BRING YOUR OWN DEVICE

– VAL AV TEKNISK LÖSNING FÖR BYOD

Kandidatuppsats i Informatik

Jonas Ahlberg
Madelen Lundqvist

2013KANI11

HÖGSKOLAN I BORÅS
INSTITUTIONEN HANDELS- OCH IT-HÖGSKOLAN

Svensk titel:	Bring Your Own Device – Val av teknisk lösning för BYOD
Engelsk titel:	Bring Your Own Device – The choice of technical BYOD solution
Utgivningsår:	2013
Författare:	Jonas Ahlberg Madelen Lundqvist
Handledare:	Patrik Hedberg

Abstract

The advanced technological devices is constantly growing in numbers, people are becoming more dependent on having them close at hand to perform various tasks. Those devices are mainly smart phones and tablets. Now that we have access to the latest and most advanced devices on the customer market we begin to use them to perform workrelated tasks more often and this is where the concept and Bring Your Own Device (BYOD) is emerging. Companies see the demand from their employees who want to work from their own devices and they try to meet the need. However, the securityrisks increases when corporate data is downloaded to the employee's private device and walk with them out of the office. Viruses also can follow the private drive into the corporate network and cause damage. It's important for companies to protect their data while the employee still is allowed to work from it's own device. This can be solved by technology and policies, which have high requirements on the security level of the technology. The issue addressed in this paper describes how a technical solution can be chosen to meet the company's main needs and also make users happy. A qualitative study was conducted using a case study at a company. The aim is to identify criterias that the company and the user have, and use these to evaluate technical solutions. This makes it easier to understand what's on the market right now and how they relate to the criterias. In the analysis criterias are identified and an evaluation of how well each technology handles the selected criteria is made. The conclusion is that the company needs to evaluate the importance of the identified evaluation criterias is for them and based on that choose a technical solution that suites the company.

Keywords: BYOD, Consumerization, Mobility

Sammanfattning

De avancerade tekniska enheterna blir ständigt fler och människan blir allt mera beroende av att ha med dem överallt för att utföra olika ärenden. I de flesta fall rör det sig om så kallade smarta telefoner och surfplattor. Nu när vi privat har tillgång till de senaste och mest avancerade enheterna börjar användandet av dem för arbetsrelaterade uppgifter få fart och begreppet Bring Your Own Device (BYOD) växer fram. Verksamheter ser efterfrågan ifrån sina anställda som vill arbeta från sin egen enhet och försöker möta behovet. Dock ökar säkerhetsriskerna när företagsdata laddas ner till den anställdes privata enhet och vandrar med dem ut ifrån kontoret. Även virus kan följa med den privata enheten in på företagets nätverk och orsaka skada. Det gäller för företagen att på bästa sätt skydda sin data samtidigt som den anställde får jobba ifrån sin egen enhet. Detta kan lösas genom teknik och policys, vilket ställer höga krav på att tekniken är säker. Frågeställningen i denna uppsats handlar om hur en teknisk lösning kan väljas så att den uppfyller verksamhetens huvudsakliga behov och dessutom gör användarna nöjda. En kvalitativ studie har utförts med en fallstudie ute på ett företag. Syftet är att identifiera kriterier som företaget och användaren har och med hjälp av dessa bedöma tekniska lösningar på ett tydligt sätt. Detta för att göra det lätt att förstå vad som finns ute på marknaden just nu och hur de förhåller sig till kriterierna. I analysen identifieras kriterierna och en bedömning av hur respektive teknik hanterar de utvalda kriterierna utförs. Slutsatsen blir att verksamheten behöver bedöma hur viktiga de identifierade utvärderingskriterierna är för dem och utifrån det välja en teknisk lösning som passar verksamheten.

Nyckelord: BYOD, Konsumentisering, Mobilitet

Förord

Vi vill tacka vår handledare Patrik Hedberg för det stöd och engagemang som han har gett oss under arbetet med uppsatsen. Vi vill även tacka Jonas Toftefors på Mölnlycke Health Care för att han ställt upp på intervju och berättat från egen erfarenhet av hur de har hanterat BYOD i sin verksamhet.

Jonas och Madelen
Borås, Augusti 2013

Innehåll

1 Inledning

Inledningsavsnittet är en introduktion till BYOD och tidigare forskning samt en problemdiskussion som leder fram till en frågeställning och slutligen uppsatsens syfte, avgränsning och målgrupp.

1.1 Bakgrund

Mobilitet är här för att stanna, i dagens samhälle har vi redan nått en otrolig utbredning av olika avancerade mobila enheter. Trenden väntas öka och enligt Gartner (2013) förväntas det år 2017 att säljas cirka tre miljarder mobila enheter, en ökning med 700 miljoner ifrån 2012. I takt med att försäljningen av mobila enheter ökar påverkas också vårt sätt att arbeta. År 2015 förväntas 1,3 miljarder människor ha ett mobilt arbete, det är 37,5% av världens arbetskraft. (Crook, Jaffe, Boggs & Drake 2011)

På 1980- och 1990-talet var det vanligt att företaget ägde datorn som den anställda arbetade ifrån. Kring millenniumskiftet började priset på datorer sjunka till nivåer som gjorde att privatpersoner hade råd att köpa en egen vilket också innebar att de även kunde använda dem för att utföra arbetsrelaterade uppgifter utanför kontorstid. (McLellan 2013)

Utvecklingen av billig högpresterande teknik har gett privatpersoner möjligheten att äga lika bra eller bättre bärbara datorer, telefoner och surfplattor (vidare benämnt som ”enheter” eller ”mobila enheter”) som det företaget erbjuder, dessutom mer personliga då användaren valt dem själv. När användarna blev bekväma med sina egna anpassade enheter började de ta med sina egna enheter till arbetsplatsen och ställa krav på att de skall fungera där. Detta har gett upphov till uttrycket ”konsumentisering” som handlar om hur ny informationsteknik sprider sig först till privatpersoner och sedan vidare in till företagen. De problem som uppstår när användaren begär åtkomst till verksamhetsdata ifrån sin privata enhet är främst relaterade till verksamhetens kontroll på den data som lagras på en enhet de inte äger. (Scarfö 2012) Den vanligaste lösningen på säkerhetsproblem som uppstår i och med att konsumentiseringen ökar är helt enkelt att förbjuda användarna att använda någonting annat än de enheter de fått tilldelade. Nackdelen med att förbjuda eller hindra användarna ifrån att använda sina egna enheter är enligt Caldwell, Zeltmann och Griffin (2012) att de som vill brukar lyckas hitta möjligheter att använda de privata enheterna trots förbudet. I en studie, publicerad i mars 2011 av *Mobile Enterprise*, uppger 63,5% av användarna att de använder sina privata enheter för att uträtta arbetsrelaterade uppgifter. Det kan skapa problem för IT avdelningen då de inte har kontroll på vad som befinner sig på nätverket och därmed omöjligt kan säkra upp det tillräckligt. Studier visar att allt fler använder sina egna enheter på jobbet olovligt (En av tre använder mobilen utan tillåtelse, 2013). Beteendet ställer arbetsgivaren inför flera ställningstaganden och utmaningar för att göra sina anställda nöjda samtidigt som de måste skydda sina affärsdata.

