolera enhetsmiljön (Kap 1.1) (Chang m.fl, 2014; Leavitt, 2013).



Figur 2. Ett exempel på ett dataflöde. Figuren visar en representation hur dataflödet transporteras mellan olika parter: verksamhet, enheter, enhetsfunktioner, applikationer och obehörig part. På enheterna finns enhetsfunktioner såsom GPS, kamera, mikrofon osv. Med hjälp av slutanvändarens tillåtelse att applikationer kan använda sig av enhetsfunktioner kan en obehörig datakommunikation ske via applikationerna och verksamhetens data om inga säkerhetsåtgärder tillämpas.

2.3 Dataintrång

Ett dataintrång är en incident där känslig, skyddad eller konfidentiell data kan ha blivit använd, granskad eller stulen av en obehörig part (Brown, 2016). Brown (2016) förklarar att förutom att data kan bli utsatt för ett dataintrång kan implikationerna även innebära problem för verksamhetens rykte samt juridiska utmaningar. Då verksamheter kan behandla känslig information som exempelvis kreditkortsinformation, immateriella rättigheter och olika företagshemligheter kan ett dataintrång leda till åtal då en incident kan bryta mot särskilda sekretesslagar (Brown, 2016).

Enligt Forbes (2015) topp 5 lista över svagheter för dataintrång listas:

- **Anställda:** Ett topphot för dataintrång är interna attacker då anställda vilka har tillgång till känslig data kan missbruka den.
- **Osäkra mobila enheter (BYOD):** När BYOD används på verksamheter saknar verksamheten kontroll över hur enheten används samt vilka säkerhetstillämpningar som appliceras för enheten i fråga. Saknas policyer för BYOD förstärks problemet ytterligare.

- **Molnlagringsapplikationer:** Det finns säkerhetsrisker med vissa molnlagringstjänster när inte datakryptering används och en avsaknad av tvåfaktorsautentisering.
- **Tjänsteleverantör från en tredje part:** Förutom en molnlösning kan andra typer av tjänster användas från en tredje part. När den tredje parten har bristande säkerhet men tillgång till verksamhetens data kan ett dataintrång ske via den tredje parten.
- **Illasinnade attacker:** En illasinnad attack för att utföra ett dataintrång kan ske med olika medel. En användare kan råka ladda ner skadliga program genom att trycka på en misstänksam länk eller genom att besöka en hemsida (när enheter samt olika noder saknar antivirus program och säkerhetsmjukvara). Ett annat sätt är när en användares lösenord knäcks. Om systemen, applikationerna samt webbläsaren inte är uppdaterade löper de större risk för att attackeras. Om säkerhetspolicyer saknas där exempelvis anställda inte vet hur en misstänksam länk ser ut alternativt ett misstänksamt e-postmeddelande.

För vår studie är det värt att kolla närmare på 3 av dessa svagheter nämligen anställda, osäkra mobila enheter (BYOD) och illasinnade attacker. Som nämnts tidigare (Kap 2.1.2) när verksamheter ska eftersträva säkerhetsmedvetenhet är det personer, teknologi, processer och procedurer samt policyer som behöver övervägas.

2.3.1 Anställda

Vi ser en koppling mellan ‘personer’ (Kap 2.1.2) och ‘anställda’ (Kap. 2.3) dvs att det är de anställda som påvisar en säkerhetsrisk för dataintrång. När de anställda saknar utbildning samt träning kan deras säkerhetsmedvetenhet försämras (Dahbur m.fl, 2017). När anställda har tillgång till mer information än vad de behöver inom sin roll och ansvarsområde kan ett internt dataintrång utgöra en mer påtaglig säkerhetsrisk (Dahbur m.fl, 2017). Förutom att mer känslig information kan spridas finns även en ökad säkerhetsrisk med att deras enheter de använder i tjänsten kan kommunicera mer information till en obehörig part med hjälp av applikationerna på enheterna (Kap 2.2).

Gollmann (2011) konkluderar också att det är de anställda som står för majoriteten av incidenter och den största andelen av skadegörelse.

2.3.2 Osäkra mobila enheter (BYOD)

Gollmann (2011) förklarar att när det finns svagheter eller brister i teknologin kan det möjliggöra för obehöriga parter att ta över kontrollen av en enhet. En illasinnad angripare kan då korrumpera data på enheten eller använda enheten som en typ av språngbräde för att utföra attacker mot en tredje part (Gollmann, 2011).

Om 'teknologi' (Kap 2.1.2) inte är konfigurerad ordentligt för att implementera säkerhetsfunktioner saknas säkerhetsmedvetenhet för verksamheten (Dahbur m.fl, 2017). Förutom BYOD som klassificeras "osäkra" gäller samma princip för CYOD och UWYT då fastän verksamheten kan övervaka användningen på enheter de själva har utfärdat (CYOD & UWYT) (Dhingra, 2016) ser vi en lucka i att upptäcka dataintrång via en applikation. När en slutanvändare ger tillstånd åt en applikation till en enhetsfunktion på respektive enhetstyp som kan användas i tjänsten blir det svårt att kontrollera dataanvändningen, upptäcka missbruk eller dataintrång som enligt Dhingra (2016) var fördelen med att använda CYOD & UWYT. Har en slutanvändare gett tillstånd till kameran åt en applikation detekteras inget dataintrång när en verksamhetsrelaterad bild kommuniceras till en obehörig part då applikationen har tillåtelse från slutanvändaren.

2.3.3 Illasinnade attacker

Dataintrång av illasinnad karaktär kan lättare ske när det saknas 'policyer' samt 'processer och procedurer' för hur teknologin används av de anställda (Kap 2.1.2) då det medför en försämrad säkerhetsmedvetenhet (Dahbur m.fl, 2017). När slutanvändare på olika enhetstyper inte förhåller sig till policyer alternativt inte förstår sig på den, pga exempelvis olämpligt eller otydligt språk, minskar förståelsen om olika säkerhetstillämpningar samt slutanvändares villighet till att följa de (LeVeque, 2006). Saknas önskvärda standards eller policyer ökar säkerhetsrisken för illasinnade attacker då slutanvändare inte följer säkerhetsföreskrifter exempelvis att uppdatera deras antivirusprogram (Gollmann, 2011).

Att applikationer får tillåtelse till enhetsfunktioner har nämnts tidigare (Kap 1.2) som en hotbild vare sig det är en medveten (illasinnad) eller automatiserad datainsamling av verksamhetsdata. Om det finns virus på en applikation, som exempelvis använder sig av enhetsfunktioner för dataintrång, kommer slutanvändaren inte erhålla en varning om att applikationen i fråga innehåller skadlig kod om inget antivirusprogram finns eller är bristfällig. Enligt Chang m.fl (2014) är skadliga program ett växande problem på mobila enheter då de tenderar att bland annat stjäla känslig information vilket beskrivs som ett säkerhetsbekymmer då dataläckage kan ske från verksamheten.

2.4 Säkerhetsåtgärder

Begreppet säkerhetsåtgärd är definierat som åtgärder utförda som skydd mot stöld, spionage, sabotage (Ordbok 1) samt liknande negativa händelser vilket kan hända mot det som önskas skyddas.
När säkerhetsåtgärder ska implementeras i praktiken på en verksamhet, samt informationsteknologi (IT) i allmänhet, är det ett ledningsbeslut (Gollmann, 2011). Den planerade tekniska säkerhetsåtgärden måste samverka med organisatoriska åtgärder för att kunna bli effektiv (Gollmann, 2011). Ledningsbeslutet ska vara baserat på en analys på de potentiella riskerna och hoten (Gollmann, 2011) (Kap 2.1.1).

När verksamhetsdata kan finnas på en enhet existerar ett säkerhetshot om enheten skulle försvinna eller bli stulen (Chang m.fl, 2014). Ett annat problem uttrycks när användare på en enhet blandar deras personliga data med verksamhetens data, detta problem kan resultera till att av misstag dataläckage sker till en obehörig part (Chang m.fl, 2014). För att tackla dessa säkerhetsrisker förespråkar Chang m.fl (2014) att verksamheter tillämpar säkerhetsåtgärder i form av säkerhetspolicyer, Mobile Device Management (MDM) och separationstekniker. Leavitt (2013) tar upp liknande säkerhetsrisker som Chang m.fl (2014) men lägger till att det även finns ett hot när olika enhetsfunktioner kan olovligen användas för att få tillgång till känslig information. Leavitt (2013) förespråkar också tillämpningen av MDM samt separationstekniker

men talar även för att använda sig av Mobile Application Management (MAM). Dhingra (2016) rekommenderar också användningen av MDM och MAM och berättar att de kan stödja verksamheten att kontrollera de olika enheterna som används av de anställda. Brodin (2016) förespråkar också användning av mjukvaruprogram, som exempelvis MDM, dock förbättras bara säkerheten om den anställde, i ett BYOD scenario, tillåter att särskilda mjukvaruprogram kan installeras på deras personliga enhet. Det är även upp till den anställde om installation tillåts, med BYOD, att avgöra hur verksamheten får kontrollera användningen på enheten, dvs att de kan begränsa verksamhetens kontroll (Brodin m.fl, 2015).

2.4.1 Säkerhetspolicyer

Gollmann (2011) samt LeVeque (2006) anser båda att policyer är en god säkerhetsåtgärd vilken kan stödja att informationssäkerheten har en omfattande inverkan på IT-utveckling och IT-användning. Policyer är uppgifter om beteende eller handlande vilket en verksamhet förväntar sig eller önskar undvika (LeVeque, 2006). Policyer bör definiera vad som ska tillämpas samt vilka individer är ansvariga för tillämpningen (LeVeque, 2006). Policyer ska beskriva vem som är ansvarig att utföra en uppgift samt ställa krav på individer i en verksamheter där det specificeras vad de får göra tillsammans med vad de inte får göra (LeVeque, 2006).

Då säkerhetspolicyer ska täcka avsevärda områden på en verksamhet på olika nivåer i detalj förklarar Gollmann (2011) att policyer kan kategoriseras mellan organisatoriska och automatiserade säkerhetspolicyer. Organisatoriska säkerhetspolicyer är en uppsättning av de lagar, regler samt praxis som reglerar hur en verksamhet hanterar, skyddar och distribuerar resurser för att uppnå särskilda säkerhetsmål på den gällande verksamheten (Gollmann, 2011). Automatiserade säkerhetspolicyer är en uppsättning av restriktioner och egenskaper som specificerar hur ett datorsystem förebygger att data missbrukas och bryter mot de uppsatta organisatoriska säkehetspolicyerna (Gollmann, 2011).
Chang m.fl (2014) berättar att för säkerhetspolicyer som täcker BYOD bör de innehålla identifieringen av vilka enheter som kan användas inom verksamhetens nätverk, tillåtna och förbjudna applikationer, samt även klassificera vilken typ av data som inte ska lagras på den

lokala enheten. Fastän Chang m.fl (2014) rekommendationer förklarar Brodin m.fl (2015) att många verksamheter saknar säkerhetspolicyer för BYOD användning samt riskhantering om något dataintrång sker eller bryter mot organisatoriska säkerhetspolicyer.

2.4.2 Separationstekniker

Genom att införa olika separationstekniker i ett BYOD scenario kan säkerheten öka för verksamheten då verksamhetens data och appar samt personliga appar och data kan förvaras och köras separat på samma enhet men på ett säkert vis (Chang m.fl, 2014). En lyckad implementation av säkerhetsåtgärden kräver att den anställdas personliga miljö inte äventyrar säkerheten för verksamhetsmiljön (Chang m.fl, 2014). Samtidigt krävs det av verksamhetsmiljön att den inte inskränker på den anställdas personliga integritet (Chang m.fl, 2014). Om verksamheten önskar utreda BYOD användning är det också av rättslig betydelse att bara information rörande verksamheten samlas in då det annars skulle försvåra utredningen om den personliga integriteten kränks (Dhingra, 2016). För att uppnå målet av en lyckad separation förespråkar Chang m.fl (2014) att verksamheter använder sig av virtualisering, ‘dual boot’ och virtuella mobila plattformar. En fördel med separering är att verksamhetsdatan kan rensas från en enhet fastän den personliga datan bibehålls intakt (Leavitt, 2013). En utmaning enligt Leavitt (2013) är att uppnå en stark kryptering inom systemet med diverse separeringstekniker där fokus ligger på att skydda verksamhetens data från andra miljöer.

2.4.2.1 Virtualisering

Vid virtualisering kan en mobil enhet vara värd för flera virtuella maskiner som agerar som en dator inom samma OS (Chang m.fl, 2014; Gollmann, 2011). Fördelen med detta är att verksamhetsmiljön kan vara helt skild från den personliga miljön (Gollmann, 2011). Dock varnar Chang m.fl (2014) att prestandan kommer försämras och att verksamhetens data kan riskeras om den anställdas OS äventyras. Därför är det viktigt enligt Gollmann (2011) att användare ska kunna anropa OS men att användaren inte ska kunna missbruka den. Gollmann (2011) förespråkar därför att det ska finnas restriktioner och anropen ska kontrolleras i enheterna. Denna säkerhetsåtgärd kan finnas i mjukvara, hårdvara och OS men fallerar om det fysiska lagret

attackeras (Gollmann, 2011) och är därför det mest utsatta lagret som behöver skyddas (Chang m.fl, 2014).

2.4.2.2 Dual boot

Vid dual boot kan två olika OS installeras på en enhet där användaren kan skifta mellan de (Chang m.fl, 2014). Med dual boot kan ett OS exempelvis vara för användarens personliga miljö och den andra för verksamhetens miljö. På CYOD och UWYT kan restriktioner för anrop till OS enkelt implementeras och kontrolleras men återigen när det kommer till BYOD sammanhang är det användaren som äger enheten och enligt Dhingra (2016) bestämmer vad som får implementeras. Det kan därför ur ett användarperspektiv förmodas vara mer godtagbart att tillåta restriktioner till OS som används inom verksamheten när det personliga OS kan lämnas i fred. Chang m.fl (2014) berättar att med denna separeringsteknik utförs helt skilda miljöer vilket kan förbättra säkerheten, dock kan växlingen mellan OS vara tidskrävande och negativt för användbarheten.

2.4.2.3 Virtuella mobila plattformar

En annan metod för att separera den personliga miljön från verksamhetens miljö är att fjärransluta virtuellt till verksamhetens datacenter (Chang m.fl, 2014). Detta kan möjliggöras på olika mobila enheter genom att installera en särskild klientapp vilken kommer se till att ingen verksamhetsrelaterad data lagras på enheten i fråga (Chang m.fl, 2014). Metoden kräver dock en konstant och stark internetanslutning vilket kommer fastställa prestandan (Chang m.fl, 2014). Gollmann (2011) berättar att särskild tillsyn krävs för fjärranslutning där åtkomstkontrollen ska ligga i fokus vilken kommer avgöra vem exakt som kan få tillgång till känslig information. Kontrollinstanser kan exempelvis vara att bara tillåta åtkomst till redan kända ‘media access control’ (MAC) adresser och ytterligare autentiseringskrav om åtkomst till särskilt känsliga resurser önskas (LeVeque, 2006).

2.4.3 Säkerhetsmjukvara på enheter

2.4.3.1 MDM

MDM är ett verktyg vars syfte är att hantera mobila enheter där en verksamhet kan säkerställa att säkerhetspolicyer följs på enheterna (Chang m.fl, 2014). MDM kan tillämpa kryptering av verksamhetens data och inaktivera sensorer samt särskilda inställningar på enheterna för att förebygga dataläckage och även möjlighet att stänga ner och radera innehållet på enheterna (Leavitt, 2013; Chang m.fl, 2014).

Trots att verksamheten får mer kontroll över de mobila enheterna är MDM bristfällig i och med att den är reaktiv och inte proaktiv mot exempelvis ett dataintrång (Leavitt, 2013). Skulle ett dataintrång ske på en enhet skulle verksamheten kunna utföra en rensning av data på enheten i fråga men i efterhand när intrånget redan har skett (Leavitt, 2013). MDM är också beroende av att vara nätverksuppkopplad för att verksamheten ska kunna utföra säkerhetskommandon till enheterna (Leavitt, 2013).

2.4.3.2 MAM

MAM är ett verktyg vilket är till för att hantera och begränsa användarens tillgång till särskilda applikationer samt skydda de tillåtna programmen och datan som finns på de (Leavitt, 2013). En verksamhet kan därför med MAM säkerställa att de anställda inte installerar förbjudna applikationer och införa policyer för en applikations mjukvarubeteende (Leavitt, 2013). Restriktioner kan vara att bara godkända applikationer kan få tillgång till verksamhetens data och nätverk (Leavitt, 2013). Leavitt (2013) varnar dock för att MAM inte på något sätt skyddar datan utan skyddet som mottas är i relation till de policyer som är uppsatta där MAM kan säkerställa datan i en förutsatt miljö men eventuellt inte i en annan.

2.5 Mätning av säkerhet

Studien ska undersöka den konkreta medvetenheten där faktiska åtgärder finns och därför vill vi konkretisera vad vi ämnar ta reda på. Att vara säkerhetsmedveten på en verksamhet har beskrivits att uppnås genom att utbilda och träna de anställda samt att se över elementen personer, teknologi, processer och procedurer samt policyer (Dahbur m.fl, 2017). Därför är undersökningen mer intresserad av konkreta åtgärder som verksamheter har implementerat för de nämnda medvetenhetsfaktorerna. Säkerhetsåtgärderna är bara effektiva eller lyckade om de faktiskt säkerställer att säkerhetspolicyer följs på de mobila enheterna (Gollmann, 2011). De flesta verksamheter kan förmodas ha instiftat en policy som berör att verksamhetens data inte ska delas med obehöriga parter. Dock brister verksamheters säkerhetsåtgärder om de inte har skydd för den problematik som har beskrivits (Kap 2.2) då policyn om att skydda data inte efterföljs. För att skydda verksamhetens data kan det inte uppnås genom att förlita säkerheten på en särskild aspekt på enheterna då ett sådant tillvägagångssätt inte kommer leverera ett tillräckligt skydd (Leavitt, 2013). Det krävs därför olika typer av skydd än att exempelvis bara installera MAM på en mobil enhet då de olika presenterade säkerhetsåtgärderna har olika individuella brister som kan äventyra säkerheten.

Gollmann (2011) berättar att för mätning av säkerhet finns det olika metoder för att fastställa hur bra eller dålig säkerheten egentligen är. Säkerhetsmätningen kan bli sedd ur ett objektivt perspektiv där exempelvis verksamheter följer den senaste uppdateringen eller relevanta ISO-certifikat (Gollmann, 2011). Mätningen kan också innehålla ett subjektivt perspektiv där säkerhetsmedveten hos de anställda undersöks eller fastställs efter verksamhetens rykte rörande säkerhet (Gollmann, 2011). Syftet med att mäta säkerheten utifrån något perspektiv kan möjliggöra att ett kvantitativt resultat kan erhållas där en som mäter kan urskilja var eventuella brister finns och var styrkorna finns (Gollmann, 2011). Gollmann (2011) förklarar att en mätning av säkerhet oavsett perspektiv på en särskild produkt eller fenomen kan ha sina brister vare sig den faktiskt mäter säkerheten då en obehörig part bara behöver upptäcka en brist för att äventyra säkerheten fastän det finns ett flertal olika säkerhetsåtgärder. Gollmann (2011) konkluderar

också att mätningen som utförs ska ses som kvalitativt i det avseende att en produkt eller fenomen inte kan generaliseras mot andra fenomen eller produkter.

2.6 Teoretisk sammanfattning av säkerhetsmedvetenhet

För vår studie passar det objektiva perspektivet bättre då vi vill undersöka konkreta åtgärder verksamheter har implementerat. Genom ett objektivt perspektiv kan vi se över hur medvetenheten ligger till på verksamheter och deras olika säkerhetsåtgärder för den säkerhetsproblematik som beskrivits. Desto fler säkerhetsåtgärder som finns i relation till problematiken går det att bättre fastställa hur bra säkerheten och medvetenheten är (Gollmann, 2011). Det har även uttryckts av Leavitt (2013) & Gollmann (2011) att ett flertal skyddsåtgärder är bättre än ett enstaka då fler kan minimera de eventuella brister som kan äventyra säkerheten. Dahbur m.fl (2017) förespråkar att personer, teknologi, processer och procedurer samt policyer är viktiga element som kommer avgöra säkerhetsmedvetenheten. När dessa element inte övervägs ökar risken för att slutanvändare inte följer de önskade säkerhetstillämpningarna på en verksamhet (LeVeque, 2006).
Till verksamheters medvetenhet är det av intresse att undersöka vilka säkerhetsåtgärder de instiftat som skyddar deras verksamhetsdata. Dessa åtgärder kommer efterfrågas till respektive kategori inom säkerhetsmedvetenhet.