Allt eftersom konsumentisering blev allt mera etablerat uppkom uttrycket Bring Your Own Device (BYOD) som i grunden beskriver att den anställde tar med sig sin egen enhet för att jobba ifrån. Tre fjärdedelar av världens IT-chefer anser att tjänster som stöder mobilt arbete är avgörande för framgången hos deras företag (Wallström 2013). Trycket på att företagen ska förändras från att förbjuda till att acceptera BYOD kommer både från anställda och från ledningshåll. Inghe (2012) exemplifierar det genom att berätta om en kund vars nytillsatta Chief Information Officer (CIO) kom till sammanträdesrummet och frågade hur han kunde koppla upp sin privata iPad, när han fick svaret att det inte gick sa han att det är något som IT-avdelningen helt enkelt får fixa.

En panel bestående av fyra tillfrågade IT-chefer på svenska kommuner och företag är överrens om att BYOD kommer att slå igenom även här i Sverige. När detta kommer ske råder det dock delade meningar om, allt från att det redan finns i verksamheten till att det inte kommer förrän 2017 (BYOD 2013). Om BYOD kommer vara intressant för alla organisationer råder det delade meningar om i media och tidningar. Analysföretaget Nucleus Research är motståndare och spår att BYOD inte kommer att visa sig vara så bra som det sägs angående minskade kostnader och mera produktiv personal. En anledning till detta är ökad kostnad för IT-support. (Analytiker dömer ut ”bring your own” 2012) IT-chefer inom näringsliv och kommuner tycker att det fortfarande är alldeles för osäkert och många säkerhetsrisker som behöver lösas, därför kommer företagen att avvakta ett tag till innan de påbörjar en implementation av BYOD (BYOD 2013).

1.2 Forskningsöversikt

Begreppet BYOD är relativt nytt, det dök upp först 2009 (Harkins u.å.). Kring BYOD finns det ännu inga doktorsavhandlingar och övriga vetenskapliga artiklar samt undersökningar är med fåtalet undantag skrivna 2012 och framåt. Detta tyder på att det började ta fart på riktigt det senaste året.

I en undersökning genomförd av Dimentional Research (2012) baserad på 768 personer inom IT-sektorn framkommer det att 89 % av deltagarna har mobila enheter såsom smartphones och surfplattor anslutna till företagsnätverket. Av dessa 89 % uppger 65 % att de både har privata och företagsägda enheter anslutna. Vidare uppger 65 % att deras företag tillåter privata enheter att ansluta till nätverket och 78 % rapporterar en dubblering av antalet anslutande privata enheter under den senaste tvåårsperioden. Hälften av de tillfrågade uppger att de är medvetna om att kunddata lagras på mobila enheter samtidigt som det framkommer att det största hotet mot data på mobila enheter är användarnas säkerhetsmedvetenhet. (Dimentional Research 2012) Fler författare instämmer med Dimentional Research om att trenden för att använda sin egen enhet för företagsrelaterade arbetsuppgifter ökar (Burt 2011).

Haejung, William och Choong (2012) har forskat om den hälsoeffekt som det nya beteendet medför. De har studerat användningen av smartphones på jobbet samt i hemmet. Beteendet benämns som OHS (office-home smartphone). Studien visar att en ökad användning av OHS leder till överbelastning av arbete som i sin tur resulterar i konflikter mellan arbetslivet och privatlivet samt ökad stress. Effekten kan minskas genom att låta anställda få en möjlighet att jobba smart och förbättra deras kvalité av arbete och produktivitet. (Haejung, William och Choong 2012)

Ganett (2012) skriver i sin artikel om att den säkerhetsansvarige på företaget ska se förbi hantering av de anställdas enheter och istället fokusera på att stärka interna nätverk. Det behövs verktyg för att säkra verifiering, autentisering och godkännande för att uppfylla företagets IT-policy. Autentisering är baskravet och ska säkerställa att personen och enheten är den som den säger sig vara. Det rekommenderas att avkräva användaren mer än ett användarnamn och lösenord för att öka säkerheten.

Scarfö (2012) menar att det finns två huvudsakliga tillvägagångssätt för att implementera en BYOD lösning, en mjuk så kallad ”Hands off approach” och en hård så kallad ”hands on approach”. Han nämner att de båda lösningarna både har fördelar och nackdelar samt att den mjukare bör vara att föredra ur användarens perspektiv. Viktigt är att skriva ett slutanvändaravtal (End User Agreement, EUA) för att skapa en enkel men tydlig bild av

vilket ansvar och vilka rättigheter användaren respektive verksamheten har. Han beskriver även tre tekniker som hanterar BYOD vilka är Mobile Device Management, Mobile Application Manegment och Mobile Information Management. Slutligen påpekas att oavsett hur verksamheten väljer att implementera BYOD bör focus ligga på att lösningen skall vara enkel och användarvänlig.

Mansfield-Devine (2012) och Caldwell, Zeltmann och Griffin (2012) har tagit fram var sin tio-punktlista med vad de anser är det viktigaste för att lyckas med BYOD. I huvudsak handlar det om vilka som skall tillåtas åtkomst, samt vilka olika enheter, operativsystem och applikationer som verksamheten skall tillåta. Det handlar även om vad verksamheten är ansvarig för vad gäller kostnader för enheter, datatrafik, support och så vidare. Caldwell, Zeltmann och Griffin (2012) går även vidare och ställer de olika operativsystemen mot varandra för att ge en bild av deras fördelar och nackdelar, de kommer fram till att Blackberry och möjligen iOS är att föredra ur säkerhetssynvinkel samt att Android i skrivande stund låg allt för långt bakom för att kunna rekommenderas.

För att få en bild av värdet av BYOD-implementationen för verksamheten genomförde Forrester Consulting (2012) en undersökning på 202 chefer i organisationer som hade ett pågående arbete med BYOD. Deltagarna ifrån USA arbetade på organisationer med minst 1000 anställda och ifrån Europa med minst 500 anställda. 82 % av de tillfrågade uppger att de anställdas produktivitet ökat och 69 % uppger att verksamhetens totala vinst ökat till följd av BYOD. Säkerhetsrelaterade kostnader, kostnader för datatrafik samt support uppges ha ökat sedan införandet men kostnader kopplade till enheten såsom inköpskostnader, kostnader för ersättning av skadade enheter och utbildning har minskat.