2.6.1 Personer

Det är de anställda som använder sig ut av mobila enheter och det är deras handlingar vilka kommer antingen säkerställa eller äventyra verksamhetens data. En verksamhet som har en säkerhetsplan för de anställda och deras användning av mobila enheter kan därför vara bättre förberedda mot säkerhetsproblematiken vi beskrivit. För att arbeta säkert är det därför viktigt att verksamheter tillhandahåller träning och utbildning för deras anställda i syfte om att förbättra säkerhetsmedvetenheten om deras enheter (Dahbur, 2017). När säkerhetsmedvetenhet finns kan det påverka de anställdas beteende att implementera de olika säkerhetsåtgärder verksamheten önskar ska efterlevas, dvs om relevant medvetenhet finns (Allam m.fl, 2014). Säkerhetsplanen borde även se till att de anställda är positionerad i sin rätta roll och ansvarar för deras respektive

ansvarsområden (Dahbur, 2017). Om en anställd har tillgång till mer information än vad de behöver inom sin roll och ansvarsområde kan ett eventuellt dataintrång medföra att mer information läcker ut. Om inte de anställda har medvetenhet om säkerhet och verksamheter inte har säkerhetsmedvetenhet över de anställda kommer majoriteten av incidenter och den största andelen av skadegörelse fortsätta relatera till de anställda (Gollmann, 2011).

2.6.2 Teknologi

Att enbart kryptera nätverksanlsutningen är inte tillräckligt längre då en ny hotbild finns där enhetsfunktioner kan utnyttjas av mjukvaruprogram för att samla in information (Chang m.fl, 2014). Teknologin som används måste därför vara modern och användarvänlig för de anställda för att uppnå säkerhetsmedvetenhet (Dahbur m.fl, 2017). Inom faktorerna modern och användarvänlig behöver det därför finnas relevanta säkerhetsåtgärder som kan hantera dagens säkerhetsproblem och nyttjas på ett vis som upplevs lätthanterligt av de anställda. Finns det brister eller svagheter i teknologin kan det möjliggöra för obehöriga parter att ta över kontrollen av en enhet (Gollmann, 2011). Rekommenderade säkerhetsåtgärder för att säkerställa enheterna kan vara att använda sig av olika separationstekniker och säkerhetsmjukvara på de mobila enheterna.

För studien är det därför av intresse att undersöka hur teknologin är konfigurerad och om det finns skyddsåtgärder för säkerhetsproblematiken som beskrivits. Detta kommer reflektera verksamheternas säkerhetsmedvetenhet kring BYOD/CYOD/UWYT användning.

2.6.3 Policyer

För att uppnå verksamhetens säkerhetsmål, att i detta fall säkerställa verksamhetens data, bör det finnas tydligt definierade riktlinjer för de anställda där de får information om hur de ska förhålla sig med deras enheter (Dahbur m.fl, 2017). Detta kan öka de anställdas förståelse om olika säkerhetstillämpningar och främja benägenheten att följa de (LeVeque, 2006). Vid utformning av policyer kring mobila enheter bör de anpassa sig bl.a efter de anställdas arbetsbörda, den önskade produktivitetsnivån och vad ledningen begär av de anställda (Allam m.fl, 2014). Saknas denna balansen mellan de olika faktorerna kommer enbart standardsäkerhet implementeras vilken kan

vara bristfällig (Allam m.fl, 2014).

Många verksamheter har beskrivits sakna säkerhetspolicyer när det kommer till anställdas mobila enheter och är då sämre medvetna om ett dataintrång sker eller bryter mot organisatoriska policyer (Brodin m.fl, 2015). Det kan därför vara av intresse för studien att undersöka själva hur det ligger till kring detta. Detta borde kombineras med att se över om policyerna, om de finns, tar hänsyn till de nämnda faktorerna som återfinns i figur 1.

2.6.4 Processer och procedurer

Processer och procedurer är vad som reglerar hur teknologin ska användas av de anställda (Dahbur m.fl, 2017). En kontinuerlig bedömning behöver göras när processer ska utformas då en verksamhet ständigt behöver förbättra samt bibehålla sin säkerhetsmedvetenhet (Allam m.fl, 2014). Likt hur policyer utformas bör även processerna anpassas till vad ledningen begär, produktivitetsnivån och arbetsbördan av de anställda (Allam m.fl, 2014). Illasinnade attacker har sitt fäste när det saknas procedurer för teknologin som används av de anställda då det försämrar deras säkerhetsmedvetenhet (Dahbur m.fl, 2017). Vi ämnar därför undersöka hur verksamheter arbetar med att ta fram processer och procedurer för de anställda på de mobila enheterna. Om de anställda känner till vilka åtgärder de ska följa kan de lättare uppnå det önskvärda säkerhetsmedvetande verksamheterna önskar följas (Gollmann, 2011).

3 Metod

Studiens metoddel kommer att förklara valet av metod och dess avgränsningar som utförts inför insamlingen av det empiriska materialet. Här behandlas även de förberedelser som har format empirin genom att fastställa och förklara valet av intervjustrukturen och dess innehåll.

3.1 Metodval

Då syftet med studien är att reda ut verksamheters medvetenhet om säkerhetsriskerna med mobila enheter, och deras konkreta åtgärder, har vi valt en kvalitativ metod. Med en kvantitativ metod kunde vi ha fastställt till vilken frekvens avgörande faktorer uppträder (Eggeby & Söderberg, 1999), men vi är mer intresserade av att undersöka hur respondenterna arbetar med att tackla säkerhetsproblematiken. Hur IT-chefer och övriga IT-ansvariga arbetar med våra kategorier i den teoretiska sammanfattning går inte alltid att uttrycka kvantitativt. Då en kvalitativ metod intresserar sig för meningar, eller innebörder, snarare än för statistiskt verifierbara samband (Alvehus, 2013), upplevs den metoden bättre besvara vår forskningsfråga i relation till vad som är centralt i den teoretiska sammanfattningen.

En kvalitativ metod innebär att datainsamlingen begränsas till ett fåtal intervjupersoner där fokus ligger på att komma åt deras åsikter, känslor, erfarenheter och tankar kring ett ämne (Alvehus, 2013). Olika slags intervjuformer är tänkbara för att räknas in för en kvalitativ ansats, Alvehus (2013) berättar att det vanligaste är en direkt interaktion ansikte mot ansikte, men allt från röst- samt videobaserade intervjuer kan vara tänkbara.
Hur intervjustrukturen är upplagd kan s

3.2 Intervjustruktur

skilja sig åt beroende på vad författarna till en uppsats specifikt vill analysera (Alvehus, 2013). Vi har valt en semistrukturerad intervjuform där intervjuaren följer ett formulär som innehåller ett fåtal öppna frågor som samtalet kommer centreras kring, respondenternas möjlighet att

påverka innehållet i intervjun ökar avsevärt och det läggs press på oss som intervjuare att ställa bra följdfrågor (Alvehus, 2013). Valet av denna intervjustruktur grundar sig i att den öppnar upp möjligheter att erhålla en djupare förståelse för respondentens svar när det finns en dialog med i bilden.

Det är av betydelse att under intervjun ställa frågor som handlar om respondentens egen verklighet, innehållsmässigt kommer detta höja kvalitén på intervjun om frågorna inte är för allmänna utan mer specifika (Alvehus, 2013). Vi som intervjuar behöver vara alerta och lyssna aktivt eftersom vi kan behöva ställa lämpliga följdfrågor där respondenten får fördjupa sig eller ange ett exempel på deras svar (Alvehus, 2013). Alla intervjuer kommer att spelas in och även transkriberas, till transkriberingen kommer både intervjufrågorna samt svaren finnas med då detta kan visa varför ett visst svar förekommer (Alvehus, 2013).

3.3 Urval

Respondenterna som medverkar kommer ha valts efter vad Alvehus (2013) kallar ett "strategiskt urval" dvs att vi söker oss enbart till individer med en särskild erfarenhet, bakgrund och insyn på verksamheterna. De medverkande personerna som kommer bidra till studien, IT-chefer och övriga IT-ansvariga, är de som fattar beslut rörande säkerhetsimplementeringar för teknologin som används. Vår forskningsfråga kan bäst besvaras om datainsamlingen kommer ifrån de som ska ansvara för säkerheten för teknologin och för att de har bäst insyn vad som gäller för de anställda. IT-chefer och övriga IT-ansvariga kommer därför representera verksamhetens säkerhetsmedvetenhet efter deras svar.

Vi kommer söka oss till stora samt medelstora företag då det med stor sannolikhet kommer finnas någon som är IT-ansvarig. Med större verksamheter kan det även antas att de använder sig av blandade enhetsformer mellan BYOD/CYOD/UWYT då BYOD är det billigaste alternativet. Vi önskar inte enbart generalisera för BYOD, vilket kan vara mer vanligt på mindre verksamheter. Vi förutsätter att säkerhetsproblematiken existerar på alla enhetsformer då även om verksamheten äger enheten med CYOD och UWYT existerar fortfarande en säkerhetsrisk om

inga säkerhetsåtgärder finns mot säkerhetsproblematiken.

3.4 Transkribering

Under transkribering av de inspelade intervjuerna kommer vi till största mån försöka få med allting som sagts för att se till att den insamlade datan återspeglar verkligheten av vad som sades. Detta kommer innebära att lyssna av särskilda delar vilka kan ha brus eller för att svaren inte lät tydliga nog. Vi har valt att exkludera utfyllnadsord som exempelvis “ehh”, “öh” och “hmm” då vi tyckte att sådana ord inte betyder något och texten blir mer läsvänlig utan de.

Vi kommer i resultatdelen sammanställa de olika svaren från intervjuerna och kategorisera de baserat på den ställda intervjufrågan. Detta utförs dels för att enklare kunna se likheter och skillnader mellan respondenternas svar vilket senare kommer undersökas djupare i analysdelen. Vi kommer även utföra en sammanfattning per kategori vi undersöker för att sammanställa det centrala som har återgetts.

3.5 Undersökningskvalité

Det är av betydelse att kritiskt granska sin undersökning för att optimera sitt resultat, under en studie bör den insamlade empirin infria två elementära krav:

- **Valid:** Empirin ska vara giltig och relevant.
- **Reliabel:** Empirin ska vara tillförlitlig och trovärdig.
  (Jacobsen, 2002)

3.5.1 Validitet

Jacobsen (2002) återger att validitet är en giltighetsprövning bestående av en intern och extern giltighet. Den interna berör trovärdigheten bakom den kvalitativa ansatsen och dess datakvalité som påverkar resultatets giltighet (Jacobsen, 2002).
För att säkerställa studiens interna validitet har intervjufrågorna utformats med hjälp av en teoretisk sammanfattning vilken i sin tur grundar sig i validering med hjälp av ett flertal av

källor. Som tidigare nämnt använder vi oss av ett strategiskt urval kring respondenterna som har bidragit till studien för att ytterligare säkerställa studiens validitet av insamlad data.

Den externa giltigheten berör tillämpningen bakom den kvalitativa ansatsen och till vilken grad de olika fynden kan generaliseras i andra sammanhang (Jacobsen, 2002). Då empirin baseras på ett fåtal respondenters tankar och åsikter om just deras verklighet kan slutsatser inte göras vilka är generaliserbara för alla. Dock ser vi att problematiken är generaliserbar för de flesta större verksamheter där exempelvis en kapad inspelning om ett affärsmöte kan ha ett enormt monetärt värde. Om verksamheter därför har skydd mot sådana attacker och liknande kan de upplevas vara bättre medvetna om säkerhetsproblematiken med mobila enheter.

3.5.2 Reliabilitet

Om empirin ska eftersträva tillförlitlighet och trovärdighet som Jacobsen (2002) förespråkar, måste studien följa en noggrann struktur under datainsamlingen. Skulle studien utföras igen vid ett annat tillfälle med samma metod och få samma resultat kan studien som utförts räknas som reliabel (Jacobsen, 2002). Innebörden för oss, med reliabilitet i åtanke, blir att se över två olika faktorer som kan påverka undersökningen:

- **Intervjuareffekt:** Intervjuaren kan påverka intervjuns innehåll samt respondenterna.
- **Observatörseffekt:** Respondenten kan påverka den som intervjuar samt intervjuns innehåll.

  (Jacobsen, 2002)

Intervjuerna bör därför följa ett särskilt konsekvent intervjusystem för att minimera intervjuarens samt respondentens effekt att forma datainsamlingen på, konceptet kallas kontexteffekten (Jacobsen, 2002). Kontexteffekten berör sammanhanget bakom datainsamlingen vilket kan ha en inverkan på studiens reliabilitet (Jacobsen, 2002). För att reducera kontexteffekten på datainsamlingen kommer vi se till att alla respondenter får samma bakgrund till vad studien undersöker, samt säkerställa deras anonymitet, följdfrågorna förbehålls att enbart fokusera på

förtydligande och exemplifiering på korta svar. Dessa åtgärder kommer finnas till som ett komplement till vår redan etablerade intervjustruktur samt intervjuguide.

3.5.3 Etik

Jacobsen (2002) diskuterar etiska aspekter under datainsamlingen vilka kan ha en inverkan på tillförlitligheten med studien. Då studerade människor har en förmåga att bete sig på ett annorlunda vis än vid en normal situation kan svaren under en intervju skilja sig från verkligheten (Jacobsen, 2002). För att tackla detta problem ska respondenternas medverkan vara frivilligt där de får kännedom om studiens bakgrund och kan när som helst dra tillbaka sitt tillstånd att använda deras data (Jacobsen, 2002).

Respondenterna har fått en allmän bakgrund om studien där huvudbegreppen medvetenhet och säkerhet med mobila enheter för de anställda har nämnts. Vi har inte gått in i för mycket detalj kring studiens syfte för att motverka anpassade svar och då det kan influera studiens tillförlitlighet om respondenterna redan känner till vad studien syftar till allt för mycket (Jacobsen, 2002).

En sista aspekt som Jacobsen (2002) tar upp är att respondenterna ska bli korrekt återgivna där inga manipulationer får existera, exempelvis där det eventuellt kan stärka studien. Vi kommer av denna anledning inkludera transkriptionerna av intervjuerna som en bilaga i studien. För att ytterligare sätta press på en korrekt återgivning kommer studien skickas till respektive respondent.

Vi respekterar respondenternas privatliv och då säkerheten på en verksamhet är ett känsligt ämne ska det inte kunna gå att identifiera respondenterna eller deras verksamhet.

3.6 Intervjuguide

Inför intervjuerna sammanställdes en intervjuguide vilken grundar sig i den teoretiska sammanfattningen. Detta är gjort för att undersöka alla kategorier som har definierats som

relevanta för att kunna besvara forskningsfrågan.

#1 - Får privata mobila enheter användas av de anställda eller hur ser det ut på er verksamhet?

- Har något särskilt hänt som bestämde det valet?

Denna fråga syftar till att se över om något medvetande finns överhuvudtaget kring användningen av mobila enheter på verksamheten. Här kan vi bl.a få reda på vilken av BYOD/CYOD/UWYT som används i kombination med att höra deras motivering om valet. Om enheten kan användas på verksamheten men inte har någon säkerhetsåtgärd får den inget resultat i mätningen för verksamhetens medvetenhet (Tabell 2).

#2 a) - Får de anställda några direktiv om hur deras mobila enheter får användas?

- Vad innehåller dessa direktiv?

Här undersöker vi vare sig de anställda får någon information som kan vara till nytta för att träna de och utbilda de om att använda enheterna på ett säkert vis. Om anställda känner till vilka åtgärder som ska följas kan de enklare uppnå det önskvärda säkerhetsmedvetandet på verksamheterna.

#2b - Är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?

- Utförs några åtgärder för att motverka detta? Kan du ge några exempel?

Här kan vi studera vare sig det finns ett medvetande alls kring säkerhetsproblematiken på verksamheten tillsammans med deras eventuella säkerhetsåtgärder.

#3 - Får de anställda ansluta till alla nätverksresurser på verksamheten med deras mobila enheter?

- Finns det olika bestämmelser för olika anställda och deras respektive roller? Hur märks detta?

Här kan vi se över vare sig de anställda begränsas åtkomst beroende på deras roller och ansvarsområden.

#4 a) - Har ni några säkerhetsåtgärder på de mobila enheterna?
- Vad är det tänkt att de ska säkerställa?

Med denna fråga kan vi se över om det finns konkreta åtgärder som är till för att skydda verksamhetens data från de anställdas olika mobila enheter. Här får vi även reda på i mer detalj om det finns medvetenhet kring säkerhetsproblematiken.

#4 b) - Behöver anställda uträtta något för att säkerhetsåtgärderna ska fungera?
- Hur går de tillväga?

Här kan vi få en inblick kring hur diverse säkerhetsåtgärder är konfigurerade och om det verkar användarvänligt att använda de av de anställda.

#5 a) - Har ni några organisatoriska policyer för de anställdas mobila enheter?
- Vad innehåller de?

I denna fråga får vi reda på om verksamheter har någon form av säkerhetsmedvetande för de mobila enheterna vilket ska göra de bättre medvetna om ett dataintrång sker eller bryter mot organisatoriska policyer.

#5 b) Har ni några automatiserade eller tekniska policyer för de anställdas mobila enheter?
- Vad innehåller de?

Här kan information ges vare sig verksamheten förfogar över automatiska åtgärder som ser till

att de organisatoriska policyerna följs.

#5 c) - Vilka faktorer vägdes in när ni utformade era säkerhetspolicyer?

- Kan du exemplifiera?

Här får vi reda på om verksamheter utformar säkerhetspolicyer exempelvis i relation till den önskade produktivitetsnivån av alla parter och arbetsbördan för de anställda.

3.7 Respondenter

Tabell 1: Information om intervjuerna.

Respondent	**Antal anställda**	**Bransch**	**Position**	**Enhetstyp**	**Intervjutyp**
IP1	~1500	IT	IT-ansvarig	BYOD & CYOD	Möte
IP2	~15000	Tillverkning	IT-ansvarig	CYOD & UWYT	Möte
IP3	~3000	Utbildning	IT-ansvarig	BYOD & CYOD	Möte
IP4	~2000	IT	IT-chef	BYOD & CYOD	Möte

4 Resultat

I detta kapitel presenteras vårt empiriska material.

4.1 Teknologi

Får privata mobila enheter användas av de anställda eller hur ser det ut på er verksamhet?

IP1, IP3 och IP4 - Använder sig ut av både BYOD & CYOD på sina verksamheter.

IP2 - Använder sig ut av CYOD & UWYT, dock kan privata mobiler tas med till jobbet men de kan inte användas för att utföra något särskilt.

Har ni några säkerhetsåtgärder på de mobila enheterna?

IP1 - Nej.

IP2 - Ordnar med operativsystemet och uppdateringar för de mobila enheterna. Använder MDM: "...om de försvinner och så där ska man anmäla det så man kan slå av de…" (Kap 7.2, s46).

IP3 och IP4 - MDM men fungerar bäst för iPhones och inte hundraprocentigt för Androidenheter. MDM ska säkerställa att enheterna är konfigurerade på rätt sätt där de uppfyller vissa säkerhetskrav men också för att verksamheten ska kunna rensa enheten och slå av de om de skulle försvinna.

Behöver anställda uträtta något för att säkerhetsåtgärderna ska fungera?

IP1 - Har inga säkerhetsåtgärder.

IP2, IP3 och IP4 - Automatisk konfigurering, anställda behöver inte göra något förutom att godkänna avtal när de hämtar ut sin enhet. Försvinner enheten behöver de säga till verksamheten.

4.1.1 Sammanfattning teknologi

IP1 - Tillåter BYOD och CYOD att användas på verksamheten men saknar säkerhetsåtgärder på de mobila enheterna.