Det finns ett antal hinder för verksamheter som vill implementera BYOD. Howze (2012) talar om att BYOD ger ökade säkerhetsrisker genom att enheterna kan föra in virus eller andra skadliga programvaror till verksamhetens nätverk. Miller, Voas & Hurlburt (2012) ser ett problem med integritetssäkerhet när privat data och företagsdata blandas på enheterna. BYOD medför även en högre belastning på nätverket säger Mansfield-Devine (2012). Något som inte är ett hinder för att implementera en BYOD lösning men är ett hinder för användandet av BYOD är att det finns en risk för att användarens integritet kränks och att användaren känner att de ger upp för stor kontroll av enheten (Scarfö, 2012).

1.3 Problemdiskussion

Det finns flera undersökningar som pekar på att användandet av privata enheter för att utföra företagsrelaterade arbetsuppgifter ökar (Dimentional Research 2012; Burt 2011). Flera källor tar även upp fördelarna med att tillåta användaren att arbeta med sin egen enhet. Dessa fördelar handlar bland annat om nöjdare anställda, ökad produktivitet, minskade kostnader och ökad vinst. (Scarfö 2012; Copeland och Crespi 2012a & 2012b; Caldwell, Zeltmann och Griffin 2012; Forrester Consulting 2012)

Det ökade användandet av privata enheter för företagsrelaterade arbetsuppgifter medför även säkerhetsproblem (Mansfield-Devine 2012; Anonymous 2012; Scarfö 2012; Ganett Co 2012). Problemen handlar i huvudsak om att verksamheten tappar kontrollen över sin data och den blandas med privat data på den anställdes enhet, vilket gör det omöjligt att skilja på vem som äger vilket data (Miller, Voas & Hurlburt 2012).

För att få kontroll på den här problematiken har en verksamhet tre huvudsakliga alternativ. De kan förbjuda eller tillåta användaren att använda sina privata enheter för arbetsrelaterade

arbetsuppgifter, alternativt kan de ignorera problemet. De två förstnämnda alternativen kan lösas med tekniska lösningar och en policy för användandet. Det finns flera artiklar skrivna om policyhantering (Mansfield-Devine 2012; Caldwell, Zeltmann och Griffin 2012) och olika tekniker finns även behandlade (Scarfö 2012).

Väljer en verksamhet att se över möjligheten att tillåta användandet av privata enheter för företagsrelaterade arbetsuppgifter ställs de inför problemet med att hitta en teknisk lösning som uppfyller verksamhetens och användarnas huvudsakliga behov. Trots att det är användarna som driver på BYOD är det företaget som måste bemöta problemet. (Scarfö 2012) Därför anser vi att tonvikten bör läggas på att verksamhetens behov uppfylls. Samtidigt anser vi inte att användarens behov bör åsidosättas, därför är det viktigt att hitta en lösning som kan accepteras av båda sidor. Eftersom alla verksamheter ser olika ut och har olika förutsättningar och behov rörande IT-säkerhet och krav på IT-verksamheten som helhet, gäller det att hitta något som passar för verksamheten. Det finns olika tekniska lösningar som hanterar BYOD på olika sätt, så en lämplig lösning bör väljas utifrån de krav som en verksamhet ställer på sin BYOD-lösning.

1.4 Frågeställning

Baserat på introduktionen (Kapitel, 1.1), forskningsöversikten (Kapitel, 1.2) och problemdiskussionen (Kapitel, 1.3) kan det konstateras att BYOD växer snabbt och hanteras av verksamheter på olika sätt. Det kan också konstateras att verksamheten har flera behov som behöver tas hänsyn till, dessutom är det viktigt att användarna känner sig nöjda med den tekniska lösningen som implementeras. Därför ser vi behovet av att besvara följande forskningshuvudfråga:

- *Hur kan en verksamhet välja en teknisk lösning för BYOD som uppfyller verksamhetens huvudsakliga behov och dessutom göra användarna nöjda?*

För att finna svar på vår huvudfråga har vi identifierat tre delfrågor som först behöver besvaras. Dessa delfrågor hjälper till att besvara huvudfrågan genom att precisera vad vi har tittat på inom området.

- *Vad innebär begreppet Bring Your Own Device (BYOD)?*
- *Vilka tekniska lösningar finns det för implementering av BYOD?*
- *Vilka huvudsakliga behov har verksamheten och användarna vid införandet av BYOD?*

1.5 Syfte

Syftet med denna uppsats är att ta reda på hur en teknisk lösning för BOYD kan väljas så att den uppfyller verksamhetens huvudsakliga behov och samtidigt gör användarna nöjda. Uppsatsen kan på så sätt fungera som ett stöd för företag som ser över möjligheten att implementera en BYOD lösning.

1.6 Avgränsning

BYOD är ett område som innefattar många olika delar vilka påverkar både användaren och verksamheten. Vi har valt att se på den tekniska implementationen av BYOD då vi i kapitel 2.1 identifierat att det finns mer berört kring de ”mjuka” aspekterna än de tekniska. Vi kommer endast titta på de tekniker som är tillgängliga i dagsläget.

1.7 Målgrupp

Målgruppen för uppsatsen är verksamheter som ser över möjligheten att implementera BYOD istället för att förbjuda användandet av privata enheter för verksamhetsrealterat arbete. Verksamheten har i någon form anställda som önskar arbeta ifrån privata enheter. Det kan handla om påtryckningar antingen ifrån ledningshåll eller från anställda, alternativt kan det handla om att IT-avdelningen sett att privata enheter förekommer och de inte vet hur det skall hanteras. Verksamhetens inriktning är av mindre vikt, allt ifrån IT-branschen till kommun och landstings verksamheter kan ha intresse av BYOD. Även akademier inom informatik och IT kan ha ett intresse för uppsatsen för att få en bättre förståelse för BYOD och olika tekniska lösningar.

1.8 Disposition

Kapitel 1 Inledning
Inledningsavsnittet är en introduktion till BYOD och tidigare forskning samt en problemdiskussion som leder fram till en frågeställning och slutligen uppsatsens syfte, avgränsning och målgrupp.

Kapitel 2 Metod
I metodkapitlet presenteras den valda metod som använts i uppsatsen. En presentation av den kunskapskaraktärisering och det vetenskapliga perspektivet. Här presenteras även vald forskningsansats, hur teori och empiri relaterar till varandra samt vald forskningsdesign. Även hur insamling av teori och empiri har gått till samt vald metod för utvärdering och avslutningsvis en sammanfattning över metodvalen.

Kapitel 3 Teoretisk referensram
I detta kapitel presenteras uppsatsens teoretiska referensram. Inledningsvis kommer en förklaring av begreppet BYOD med dess för och nackdelar. Även förklaring kring säkerhet begreppen ”hands on” och ”hands off” tas upp. Avslutningsvis förklaras olika tekniska lösningarna och hur de fungerar samt delfrågorna besvaras.

Kapitel 4 Empiri
I detta kapitel presenteras den empiri som samlats in under en intervju med Jonas Toftefors på Mölnlycke Health Care.

Kapitel 5 Analys
Kapitlet presenterar en analys av den insamlade teorin och empirin. Först analyseras teorin och empirin för att få fram ett antal utvärderingskriterier, därifrån väljs sedan relevanta kriterier ut. Slutligen utvärderas respektive teknik utifrån de olika utvärderingskriterierna.

Kapitel 6 Resultat och diskussion
Här presenteras först resultatet ifrån analysen följt av en diskussion kring den. Vi har tagit hänsyn till studiens hermeneutiska synsätt där begreppet samt teknikernas delar har analyserats under föregående kapitel och nu hur delarna förhåller sig till helheten.

Kapitel 7 Slutsats och diskussion
I följande kapitel beskrivs slutsatsen där frågeställningen besvaras och det fungerarsom en sammanställning ifrån analysdelen. Även en utvärdering av vald metod samt de valda utvärderingskriterierna kommer att diskuteras. Slutligen ges förslag till fortsatt forskning.

2 Metod

I metodkapitlet presenteras den valda metod som använts i uppsatsen. En presentation av den kunskapskaraktärisering och det vetenskapliga perspektivet. Här presenteras även vald forskningsansats, hur teori och empiri relaterar till varandra samt vald forskningsdesign. Även hur insamling av teori och empiri har gått till samt vald metod för utvärdering och avslutningsvis en sammanfattning över metodvalen.

2.1 Kunskapskaraktärisering

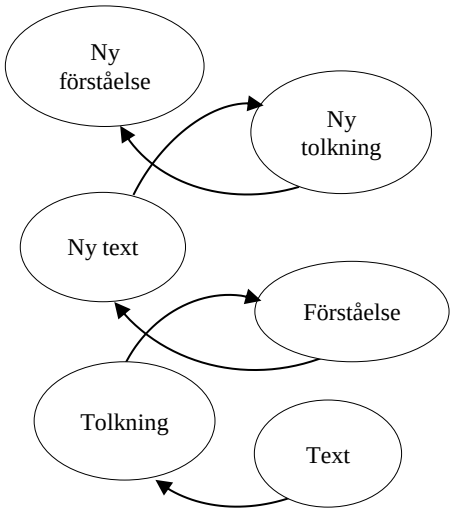
Goldkuhl (2011) talar om att det finns olika former av kunskap som ska eftersträvas i samband med kunskapsutveckling. De kunskapsformerna han nämner är kategoriell, klassificerande, karaktäriserande, förklarande, vägledande, värdeskapande, kritisk och prospektiv kunskap. Baserad på uppsatsens huvudfråga som är: ”*Hur kan en verksamhet välja en teknisk lösning för BYOD som uppfyller verksamhetens huvudsakliga behov och dessutom göra användarna nöjda?”,* kommer kunskapsformen att bli både kategoriell och vägledande.

Kategoriell kunskap handlar om att det som studeras ska begreppsliggöras och fenomen ska delas in i olika kategorier (Goldkuhl 2011). Han menar på att kategoriell kunskap kan ses som en del i alla de övriga kunskapsformerna eftersom det oftast först och främst handlar om att definiera och klargöra begrepp i all kunskapsutveckling. När det gäller vägledande kunskap går det inte att säga om det är sant eller falskt, utan författarna får se det mera som vilket som är mest lämpligt. Vägledande kunskap har till syfte att tala om hur forskaren bör gå tillväga i olika situationer. (Goldkuhl 2011) Eftersom uppsatsen kommer resultera i kriterier och egenskaper kring tekniska lösningar och ska fungera som stöd till företag som funderar på att implementera en teknisk lösning för BYOD blir kunskapsformen både kategoriell och vägledande. Goldkuhl (2011) säger även att i vägledande kunskap ska forskaren tänka på värdekunskap, alltså vilket är det önskvärda värdet som forskaren vill att handlingen ska leda till. Detta kan appliceras på frågeformulering genom att de olika tekniska lösningar som presenteras resulterar i olika effekter för företaget och de anställda.

2.2 Vetenskapligt perspektiv

Med utgångspunkt i frågeställningen och kunskapskaraktäriseringen (kategoriell och vägledande kunskap) har studien antagit ett hermeneutiskt synsätt. Hermeneutiken handlar om tolkningslära där forskarna studerar, tolkar och försöker förstå. Forskare som har ett hermeneutiskt synsätt ska vara öppna, ”subjektiva” och engagerade. (Patel 2011) Detta görs i uppsatsen genom att försöka skapa en förståelse för hur en teknisk lösning kan väljas så att den uppfyller verksamhetens huvudsakliga behov och dessutom gör användarna nöjda. Vi studerar begreppet BYOD både i teori och i praktik för att skapa en förståelse och för att kunna besvara huvudfrågan.

Det hermeneutiska synsättet handlar även om att studera helheten och titta på hur delarna förhåller sig till helheten och växla mellan att titta på helheten och delarna för att komma fram till en fullständig förståelse. Uppsatsen har formats efter den hermeneutiska spiralen som är illustrerad i figur 1 där text, tolkning och förståelse leder till



Figur 1. Hermeneutiska spiralen, Egen utvecklad efter Patel, 2011.

ny text som igen tolkas och ger en ny förståelse och följer detta mönster tills förståelse har uppnåtts. (Patel 2011)

2.3 Forskningsansats

De finns två olika forskningsansatser, kvantitativ och kvalitativ forskning. Kvantitativ forskning lägger sitt fokus på insamling av stora mängder data som sedan analyseras. Den har en deduktiv inriktning där teorier prövas genom insamling av empiri. Den kunskapsteoretiska inriktningen är en naturvetenskaplig modell som har positivismen som huvudinriktning. Den kvalitativa forskningen handlar om att fokus läggs på insamling och analys av ord istället för siffror. Den kunskapsteoretiska inriktningen innebär att forskarna ska ha ett tolkande synsätt där insamlingen av teori i huvudsak är induktiv och där empirin genererar teori. Den kvalitativa forskningens ontologiska inriktning är konstruktionism vilket innebär att ta hänsyn till hur individen tolkar och påverkar sin omgivning. (Bryman 2011) Uppsatsens forskningsansats har varit kvalitativ eftersom frågeställningen handlar om att undersöka hur en teknisk lösning kan väljas så att den uppfyller verksamhetens huvudsakliga behov och dessutom gör användarna nöjda. Uppsatsen har antagit ett hermeneutiskt synsätt då vi ska samla in och analysera ord för att på så sätt tolka och förstå svaret på frågan.