IP2 - Tillåter CYOD och UWYT att användas på verksamheten. BYOD kan inte komma åt några

verksamhetsresurser men kan ändå tas med till verksamheten. Använder MDM. Anställda behöver inte utföra något särskilt för att MDM ska funka, försvinner en enhet ska de säga till.
IP3 och IP4 - Använder BYOD och CYOD på verksamheten och som säkerhetsåtgärd har de MDM. Anställda behöver inte utföra något särskilt för att MDM ska funka, försvinner en enhet ska de säga till.

4.2 Personer

Får de anställda några direktiv om hur deras mobila enheter får användas?
IP1 - Nej.
IP2 - Ja, IT-säkerhetsinformation att det ska finnas lås, försvinner de ska man anmäla det för att kunna slå av de, att man bara har tillgång till mejlen.
IP3 -Ja, allmänna informationssäkerhetsregler ska följas som inkluderar de mobila enheterna. Dock som statlig myndighet gäller offentlighetsprincipen där all allmän information ska kunna vara tillgänglig för allmänheten på de mobila enheterna.
IP4 - Ja, man får reda på sina rättigheter och skyldigheter i form av medvetenhetsträning där man får reda på vad man får göra och inte får göra med enheterna, att man ska hålla koll på sina enheter så de inte kommer bort.

Är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?
IP1 - Nej, hoppas på det men har inga åtgärder för att motverka att det händer.
IP2 - Nej, känner till att det kan hända men har inget direkt skydd mot det problemet utan resonerar att deras säkerhetsmedvetenhetsträning för att undvika dataläckage ska vara till hjälp.
IP3 - Nej, anser att de anställda har dålig koll på säkerhet i allmänhet och att de inte blir upplysta om att säkerställa enhetsfunktionerna heller av IT-avdelningen.
IP4 - Nej, tror inte att de anställda är medvetna om det och det är inget de informerar de anställda om heller.

Får de anställda ansluta till alla nätverksresurser på verksamheten med deras mobila enheter?

IP1, IP2 och IP4 - Har begränsningar för vad de anställda kan ansluta till.

IP3 - Kan koppla upp sig till vart som helst på det trådlösa nätet och gästnätet där offentlig information kan kommas åt och måste finnas på grund av offentlighetsprincipen. Dock för administrativa system finns begränsningar där bara vissa med behörighet kan komma åt systemet.

4.2.1 Sammanfattning personer

IP1 - Inga direktiv ges för de mobila enheterna.

IP2, IP3 och IP4 - Ger ut direktiv för de mobila enheterna.

Ingen av respondenterna utför någon särskild åtgärd mot enhetsfunktionerna på de mobila enheterna eller informerar de anställda om det. Alla respondenterna har begränsningar för vad de anställda kan ansluta till, för IP3 finns det inga begränsningar för att komma åt allmän information men det finns begränsningar för åtkomst till det administrativa systemet.

4.3 Policyer

Har ni några organisatoriska policyer för de anställdas mobila enheter?

IP1 och IP4 - Har ett allmänt sekretessavtal som inkluderar mobila enheter där den anställda går med på att ingen verksamhetsinformation ska delas med någon utomstående.

IP2 - Behålla lösenord för sig själv, ej lämna ifrån sig sina enheter där den anställda inte har koll på de: “...vi säger att man handlar på vägen hem då är det till exempel fel att lämna sin datorväska och mobil i bilen.” (Kap 7.2, s47).

IP3 - Allmänt informationssäkerhetspolicy men “...ingenting explicit för telefoner.” (Kap 7.3, s50).

Har ni några automatiserade eller tekniska policyer för de anställdas mobila enheter?

IP1 - Nej.

IP2 - Konfigurering med mejlen när enheten hämtas.

IP3 - Nej.

IP4 - Flera tekniska policyer när en enhet ansluter mot verksamheten exempelvis lösenordskrav och kontroll på att enheten är patchad korrekt.

4.3.1 Sammanfattning policyer

IP1, IP2 och IP4 - Har organisatoriska policyer som gäller för mobila enheter men vaga riktlinjer där allmänna sekretessavtal ska tillgodoräkna allt.

IP2 och IP4 - Har tekniska policyer för de mobila enheterna som ser till att anslutningen är säker och patchad korrekt.

4.4 Processer och procedurer

Vilka faktorer vägdes in när ni utformade era säkerhetspolicyer?

IP1, IP2 och IP3 - Har inga specifika processer eller procedurer för de mobila enheterna.

IP4 - Följer löpande best practices där mjukvaran konfigureras därefter.

4.4.1 Sammanfattning processer och procedurer

IP4 - Följer löpande best practices där mjukvaran konfiguereras därefter. De anställda behöver utföra vissa åtaganden för att säkerhetsåtgärder ska fungera korrekt.

IP1, IP2 och IP3 - Har inga specifika processer eller procedurer för de mobila enheterna.

Tabell 2: Sammanfattat resultat på de olika kategorierna.

Verksamhetens medvetenhet	**Personer**	**Teknologi**	**Policyer**	**Processer och procedurer**
IP1	1/3	0/3	1/2	0/1
IP2	2/3	3/3	2/2	0/1
IP3	2/3	3/3	0/2	0/1
IP4	2/3	3/3	2/2	1/1

5 Analys och diskussion

Här kommer den insamlade empirin diskuteras och analyseras mot det teoretiska ramverket. Syftet med detta är att påvisa skillnader, likheter och eventuella tendenser som kan komma att uttryckas.

5.1 Personer

Dahbur m.fl (2017) anser att en god säkerhetsmedvetenhet finns när de anställda är positionerade i sina rätta roller där de inte har tillgång till mer information än de behöver och att de erhåller säkerhetsträning. Enligt alla våra respondenter finns begränsningar för vad de anställda kan ansluta till på verksamheten vilket talar för att de anställda är positionerade i sina rätta roller. 3 av 4 respondenter ger direktiv för de anställdas mobila enheter vilket tyder på att de anställda blir tränade inom säkerhet. När utbildning finns för respondenternas respektive anställda ska detta enligt LeVeque (2006) medföra att förståelsen om säkerhetstillämpningar ökar och stödja att de följs. Allam m.fl (2014) menar att när fokuset kring säkerhet läggs på individen och inte enheten som ska skyddas ska säkerhetsrisken bland annat minska då individens beteende influeras där det ska påverka vad de gör så det gynnar säkerheten.
Ingen av respondenterna har visat tecken på att de utbildar de anställda om att enhetsfunktioner kan samla in verksamhetsinformation. Detta kan innebära negativa följder för verksamheterna då som tidigare nämnt av Gollmann (2011) är det de anställda som står för majoriteten av incidenter och den största andelen av skadegörelse. När de anställda inte har några förhållningsregler med deras enhetsfunktioner på deras mobila enheter kommer det enligt Dahbur m.fl (2017) innebära att säkerhetsmedvetenheten blir obefintlig och att säkerhetsriskerna ökar för detta.

IP2 talar om att de inte arbetar specifikt mot att säkra enhetsfunktioner men mot samma mål det vill säga att dataläckage inte ska ske. Av respondenternas svar, verkar de alla i allmänhet jobba mot dataläckage men att detta ska ske via metoder som att sätta lås på enheterna, hålla koll på de och att anmäla om de försvinner. Respondenterna tycks fokusera för de anställda att säkerställa den fysiska säkerheten med enheterna, att säkerställa mot hotet av att enheterna blir stulna eller nyttjas fysiskt av en obehörig person. Säkerhetsproblematiken i studien hade för de anställda

bättre tacklats om de fick direktiv om att begränsa applikationernas tillåtelse att använda enhetsfunktioner. Risken med att ge ut för många tidskrävande direktiv kan enligt Allam m.fl (2014) innebära att bara traditionell säkerhet appliceras samt enligt LeVeque (2006) blir svårare att övervinna motståndet från slutanvändare. I nuläget tycks det inte finnas för många tidskrävande direktiv då 'traditionell säkerhet' appliceras och vi ser utrymme för fler direktiv för de anställda då de representerar den största hotbilden för en verksamhet.

5.2 Teknologi

För att sträva efter säkerhetsmedvetenhet på en verksamhet förespråkas att teknologin bör vara modern samt användarvänlig för de anställda (Dahbur m.fl, 2017). MDM beskrivs enligt Chang m.fl (2014) bland annat som ett verktyg där en verksamhet kan säkerställa att säkerhetspolicyer följs på enheterna. Detta syfte stämmer överens för IP4 där de kan kontrollera patchningen, om enheterna är root kitade och konfigureringen i allmänhet om enheten uppfyller verksamhetens säkerhetspolicyer. Ett annat syfte enligt Chang m.fl (2014) samt Leavitt (2013) är möjlighet för verksamheten, att vid upptäckt om förlust eller obehörig användning, radera innehållet och slå av enheterna. 3 av 4 respondenter använder MDM på sina verksamheter där de alla uppger att möjligheten till att slå av och radera innehållet på enheter är syftet till att de använder verktyget. Av respondenterna får vi reda på att MDM inte fungerar hundraprocentigt för alla typer enheterna, där iPhone är bäst anpassad men att Android antingen inte är kompatibel eller som för IP3 uppger att MDM kommer på köpet enbart för iPhone. Av detta förstår vi att MDM inte är aktivt eller fungerar på alla enheter men att på enheterna där MDM funkar är det bara de som får lov att ansluta till verksamhetens nätverksresurser. Detta då VPN-access bara tillåts om MDM uppger att säkerhetspolicyerna verksamheten har är uppfyllda som för IP4.
För att MDM ska fungera behöver inte de anställda utföra något utan respondenterna har uppgett att om enheter skulle försvinna så behöver de anställda säga till, inget annat. Säkerhetsåtgärden upplevs därför vara användarvänlig efter vad Dahbur (2017) förespråkade i den grad att den inte är tidskrävande utan finns i bakgrunden utan att den märks av.

Säkerhetsåtgärden MDM kan skydda, som för kategorin personer, det fysiska kring enheten som

skyddar mot förlust eller missbruk där innehållet kan raderas och enheten slås av. MDM skyddar även kring tekniska konfigureringar på enheten vilket motverkar att osäkra anslutningar kan göras. Detta ser vi som positivt i relation till säkerhetsproblematiken då desto fler begränsningar som finns på enheterna kan det minska risken för dataintrång. Det vi saknar dock från respondenterna är teknologiska säkerhetsåtgärder vilka ska skapa begränsningar för mjukvarubeteendet på enheterna. Likt Leavitt (2013) som förespråkar användningen av MAM kan verksamheterna införa policyer rörande applikationernas tillåtelse att använda sig ut av enhetsfunktioner och MAM som säkerställer att policyerna följs.