2.4 Relationen mellan teori och empiri

Det finns tre huvudsakliga angreppssätt som är lämpliga när det gäller relationen mellan teori och empiri, dessa är antingen ett deduktivt angreppssätt där teorin ska leda till observationer/resultat eller ett induktivt angreppssätt där observationer/resultat ska generera teori eller abduktion som är ett angreppsätt där både deduktion och induktion blandas. (Patel 2011) Både ett deduktivt och induktivt angreppssätt har använts och de har fått stötta varandra för skapande av en teoretisk och empirisk grund. Studien inleddes med ett deduktivt angreppsätt där teori samlades in för att skapa en grund. Det var här som problemformuleringen och delfrågorna skapades genom identifiering av ett behov. Därefter övergick studien till ett induktivt angreppssätt där empirin insamlades under en intervju för att identifiera kriterier som en verksamhet hade på en BYOD lösning. Sen övergick angreppssättet till ett deduktivt sätt där mera teori insamlades för att besvara resterande frågor. Därefter skedde ett parallellt arbete genom både induktivt och deduktivt angreppssätt där tolkning av empirin och insamlingen av relevant teori ledde fram till en analys, resultat och slutsats. Eftersom uppsatsen ska generera både kategoriell och vägledande kunskap har en djup förståelse för tekniken skapats genom att låta empirin komplettera analysen. Detta har gjorts genom att kunskap från praktiskt arbete och svaret på delfrågan hjälpte till att besvara huvudfrågan som på så sätt fått en grund ifrån både teorin och empirin.

2.5 Forskningsdesign

Som tidigare nämnts har uppsatsen en kvalitativ metodansats för att besvara frågeställningen. För val av formen på design för insamling av empiri finns det tre stycken som är vanligast att tillämpa. Dessa är enligt Patel (2011) surveystudier, experiment och fallstudier. Surveystudier handlar om att undersökningen sker över en större avgränsad grupp och ska oftast besvara frågor som vad, var, när och hur. Under en experimentstudie studeras olika variabler och vad som kan påverka dessa, i syfte att försöka få kontroll på dem. (Patel 2011) Dessa båda forskningsdesigner kan inte hjälpa till att besvara frågeställningen eftersom surveystudier oftast är lämpliga ihop med kvantitativa studier och svaret på frågeställningen inte hittas genom att studera och påverka olika variabler som i en experimentell studie. Fallstudie definieras som en design som täcker en detaljerad och ingående analys av ett enda fall där en mindre avgränsad grupp studeras (Patel 2011). En fallstudie utfördes där empirin samlades in

för att identifiera kriterier och för att få en inblick i hur det i praktiken fungerar när ett företag har hanterat BYOD med hjälp av en teknisk lösning. Eftersom uppsatsens kunskap är kategoriserande och vägledande kan informationen ifrån fallstudien resultera i en förståelse för tekniken och en identifiering av kriterier som kan användas för analys och slutsats.

2.6 Insamling av teori

Litteraturgenomgång påbörjades med att undersöka hur allmänintresset såg ut kring BYOD. För att navigera kring allmänintresset användes sökmotorn Google och databasen mediearkivet för att hitta relevanta artiklar. Efter insamlandet av artiklar till allmänintresset skapades en större förståelse för ämnet.

Studien fortsatte genom att söka upp vetenskapliga artiklar och till detta användes Högskolan i Borås sökverktyg ”Summon” som ger sökresultat ifrån samtliga databaser som Högskolan erbjuder. Syftet var att finna artiklar som var vetenskapligt granskade och publicerade antingen på konferenser eller i tidsskrifter, filtrering vid sökningen användes för att utesluta icke vetenskapliga artiklar. Bryman (2011) säger att genomgång av existerande litteratur inom området har till syfte att ta reda på vad som gjorts tidigare och vilken kunskap som redan finns. Genom en genomgång av artiklar som var relevanta för begreppet BYOD och för att besvara frågeställningen har studien på ett vetenskapligt sätt gått igenom vad som redan har gjorts inom BYOD. Under litteraturgenomgången upptäcktes att det mesta var skrivet 2012 och att det inte fanns några doktorsavhandlingar och att de artiklar som publicerats i huvudsak kommer ifrån konferenser. Detta beror troligtvis på att ämnet började diskuteras mest aktivt under 2012 och artiklar har en snabbare publiceringstid än avhandlingar.

Eftersom frågeformuleringen är hur en teknisk lösning för BYOD kan implementeras så att den uppfyller verksamhetens huvudsakliga behov och dessutom gör användarna nöjda, samt att utvecklingen här sker snabbt, har källorna varit media som är mera aktiv och snabbrörlig för att få aktuell information. Därför vände vi oss till bloggar och digitala tidningar med relevant information där BYOD diskuteras hela tiden och som publiceras samtidigt som vi samlar in teorin. Sökord som använts för att finna relevanta källor har varit bland annat BYOD, mobility, consumerization, technology, network acess controll, Mobile Application Managment (MAM), Mobile Device managment (MDM), Virtuall Desktop Infrastrukture (VDI).

Den främsta datakällan kommer ifrån utvalda dokument. Bryman (2011) säger att ordet dokument kan stå för många olika typer av källor, men ska vara material som kan läsas, inte har skapats speciellt i ett samhällsvetenskapligt syfte, ska finnas bevarat och vara tillgängligt för analys och vara relevant för en samhällsvetare. De olika dokumenttyperna som finns är personliga dokument, officiella dokument ifrån statliga myndigheter eller som är mera privata ifrån en organisation, massmediedokument och virtuella dokument (Bryman 2011). Rapportens insamling av dokument har skett genom virtuella dokument som hämtats på nätet. När dokumenten är utvalda kan Brymans (2011) lista över bedömningskriterier vara lämplig att använda sig av för att bedöma dokumentets kvalitet.

1. Autenticitet (Är materialet äkta och av ett otvetydigt ursprung?)
2. Trovärdighet (Är materialet utan felaktigheter och förvrängningar?)
3. Representativitet (Är materialet typiskt för den kategori den tillhör)? Om så inte är fallet, känner man till i vilken grad det inte är typiskt?)
4. Meningsfullhet (Är materialet tydligt och begripligt?)

I uppsatsen har dessa bedömningskriterier tagits till hjälp vid val av dokument som använts som datakällor för att fastställa dess kvalitet. Det Bryman (2011) säger är att det är viktigt att tänka på de fyra bedömningskriterierna för virtuella dokument. För att styrka autenticitet är det viktigt att vara vaksam eftersom vem som helst kan skapa en hemsida eller skriva bloggar, dessutom kan det bli svårt att kontrollera trovärdheten på vissa sidor då dessa kan vara skrivna med en partisk synvinkel. Även representativitet är svårt att bedöma eftersom Internet är en plats med ständiga förändringar och språket som används kräver oftast en förståelse för ämnet vilket resulterar i att meningsfullheten kan bli svår att avgöra. (Bryman 2011) Alla de valda dokumenten i denna uppsats har kritiskt granskats för bedömning av källor, samt vem som skrivit till exempel artikeln och vilken typ av tidskrift den är publicerad i.

2.7 Insamling av empiri

För att identifiera vad en teknik bör uppfylla för att vara användbar för verksamheten som skall införa BYOD studerades hur en implementation har gått till i praktiken. Valet av företag att intervjua gjordes genom ett målstyrt urval som enligt Bryman (2011) görs med hjälp av två nivåer, samt utifrån uppsatsens mål. Det först valet gjordes med kriteriet av ett relevant företag som var intresserade av att hantera BYOD och dessutom redan hade valt en lösning för hantering av BYOD, så det blev Mölnlycke Health Care. Därefter kom valet av intervjuperson vilket i Mölnlyckes fall handlade om att kontakta den som var involverad i Enterprice Architekture för IT.

Bryman (2011) säger att kvalitativa metoder studeras bäst med hjälp av intervjuer eller en deltagande observation där en intervju går ut på att den som håller i intervjun ställer frågor till respondenten och under en deltagande observation studerar forskaren passivt sitt objekt. Fördelen med en intervju är att vissa frågeställningar lämpar sig bättre att studera under en intervju framför deltagande observationer. Det går lättare att rekonstruera händelser och ta hänsyn till etiska synpunkter och de reaktiva effekter som kan uppstå. Vid intervjuer påverkas respondentens liv i mindre grad och det är en större frihet. Det blir även ett specifikt fokus och det är lättare att göra en longitudinell forskning under en intervju. Det som kan ses som nackdelar mot intervjuer är att det är lätt att missa avvikande och dolda aktiviteter. Det är också svårt att se världen ur den andres ögon eller att lära sig det lokala språkbruket. I en intervju kan det också vara svårare att möta det oväntade och vara flexibel. Sensitiviteten är svår att hålla vad gäller kontexten och en naturalistisk tonvikt. (Bryman 2011)

Enligt Bryman (2011) finns det två huvudsakliga former av kvalitativa intervjuer, ostrukturerade och semistrukturerade intervjuer. I den ostrukturerade intervjun ges respondenten möjlighet att associera fritt och kan liknas vid ett vanligt samtal. I en semistrukturerad intervju är vissa frågor förbestämda och det finns en möjlighet att ställa följdfrågor beroende på viktiga svar ifrån respondenten. Uppsättningen av frågorna kan ses som ett frågeschema och vara formulerade på ett allmänt sätt. En nackdel med detta sätt som kan påverka resultatet kan vara att frågorna är oklart formulerade samt på vilket sätt intervjuare ställer frågan. Respondenten kan också missförstå frågan alternativt dokumenterar intervjuaren svaren på ett felaktigt sätt. (Bryman 2011)

Den intervju som utfördes var semistrukturerad där ett visst antal frågor var förbestämda för att styra intervjun i rätt riktning, det fanns utrymme för följdfrågor kring intressanta svar och spår som respondenten tog. Respondenten fick berätta om sin erfarenhet och tankar kring BYOD och den teknik de använt sig av samt hur de har implementerat den. Intervjun skedde i Göteborg på Mölnlycke Health Care’s kontor och varade i cirka 1,5 timme, intervjun spelades in.

2.8 Analysmetod

Patel (2011) säger att det under datainsamlingen och den inledande analysen är viktigt att anteckna och spara de tankar som uppkommer kring materialet för användning under den slutliga analysen. För dokumentering av materialet under analysen säger Patel (2011) att det är viktigt att välja bra benämningar på kategorierna som texten placeras under och få en bra struktur på innehållet för att göra det lätt för läsaren att följa med och även på ett tydligt sätt få med författarnas kommentarer och tankar kring svaren. Patel (2011) säger även att inför analysen bör texten läsas igenom flera gånger.

För att på bästa sätt tolka de insamlade dokumenten säger Bryman att det finns tre lämpliga angreppssätt. Det kan ske med hjälp av kvalitativ innehållsanalys, semiotik eller hermeneutik. En kvalitativ innehållsanalys syftar till att söka efter bakomliggande teman i det material som skall analyseras. Angreppssättet semiotik är läran om tecken där det är symboler i vardagen som analyseras, det sistnämnda angreppsättet hermeneutik handlar det om att analysera texter och få fram textens mening utifrån det perspektiv som dess upphovsman haft. (Bryman 2011)

Vi har tillämpat de ovan nämnda angreppsätten genom att först under insamlingen av materialet anteckna tankar och funderingar för att kunna användas vid den framtida analysen. För att kunna besvara frågeställningen behövde vi först ta reda på vilka behov företaget och användarna på verksamheten hade rörande BYOD och tekniken däromkring. Detta gjordes genom att vi bearbetat materialet som fanns i textform både ifrån empirin och teorin genom att läsa texterna flera gånger. På så sätt kunde vi identifiera olika behov och utifrån dem utforma lämpliga utvärderingskriterier som känns viktiga för både företaget och användarna. Sen försökte vi se samband och likheter mellan empirin och teorin och göra ett urval över vilka kriterier som var mest relevanta utifrån företagets och användarnas perspektiv.

Nästa steg var att identifiera egenskaper hos de olika teknikerna för att med hjälp av dem kunna bedöma hur de förhåller sig till de olika utvärderingskriterierna. Vi använde den kvalitativa innehållsanalysen för att leta efter bakomliggande teman i teoritexten för att på så sätt upptäcka egenskaperna. Även här gjordes en jämförelse mellan de olika teknikerna för att hitta gemensamma egenskaper som kunde väljas ut för vidare analys.

När både utvärderingskriterier och teknikernas egenskaper var identifierade och utvalda kunde dessa sammanställas och bedömas utifrån hur teknikerna förhåller sig till de olika utvärderingskriterierna och på så sätt besvara frågeställningen *”Hur kan en verksamhet välja en teknisk lösning för BYOD som uppfyller verksamhetens huvudsakliga behov och dessutom göra användarna nöjda?”.*

Eftersom uppsatsens kunskapskarakterisering bland annat handlar om vägledande kunskap ville vi även reflektera över vilka effekter de olika teknikerna kunde generera om ett företag valde den ena tekniken eller den andra. Detta gjorde vi genom ett resultatkapitel där vi analyserade teknikerna var för sig och beroende på hur de hanterar de olika utvärderingskriterierna kunde vi se mönster av vilka effekter de troligen skulle resultera i för både företaget och användarna.

2.9 Utvärderingsmetod

Utvärderingsmetoden för bedömning av resultatet är baserad på Brymans teori, där han säger att reliabilitet, replikation och validitet är de viktigaste kriterierna vid en bedömning. (Bryman 2011) Bryman menar att det för kvalitativa undersökningar kan lämpa sig med andra kriterier

som till exempel tillförlitlighet som är mera anpassade för den kvalitativa forskningen. Kriteriet tillförlitlighet som täcker upp både reliabilitet och validitet med hjälp av sina delkriterier har därför använts vid utvärderingen för uppsatsen. Replikation handlar om att kunna upprepa studien och är enligt Bryman (2011) svårt att applicera på en kvalitativ studie eftersom det i de flesta fall handlar om tolkning av ord och text vilket inte går att upprepa med exakt samma resultat igen, därför har kriteriet replikation valts bort ifrån denna uppsats.