Att använda sig ut av både MDM och MAM hade varit att föredra för att ytterligare skydda sig mot dataintrång. I nuläget med MDM är verksamheterna reaktiva och skulle MAM varit i bruk skulle de även vara proaktiva.

5.3 Policyer

Policyer eller riktlinjer för de anställdas enheter är viktigt att finnas då de kan hjälpa till att säkerställa att verksamhetens säkerhetsmål uppnås, dvs att skydda verksamhetens data (Dahbur m.fl, 2017). Likt vad Brodin m.fl (2015) har uttryckt och utifrån respondenternas svar saknas det specifika säkerhetspolicyer när det kommer till de anställdas mobila enheter. Utifrån respondenternas svar rör det sig mer om allmänna sekretessavtal där de mobila enheterna tillgodoräknas och policyer som ska skydda de från fysiska hot, exempelvis IP2 som begär av de anställda att inte lämna ifrån sig enheterna när de ska gå och handla. Dessa riktlinjer upplevs som Allam m.fl (2014) uttryckt tidigare som ‘traditionell säkerhet’ när det saknas påtryckningar från ledningen att säkra de mobila enheterna efter moderna hotbilder där stöld av verksamhetsdata inte bara sker fysiskt men också via mjukvara. När anställda saknar riktlinjer minskar det chansen för dem att konfigurera enheterna på ett mer säkert vis eftersom ingen kräver det av de (LeVeque, 2006).

Vi saknar policyer vilka enligt Dahbur m.fl (2017) bör vara tydligt definierade för de mobila enheterna och där de även innehåller ledningsstöd för att säkerställa att policyerna efterföljs.

Automatiska policyer kan förvisso säkerställa att organisatoriska policyer efterföljs men i nuläget säkerställer de för 2 av 4 respondenter att säker anslutning till verksamheten finns och lösenordskrav. Om anställda förstod betydelsen av att begränsa applikationernas behörighet till olika enhetsfunktioner skulle säkerhetsriskerna på verksamheten minska avsevärt, men detta skulle bara kunna ske om ledningen inkluderade det i deras medvetenhetsträning.

5.4 Processer och procedurer

Processer och procedurer är vad som reglerar hur teknologin ska användas av de anställda (Dahbur m.fl, 2017). Av alla respondenter är det bara IP4 vilka utformar deras policyer och mjukvara löpande utifrån best-practices som enligt Dahbur m.fl (2017) kommer främja processernas effektivitet. IP4 nämner också avsaknaden av tillverkare vilka rekommenderar automatiska inställningar för enheter och just detta skulle kunna vara intressant för studien. Detta relaterar till att hur verksamheter utarbetar deras processer rekommenderas att en kontinuerlig bedömning görs i syfte att ständigt förbättra samt bibehålla sin säkerhetsmedvetenhet (Allam m.fl, 2014). Om best-practices inkluderade automatiska inställningar för de mobila enheterna kunde eventuellt andra säkerhetsåtgärder än MDM finnas till på enheterna. Med den nuvarande proceduren för verksamheten ser vi bara att de bibehåller och förbättrar sin befintliga säkerhetsmedvetenhet kring den fysiska säkerheten samt säkra anslutningar till nätverksresurser.

6. Slutsats

Vår forskningsfråga var:

- Hur medvetna är IT-chefer och övriga IT-ansvariga om säkerhetsproblematiken med BYOD/CYOD/UWYT?

Den empiriska undersökningen tyder på att IT-chefer och övriga IT-ansvariga är väl medvetna om att BYOD/CYOD/UWYT innebär risker mot verksamheten. Riskerna bemöts genom att begränsa åtkomst till känsliga nätverksresurser från mobila enheter. De anställda begränsas också baserat på deras ansvarsområden där åtkomst ges enbart efter behov gentemot deras arbetsuppgifter.
Som teknisk säkerhetsåtgärd instiftar de flesta av respondenterna MDM vilket är till för att skydda mot fysiska omständigheter mot enheterna samt för säkra anslutningar mot verksamheten. Övriga säkerhetspolicyer som fanns var mot dataläckage i form av att de anställda skulle även här tänka på sin fysiska omgivning i form av att bland annat applicera lösenord på enheterna och att hålla koll på de samt anmäla om de försvinner. Vi upptäckte att de anställda behövde knappt lägga någon tid alls på att säkerställa deras enheter då inga övriga direktiv gavs som kunde involvera hur enheterna ska användas på ett säkert vis, det vill säga den interna säkerheten. Den interna säkerheten tycks enbart läggas på verksamhetens axlar och som tidigare nämnt följer ingen av respondenterna best-practice metoder för automatisk alternativt manuell konfigurering på de mobila enheterna som kan stödja just den interna säkerheten. Som tidigare nämnt av Leavitt (2013) går det ej att förlita säkerheten helt till en enstaka åtgärd då de alltid innehåller individuella brister. Därför är flera säkerhetsåtgärder bättre än en enstaka.

Det har framkommit att IT-chefer och övriga IT-ansvariga verkar känna till problematiken att enhetsfunktioner kan komma åt verksamhetsinformation. Trots kännedom om att problemet existerar tycks inga åtgärder finnas för att motverka att det sker varken tekniskt eller via direktiv för de anställda.

6.1 Förslag till fortsatt forskning

Som slutsatsen uppgett ligger fokus kring den externa säkerheten samt säkra anslutningar enligt de ansvariga på IT-avdelningarna. Vi skulle därför föreslå att för att komplettera denna studien kan man forska om varför IT-avdelningar inte prioriterar att säkra den interna säkerheten för de anställda. Detta i samband med att det är de anställda som orsakar mest skada statistiskt på verksamheterna och att alla hotbilder som involverar just de anställda bör ses över.

7. Transkribering

7.1 Intervju 1 - IP1

M = Marcus , X = IP1

M: Får privata mobila enheter användas av de anställda eller hur ser det ut på verksamheten?
X: Ja, det är inga problem att använda sin privata enhet på jobbet.
M: Får anställda någon enhet från verksamheten?
X: Ja utlånad, de brukar få välja mellan 3 olika modeller från 3 olika företag.
M: Ok, så det är lite blandat mellan privat och…?
X: Precis.
M: Får de anställda några direktiv om hur deras mobila enheter får användas?
X: Nej.
M: Ingenting?
X: Nej.
M: Ok, är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?
X: Ja den kan samla in, asså verksamhetsrelaterad information, ja visst.
M: Jag tänkte i och med att man kan blanda den personliga miljön med verksamhetsmiljön…
X: Du menar att personliga mobiler ska samla in verksamhetsinformation också?

M: Eftersom en anställd kan blanda den personliga miljön med verksamhetsmiljön med tillåtelse av...

X: Ja, jag hoppas det iallafall.

M: Utförs några åtgärder för att motverka detta?

X: Nej inget specifikt.

M: Får de anställda ansluta till alla nätverksresurser på verksamheten med deras mobila enheter?

X: Det jag kan säga är att man behöver en proxy för att komma ut från det interna nätet, och den här proxyn gör också att man inte kan komma åt några interna resurser hemifrån utan att använda då SSH för att tunnla in. Man kan till exempel inte komma åt sin mejl hemifrån utan då måste man använda sin jobbmobil för att tunnla in helt enkelt till det interna nätet.

M: Ok, finns det olika bestämmelser för olika anställda asså beroende på deras roller?

X: Det är beroende av behovet för en anställd vad de behöver för sina arbetsuppgifter, så det är uppdelat vad man kan komma åt.

M: Ok, sen kan jag nämnt detta tidigare men finns det några säkerhetsåtgärder på de mobila enheterna som används i tjänsten?

X: Nej, inget särskilt.

M: Och eftersom ni inte har det ska jag inte ställa den följdfrågan. Men finns det några organisatoriska policyer för de anställdas mobila enheter?

X: Asså när anställda hämtar ut mobila enheter ges ingen direkt information vad mobilen ska användas till eller inte användas till utan det är rätt självklart, sen finns det ju allmänna sekretessavtal som inkluderar mobila enheter där anställda skriver under och är med på att ingen företagsinformation ska delas med någon utomstående.

M: Ok, har ni några automatiserade eller tekniska policyer för de anställdas mobila enheter?

X: Nej det skulle jag inte påstå i nuläget.

7.2 Intervju 2 - IP2

M = Marcus , X = IP2

M: Får privata mobila enheter användas av de anställda eller hur ser det ut på er verksamhet?

X: Asså privata mobiler får du ju använda men du kopplar ju de inte till någonting som bolaget har.

M: Ok, så hur får de användas?

X: Det är klart att de anställda får ha sina mobiler men de använder de privat i så fall.

M: Ok så man kan ha med sig sin mobil till jobbet men man kan inte använda de till något jobbrelaterat?

X: Nej för att typ mejl och allt sånt läggs in bara på din mobil, kan hända ibland att vissa har det speciellt.

M: Ok, hur blir det då, ges enheter ut av verksamheten?

X: Ja.

M: Ok, får man välja eller är det bestämt?

X: Från början fick man välja antingen iphone eller android, men nu senast har det bara varit iphone som gäller som nyanställd för den synkade bäst med kunder.

M: Får de anställda några direktiv om hur deras mobila enheter får användas?

X: Ja.

M: Och vad innehåller dessa direktiv?

X: Asså det är mer allmänt om IT-säkerhet att man ska ha lås på de och tänka på att om de försvinner och så där ska man anmäla det så man kan slå av de och så vidare, så det är lite mer så sunt förnuft direktiv. Man har tillgång till mejlen i mobilen men inte till hela intranätet, det har man inte. Så att det är lite begränsat vad man kan göra också med de mobila enheterna.

M: Ok, är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?

X: Jaja man har ju samma virus- och trojanproblem sen har ju jag till exempel inte jättemånga appar men det kanske går att leta sig in ändå.

M: Ok, utförs några åtgärder för att motverka detta?