2.9.1 Tillförlitlighet

Studien genomfördes med hög tillförlitlighet i åtanke genom att ta hjälp av Brymans tre delkriterierna som finns för att öka tillförlitlighet. Dessa delkriterier är överförbarhet, pålitlighet och en möjlighet att styrka och konfirmera. (Bryman 2011) Följande underrubriker beskriver på vilket sätt delkriterierna har applicerats på studien.

Överförbarhet
Bryman (2011) säger att överförbarhet kan ses som extern validitet. Resultatet som kommer fram ska vara överförbart till en annan miljö och detta uppnås bäst genom en fyllig och tät beskrivning av de detaljer som identifierats. Fallstudien har en medveten låg överförbarhet eftersom den har till syfte att resultera i en identifiering av kriterier som gäller för den specifika situationen snarare än att se ett generellt beteende. Däremot har de insamlade dokumenten en hög överförbarhet eftersom de har samlats in med en så stor bredd som möjligt. Detta ska sen kunna ses som en databas för andra forskare och resultatet har då fått en hög överförbarhet. Då BYOD fortfarande är ett väldigt nytt ämne är syftet att bygga upp en bra grund som ska kunna vidareutvecklas och anpassas allt eftersom tekniken går vidare samt beroende på vilket företag som tänkt använda sig av BYOD.

Pålitlighet
Enligt Bryman (2011) är det samma sak som reliabilitet där forskarna ska sträva efter att få likartade resultat vid andra tillfällen. Detta delkriterie är svårt att uppnå då kvalitativa studier oftast resulterar i stora mängder data som ska granskas av utomstående personer. Men grundtanken här är att ta hjälp av utomstående personer som får fungera som granskare både under processens gång och när resultatet är uppnått. Uppsatsen får då ett granskande synsätt som ökar pålitligheten. (Bryman 2011) Då denna uppsats kommer generera i stora mängder data på kort tid blir det olämpligt att använda flera olika granskare, därför får examinatorn fungera som granskare.

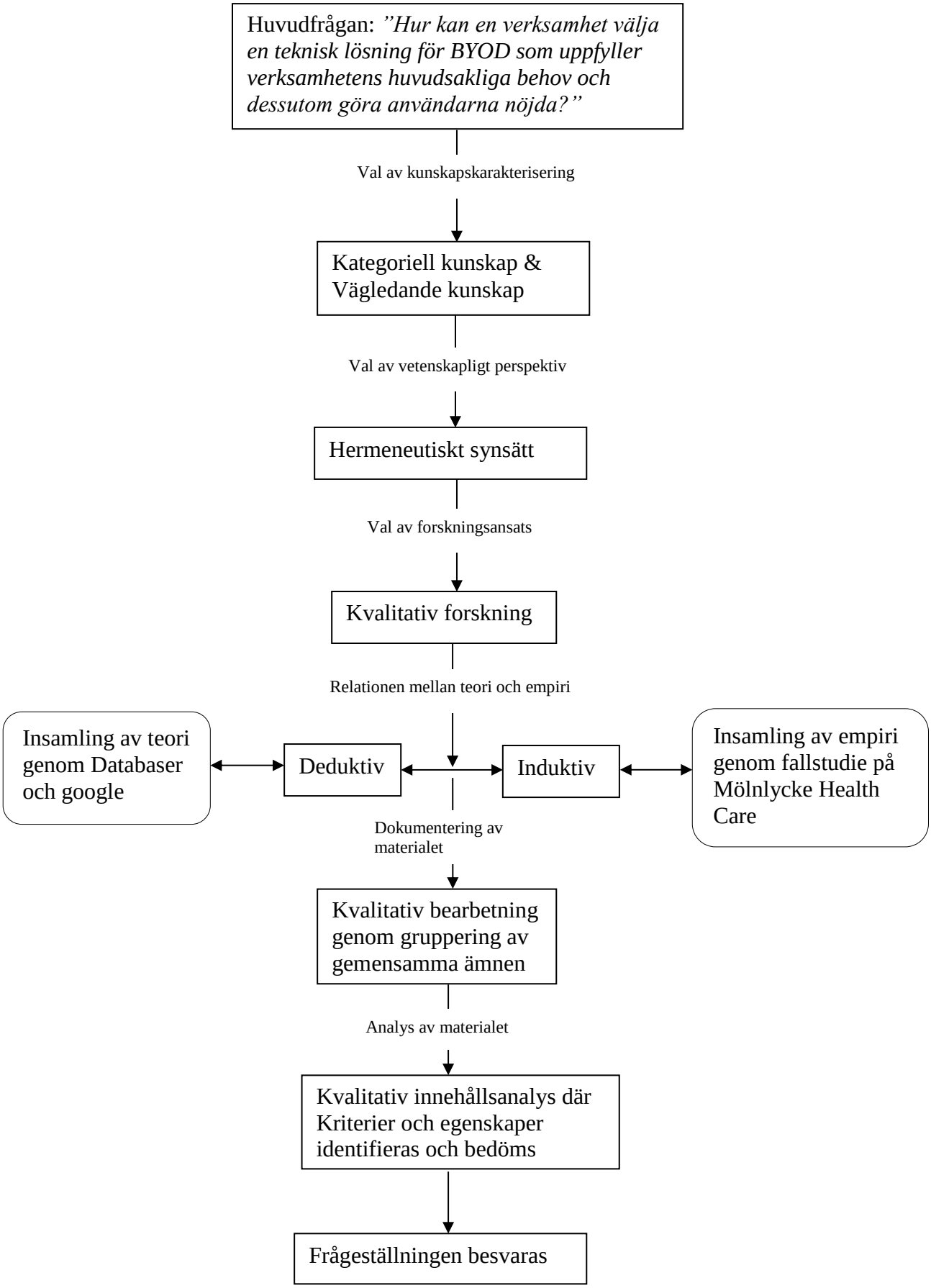
Möjlighet att styrka och konfirmera
Här är det viktigt att påvisa att innehållet inte låtit sig medvetet spegla några personliga värderingar eller teoretiska inriktningar som påverkat den slutsats som redovisas eller hur utförandet har skett (Bryman 2011). Det ska synas att rapporten är agerad i god tro och detta styrks genom att vara noga med att grunda påståenden och argument i teorin. Genom att den insamlade empirin har granskats och godkänts av respondenten har risken minimerats för att återgivandet av empirin påverkats av personliga tolkningar och värderingar.

2.10 Presentation

Hela forskningen presenteras i uppsatsform och är utformad på ett sådant sätt som lämpar sig bäst till målgruppen. Syftet med uppsatsen var att generera kategoriell kunskap om de olika teknikerna som lämpar sig för hantering av BYOD. Uppsatsen kommer efter ett godkännande ifrån examinator tillgängligöras på Borås Academic Digital Archive (BADA).