X: Vi arbetar kanske inte direkt mot enhetsfunktioner men just detta med dataläckage kan jag säga att vi jobbar med att ta fram utbildningar för de anställda där de får ta del av information så som att låsa datorn, tänka på att informationsläckage kan ske för att någon tittat på din skärm på

flyget och så vidare, sen är det ju det här med social engineering det här med att det kommer in någon på kontoret du inte känner igen, men det är ju inte direkt riktat mot mobila enheter utan det är mer allmän säkerhetsinformation vi ger ut.

M: Ok, får de anställda ansluta till alla nätverksresurser på verksamheten med deras mobila enheter?

X: Nej, nu har vi bara mejl, så man har inte fler tjänster, trycker jag på en länk som går till ett dokument i intranätet så kommer inte den öppnas.

M: Ok, finns det olika bestämmelser för olika anställda?

X: Asså vi är ju så stora så jag kan inte svara definitivt så det är möjligt men jag kan säga att för majoriteten är det begränsat.

M: Har ni några säkerhetsåtgärder på de mobila enheterna?

X: Inte mer än att vi sätter upp operativsystem och uppdateringar och allt som behöver ställas in.

M: Ok, behöver man göra något för att detta ska fungera eller hur ser det ut?

X: Nä det, man beställer sin telefon och sen hämtar man den och sen gör vi inställningar för att koppla på mejlen och så har man sin telefon.

M: Ok så det är automatiskt?

X: Ja.

M: Finns det några organisatoriska policyer för de anställdas mobila enheter?

X: Asså man ska behålla sina lösenord för sig själv, man ska inte dela ut det ens för familjemedlemmar, det är ju deras mobil, så man är ju ansvarig för det man gör.

M: Ok…

X: Sen har vi ju såna regulations att man inte får lämna ifrån sig sin enhet till exempel sin dator eller mobil i bilen. Asså vi säger att man handlar på vägen hem då är det till exempel fel att lämna sin datorväska och mobil i bilen.

M: Ok, du kan ha svarat på detta innan men finns det några automatiserade eller tekniska policyer för de anställdas mobila enheter?

X: Nä inte mer än den inställningen med mejlen när man hämtar ut sin enhet.

7.3 Intervju 3 - IP3

M = Marcus , X = IP3

M: Får privata mobila enheter användas av de anställda eller hur ser det ut på er verksamhet?
X: Allt går bra.
M: Får de anställda någon verksamhetsenhet från er?
X: Får de en verksamhets…
M: Asså får de någon enhet från verksamheten?
X: Jaha, inte alla men har man behov av det så får man.
M: Ok, är det bestämt vilken enhet man ska ha eller får man välja?
X: Som statlig myndighet har man ju upphandlingsavtal och upphandlingsavtalen måste följas, och där finns en bra mängd alltså av de vanliga telefonerna finns där. Men vill du ha en speciell sån där One Plus eller Nexus eller nåt sånt där så vet jag att de inte finns på avtalen för att jag själv ska byta telefon så de finns inte. Så vi har inte alla men det är Samsung, det är Lenovos, Iphone.
M: Och där kan man välja mellan de?
X: Där kan man själv välja ja, det är upp till dig och din chef hur mycket du ska, A om du ska ha ett mobilabonnemang och B hur mycket pengar du får lägga. Sen kommer det ju inte hindra folk på universitetet att gå runt avtalen. Säga att jag inte bryr mig inte ett dugg om det här jag har egna pengar till mitt forskningsprojekt, jag vill hellre ha en, sätta in vilket märke som helst och köper jag det. Vilket gör att universitetet får lite klagomål från riksrevisionen då och då för att vi handlar utanför avtalen och det har vi precis fått ett sånt. Vi handlar en hel del faktiskt som ligger utanför avtalen, men så det kan säkert göra för mobiltelefoner också.
M: Ok, får de anställda några direktiv om hur deras mobila enheter får användas?
X: Nej.
M: OK.
X: Asså det finns ju ett regelverk asså dels för att få köpa de och dels hur du får använda IT på

universitetet där det finns informationssäkerhetsregler och det gäller ju även de mobila enheter, laptopar, plattor eller telefoner blir ju jämställt ur en informationssäkerhetssynpunkt. Vi har offentlighets och sekretesslagen som säger att du får inte ha information liggande bara på till exempel en telefon för att inte Universitetet som helhet kan nå den. För all information på en statlig myndighet omfattas av offentlighetsprincipen, därför får du inte gömma information som vi inte kan komma åt. Så du får gärna ha den på din telefon men det får inte vara det som endast finns, likadant för en platta eller laptop eller om du lägger det i molnet så måste vi kunna komma åt den.

M: Ok, är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?

X: Jag skulle säga att det är nog ganska, universitetet här har rent allmänt dålig förståelse för informationssäkerhet asså de har dålig förståelse för hur information behandlas rent allmänt. Och när vi pratar telefoner så ju länge bort det kommer från en server där folk förstår här är information som ligger på en server och det är liksom databaserad information, ju längre ut du kommer från det när du kommer ner telefonens så tänker inte folk på att det här är faktiskt också en dator som innehåller information. Det gör de inte och det är inte så att vi på något sätt upplyser de om det explicit, det har upplysts när vi fick de nya reglerna och då går man i princip uppifrån och ner, då går man och säger till prefekterna att det finns nya informationssäkerhetsregler och det är alltid prefekterna ansvar att se till att hans anställda känner till de sakerna de ska känna till. Det är ett problem eftersom prefekten får allt skit på universitet, säger man att det är prefektens ansvar och hänvisar att det är prefektens ansvar. Och prefekten kan inte, för det är ofta en duktig forskare som råkar bli prefekt av en eller annan orsak men som inte är världens bästa just på att styra verksamhet och vara administratör. Så att vi har då massa folk här som är duktiga forskare som inte får mycket tid till forskning och som är dåliga på att vara administratörer eftersom de har hamnat på prefektsidan.

M: Ok, får de anställda ansluta till alla nätverksresurser med deras mobila enheter?

X: Asså vi har ju ett stort gemensamt trådlöst nät och det är XXXXX sen förutom det så finns det några små och det är XXXXX som är gästnätet och de får koppla upp sig varsomhelst.

M: Ok, kan det finns några olika bestämmelser beroende på anställd och deras respektive roller?

X: Inte när det gäller telefoner som så, systemmässigt så är det ju som vanligt liksom om du loggar post på vi säger XXXXX eller XXXXX såna här administrativa system så finns där en kontroll på vem du är och vad du får lov att göra men ingenting som ligger i nätet. Asså vi har inte nätinloggning eller så där som kan styra dig på olika typer av rättigheter och tillgång till resurser det har vi inte.

M: Ok, finns det några säkerhetsåtgärder på de mobila enheterna?

X: Ja, på iPhone sidan har vi möjlighet att gå in och stänga ner men inte på Android.

M: OK, vad är det tänkt att den då säkerhetsåtgärden på iPhone ska säkerhetsställa?

X: Asså det är egentligen så att vi får med det på köpet så att säga, och vad vi kan göra i princip så är det bara att om den försvinner eller blir stulen så kan den brytas och raderas. Det är mest inte så mycket tankar iallafall vart så mycket att informationssäkerhetsmässigt att vi ska se till att universitetets hemliga information inte läcker ut för att vi har som sagt offentlighetsprinciper så det är inte så mycket som är hemligt. Vi kan ganska lätt berätta vad som är hemligt på ett universitet och allting annat är ju offentligt. Då kan du ju bara komma och berätta för en registrator att du vill ta del av den och den informationen om den råkar ligga på en telefon ja då får du ta fram det.

M: Behöver en anställd uträtta något för att den säkerhetsåtgärden ska fungera?

X: Han får ju säga till att min telefon är stulen, jag har blivit av med den, så det är inte han själv som gör någonting utan det sköts här.

M: Ok, så den finns på mobilen redan.

X: Ja på det kontot som de får liksom. Så länge de gör uppköp och inte köper upp en telefon på stan och handlar en egen telefon för de råkar ha lite pengar. Så att om du följer lagen, upphandlingslagen, och köper via de avtal vi har så är det Telias, vi har Telia på alla då är det så att vi kan koppla de till växeln, så den här kan ringa gratis hela Sverige så länge jag ringer till universitet för den är kopplad till vår växel oavsett var jag finns i landet. Så att så länge man har de här Telia abonnemang har vi också möjlighet att radera iPhones.

M: Ok, har ni några organisatoriska policyer för de anställdas mobila enheter?

X: Inte specifikt, asså den policyn vi har är asså informationssäkerhetspolicyn sen så finns det inte mycket mer, ingenting explicit för telefoner.

M: Ok, har ni några automatiserade eller tekniska policyer för de anställdas mobila enheter?
X: Nej.

7.4 Intervju 4 - IP4

M = Marcus , X = IP4

M: Får privata mobila enheter användas av de anställda eller hur ser det ut på er verksamhet?
X: Jo det får de lov att göra, absolut men de får inte komma åt produktionsnät så vi är ganska hårt segmenterade. Det enda man får ha på en privat telefon är egentligen mejlen och då är det ju, när man slår på mejlen så får man ett gäng förhållningsregler som man måste gå på som ger oss rätten att remote wipea telefonen, man måste ha pinkod som är tillräckligt komplext och så, och det kommer nog också ganska snart att försvinna även mejlen eftersom det är så enkelt att root kita vissa android. Men än så länge är det så framförallt att vi inte från Sverige äger allas mobiltelefoner utan ute i världen framförallt på amerikanska sidan så har man privata mobiltelefoner även i jobbet och de kan vi inte av olika skäl managera hur vi vill utan att användaren ger ok.
M: Asså utan att användaren…?
X: Att användaren i sig ger ok på att vi tar över kontrollen på deras privata telefoner. Men bara mejlen som sagt och inte på produktionsnäten då.
M: Får de anställda enheter från verksamheten?
X: Ja i många länder får man det, i Sverige får ju alla enheter, de kommer i och för sig inte heller in på näten men man kan få i Sverige VPN-access om man har behov av det men där har du också lite hårdare kontroll på enheter.
M: Du kan ha nämnt det redan, men får de anställda några direktiv om hur deras mobila enheter får användas?
X: Ja fast vi har ju nätverkssäkerhet också så vi vet ju att de inte kommer in på näten.
M: Ok, vad innehåller dessa direktiv?
X: Asså allt man gör egentligen när man får sitt konto eller sin mobiltelefon eller vad som helst

så får man att man har dels rättigheter och dels skyldigheter, förhållningsregler gällande mobiltelefonen är ju mer awareness training liknande, du får inte göra detta du får inte göra det här, du ska hålla koll på din telefon, du ska tänka på de här olika sakerna, inte så mycket mer än så.

M: Är era anställda införstådda att enhetsfunktioner på de mobila enheterna kan samla in verksamhetsrelaterad information?

X: Det tror jag inte att de är, några är det såklart men det är inget vi informerar om.

M: Ok, får, ja du har också nämnt detta, men får de anställda ansluta till alla nätverksresurser på verksamheten med deras mobila enheter?

X: Nä, absolut inte. Asså man kommer ju inte, det är ju ett skalskydd, vi har ju flera olika lager liksom, man kommer ju till gästnätet och via gästnätet kommer man sen åt en del publika webbtjänster framförallt då, några av de kommer man inte åt utanför XXXXX men de allra flesta är ju publika tjänster. Och det som är, det som skulle anses känsligt där är väl just mejlen och kanske någon proxytjänst till några applikationer.

M: Ok, har ni några säkerhetsåtgärder på de mobila enheterna?

X: Vi har Mobile Device Management som vi använder men tyvärr är det nog ändå så att tack vare, vi kan ju kolla om enheter är root kitade och så där men Android finns ju i så pass många versioner och så pass många avarter så det är inte alltid skyddet är hundraprocentigt ändå, så vi litar inte fullt ut på Mobile Device Management mjukvaran.

M: Ok, vad är det tänkt att den ska säkerställa?

X: Asså det första vi på IT vill kolla det är ju root kit, säkerhetspatcha, det senaste var ju blåtand till exempel, vi har kontroll på att alla enheter är patchade mot det, vi har en VPN klient som man kan installera på sin mobiltelefon om man får tillåtelse till det. Då har den en host-check där vi säkerställer att vissa saker är konfigurerade på rätt sätt och så där annars kan man inte ansluta. I övrigt så används Device Management bara till att se till att appar och så där är uppdaterade.

M: Behöver anställda uträtta något för att de säkerhetsåtgärderna ska fungera?

X: Nej asså det behöver man inte göra, man behöver ju godkänna avtal och så där på vissa telefoner vilket vi inte kan göra automatiskt, så rent faktiskt så kan man låta bli att patcha sin telefon, men då kommer man inte heller in på nätet om man har VPN-access.

M: Ok, har ni några organisatoriska policyer för de anställdas mobila enheter?

X: Ja asså man får ju ett dokument att skriva under när man får sin telefon utöver det så har vi inte det idag. Vi håller på att aligna våra säkerhetsrutiner till ISO 27001.

M: Vad sa du ISO?

X: 27001, som informationssäkerhetsstandard då. Men viktigast för oss är ju inte mobiltelefonerna eftersom de har så begränsad access.

M: Vad innehåller det dokumentet man skriver på?

X: Ja det är ju de här förhållningsreglerna vad man får inte får göra på telefonen, VPN om man får VPN-access så är processen lite mer rigorös då behöver man i och för sig inte skriva på ett papper men då får man, då blir man kontaktad och får förhållningsregler, de är ju i och för sig personliga idag, det är någon som berättar, så jag kan inte säga att det är på ett visst sätt liksom. Men där är det ju så att det är ganska känsligt och hade IT fått bestämma så hade ju vi inte släppt in några mobiltelefoner alls på nätverken, kanske iPhone hade funkat men Android hade vi inte, såfall bara vissa specifika versioner.

M: Ok, har ni några automatiserade eller tekniska policyer på de anställdas mobila enheter?

X: Ja absolut, till exempel om du ansluter webbmejlen så blir du direkt promptad att vi kan remote wipea, vi ställer krav på lösenord och så där som du måste acceptera, har du VPN-klienten ställer vi krav i form ut av en host checker som din mobil måste vara patchad enligt reglerna i Mobile Device Management, så det ändras ju kontinuerligt, så tekniska begränsningar finns det absolut.

M: Till den sista då, fanns det några särskild faktorer som vägdes in när de säkerhetspolicyerna formades i relation till de mobila enheterna?

X: Asså vi följer löpande best practices, vi prenumerationstjänstar där vi konfigurerar mjukvaran därefter. Så egentligen kan man väl säga att Mobile Device Management som man traditionellt använder använder inte vi till det utan det är VPN koncentratorns host check. Det där är ju ett ständigt bevakande, så ingen mer struktur så, än så länge så har vi inte hittat några tillverkare som faktiskt rekommenderar bra inställningar automatiskt heller utan där är vi reaktiva.

8. Referenser

Alberts, C. and Dorofee, A. (2003): Managing Information Security Risks. Pearson Education, Boston, 2003

Allam, S.; Flowerday, S.V.; Flowerday, E.. (2014): Smartphone information security awareness: A victim of operational pressures. Computers and Security, May 2014, 42:55-65 Language: English. DOI: 10.1016/j.cose.2014.01.005

Alvehus, J. (2013). Skriva uppsats med kvalitativ metod : en handbok. Liber. Upplaga 1.

App Store (2017): Wikipedia. *App Store (iOS)* [Elektronisk], Tillgänglig: https://en.wikipedia.org/wiki/App_Store_(iOS) [2017-09-05]

Arlitsch, K. & Edelman, A. (2014): Staying Safe: Cyber Security for People and Organizations *Journal of Library Administration.* Jan2014, Vol. 54 Issue 1, p46-56. 11p. DOI: 10.1080/01930826.2014.893116.

BlackBerry (2017): The World's Most Secure Android Smartphones [Elektronisk], Tillgänglig: https://global.blackberry.com/en/smartphones/dtek50-60-by-blackberry/overview [2017-09-08]

Brodin, M (2016): BYOD vs. CYOD: What is the difference?, 9th IADIS International Conference Information Systems 2016

Brodin, M., Rose, J. & Åhlfeldt, R.-M., 2015. Management issues for Bring Your Own Device. , 2015, pp.1–12.

Brown, H. (2016): After the data breach: Managing the crisis and mitigating the impact. Journal of Business Continuity & Emergency Planning. Summer2016, Vol. 9 Issue 4, p317-328. 12p.

Business Insider (2017): BlackBerry's share of the global smartphone market is now officially 0% [Elektronisk], Tillgänglig: http://nordic.businessinsider.com/blackberry-smartphone-marketshare-zero-percent-gartner-q4-2016-2017-2?r=UK&IR=T [2017-09-08]

Chang, J.M; Ho, P.C; Chang, T.C. (2014): Securing BYOD. IT Professional, Sep2014, Vol. 16 Issue 5, p9-11, 3p. Publisher: IEEE.

Dahbur, K; Bashabsheh, Z; Bashabsheh, D. (2017): Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review.* 2017, Vol. 13 Issue 1, p37-58. 22p.

Dhingra, M (2016): Legal Issues in Secure Implementation of Bring Your Own Device (BYOD), Procedia Computer Science 78 (2016) 179 – 184

Eggeby, E. Söderberg, J. (1999). Kvantitativa metoder. Studentlitteratur. Upplaga 1

Forbes (2015): The Top 5 Data Breach Vulnerabilities. [Elektronisk], Tillgänglig: https://www.forbes.com/sites/ericbasu/2015/11/05/the-top-5-data-breach-vulnerabilities/#6f470b754d04 [2017-10-19]

Gollmann, D. (2011): Computer Security. 3rd ed. Wiley. ISBN 978-0-470-74115-3, 460 p.

Google Play (2017): Wikipedia. *Google Play* [Elektronisk], Tillgänglig: https://en.wikipedia.org/wiki/Google_Play [2017-09-05]

IEEE (1998): IEEE Recommended Practice for Software Requirements Specifications, IEEE Std, 830-1998

Koceski S och Koceska N (2011): Interaction Between Players of Mobile Phone Game with Augmented Reality (AR) Interface, User Science and Engineering (i-USEr), 2011 International Conference on, 245-250

Leavitt, N. (2013): Today's Mobile Security Requires a New Approach. Computer (00189162). Nov2013, Vol. 46 Issue 11, p16-19. 4p. DOI: 10.1109/MC.2013.400.

LeVeque, V. (2006): Information Security – A Strategic Approach. Wiley-IEEE Computer Society Press. ISBN 0471736120, 290 p.

Lin J, Amini S, Hong J, Sadeh N, Lindqvist J, och Zhang J. (2012): Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp'12). 501–510.

Lin J, Liu B, Sadeh N, och Hong J. (2014): Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In Proceedings of the 2014 Symposium On Usable Privacy and Security (SOUPS'14).

Lyne J (Sophos) (2011): Mobile device security – what's coming next? [Elektronisk], Tillgänglig: https://www.sophos.com/es-es/medialibrary/PDFs/other/Mobile%20device%20security%20%20whats%20coming%20next.pdf [2017-09-08]

New Scientist (2010): Geo-tags reveal celeb secrets [Elektronisk], Tillgänglig: https://www.newscientist.com/article/dn19160-geo-tags-reveal-celeb-secrets/ [2017-09-05]

Ordbok 1: Security measures [Elektronisk], Tillgänglig: http://www.thefreedictionary.com/security+measures [2017-10-01]

Ordbok 2: Dictionary of Computer and Internet Terms. Barron's Business Guides (8 ed.). Hauppauge, New York: Barron's Educational Series. 2003. p. 171.

PC Magazine (2011): Inventor of the Cell Phone Says No to AT&T-Mobile, Yes to Apps, and More [Elektronisk], Tillgänglig: https://www.pcmag.com/article2/0,2817,2383578,00.asp [2017-08-25]

PCWorld (2012): A brief history of GPS [Elektronisk], Tillgänglig: http://www.pcworld.com/article/2000276/a-brief-history-of-gps.html [2017-08-26]

TechPro (2015): Research: 74 percent using or adopting BYOD [Elektronisk], Tillgänglig: http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/ [2017-09-17]

Wang H, Li Y, Guo Y, Agarwal Y och Hong J (2017): Understanding the Purpose of Permission Use in Mobile Apps, ACM Trans. Inf. Syst. 35, 4, Article 43 (July 2017), 40 pages.