2.11 Sammanfattning

I en egen modell som presenteras i Figur 2 sammanfattas metodvalen för detta arbete.



Figur 2: Metodval, Egen

3 Teoretisk referensram

I detta kapitel presenteras uppsatsens teoretiska referensram. Inledningsvis kommer en förklaring av begreppet BYOD med dess för och nackdelar. Även förklaring kring säkerhet begreppen ”hands on” och ”hands off” tas upp. Avslutningsvis förklaras olika tekniska lösningarna och hur de fungerar samt delfrågorna besvaras.

3.1 Bring Your Own Device (BYOD)

BYOD handlar om hur den anställde blir allt mera van vid att organisera sitt privata liv med hjälp av sin smartphone och förväntar sig kunna göra detsamma med sin arbetsrelaterade information på sin egen smartphone. Det är denna handling ifrån användarens sida som kallas för BYOD. (Caldwell, Zeltmann och Griffin 2012)

French (2011) anser att BYOD begreppet är en motreaktion som uppkommit på grund av företagens policyrestrektioner som säger att endast vissa utvalda enheter får användas för att utföra arbetsrelaterade uppgifter. Detta leder till att den anställde hittar egna vägar att gå runt företagets policy för att få jobba ifrån sin egen enhet. Anledningen till att företagen vill neka sina anställda att jobba ifrån egna enheter anser French (2011) handlar om bekvämlighet ifrån företagets sida. Det blir lättare att förvalta systemet, lättare med enhetsunderhåll, och kostnader för IT-support hålls nere samt potentiella säkerhetsrisker, och/eller belastning på det interna systemet som inte är designat för okontrollerade enheter. När företaget accepterar BYOD ses det som en ”motreaktion på motreaktionen” då verksamheten vill få koll på de enheter som tidigare användes bakom ryggen på dem. (French 2011)

Den största drivfaktorn till att BYOD uppkommit är konsumentiseringen som beskrivs bäst enligt Scarfö (2012) som en trend där ny informationsteknologi först sprider sig till användarens marknad och sedan vidare in till företag och organisationer, i stället för tvärt om. Han menar även att det inte bara är smartphones och surfplattor som räknas hit utan även olika tjänster såsom social media och klassiska eposttjänster.

3.1.1 För och nackdelar med BYOD

Caldwell, Zeltmann och Griffin (2012) säger att BYOD är bra för verksamheter och att det leder till ökad produktivitet bland de anställda. Även Inghe (2012) instämmer med att de anställda upplever sig själva som mer produktiva och effektivare i sitt arbete eftersom BYOD uppmuntrar dem till att arbeta oberoende av tid och plats.

Mobile Enterprise säger i Caldwell, Zeltmann och Griffin (2012) artikel att företagens intresse ligger i att minska kostnader och öka vinster. Teknologi är en stor kostnad för de flesta företag och genom att låta sina anställda köpa, ta hand om och underhålla sin egen enhet kan kostnaderna minska för företaget eftersom det blir färre enheter för IT-avdelningen att ta hand om. Även Scarfö (2012) instämmer med ovanstående om att den största vinsten är minskade kostnader och ökad produktivitet. Även Copeland och Crespi (2012a & 2012b) och Forrester Consulting (2012) talar om samma fördelar med BYOD som övriga författare. En sammanfattning av de fördelar som nämns med BYOD är:

- Flexiblare arbete för de anställda
- Nöjdare anställda
- Ökad produktivitet
- Minskade kostnader

Howze (2012) är en teknikguru med 25 års erfarenhet ifrån IT och kommunikation och han vill påpeka farorna med BYOD. Han säger att det flesta smarta enheter som vi bär med oss saknar i princip helt några inbyggda säkerhetfunktioner vilket kan resultera i att virus eller andra skadliga programvaror kan skada företagsinformationen och de smarta enheterna blir som trojanska hästar som invaderar arbetsplatsen. Howze (2012) säger även att lättillgänglig access till social media skapar improduktivitet och är en attack vektor där virus sprids och information blir stulen. En undersökning ifrån Dimentional Research (2012) visar även att det är användarnas brist på säkerhetsmedvetenhet som är det största hotet för företagsdata. Fler som håller med Howze om att BYOD ger ökade säkerhetsproblem är Mansfield-Devine (2012), Anonymous (2012), Scarfö (2012) och Ganett Co (2012).

Miller, Voas & Hurlburt (2012) säger att risken ökar för att konfidentiell verksamhetsdata börjar vandra ut från kontoret på grund av att användarna lagrar den på sin enhet. På en enhet som verksamheten äger finns möjligheten att påtvinga en stark säkerhetspolicy som syftar till att skydda den typen av konfidentiell verksamhetsdata. Däremot på en privat enhet är det av naturliga skäl svårt för verksamheten att påverka enhetens säkerhetspolicy, så att verksamhetens konfidentiella data blir bättre skyddat. Det är inte bara lagringen av verksamhetsdata på den anställdes enhet som ökar säkerhetsriskerna utan även när användarens privata data blandas med arbetsrelaterad information. En åtgärd emot denna risk är att en gräns måste hållas/skapas mellan vad som tillhör vem på den anställdes enhet. (Miller, Voas & Hurlburt 2012)

Ytterligare en nackdel med BYOD är att de egna enheterna orsakar en högre nätverksbelastning. Mansfield-Devine (2012) menar på att användarna ofta har flera olika privata enheter som de förväntar sig kunna koppla upp mot nätverket samtidigt. Är inte nätverket dimensionerat för att klara av den ökade belastningen kan följden bli att det går ut över möjligheten för användarna att utföra sina dagliga arbetsuppgifter så effektivt som möjligt. (Mansfield-Devine 2012)

Det finns även ytterligare aspekter som kan påverkas negativt vid införandet av BYOD och det är ur den anställdes synvinkel. Rymon (2012) talar om att den egna enheten är mer än bara en elektronisk enhet för den anställde, den skall istället ses som en modern accessoar för alla sysslor, även arbetsrelaterade. Den anställde vill känna att de har kontrollen över sin enhet, de vill ha hög integritet och samtidigt behålla användarupplevelsen när de jobbar med den. Vid den vanligaste hanteringen av BYOD för att skydda verksamhetsdata får verksamheten full kontroll över enheten och dess data vilket är oönskat utifrån den anställdes synvinkel. (Rymon 2012)

Även flera olika kostnader dyker upp i samband med nackdelar emot införande av BYOD. Brandel (2012) säger att i vissa lägen kan BYOD orsaka ökade kostnader om verksamheten inte är väl införstådda med hur BYOD påverkar verksamheten. Genom att vara medveten om var risken för ökade kostnader ligger kan verksamheten vara beredd på att motverka det. Arbetet för att kunna stödja alla de olika enheterna som de anställda vill arbeta ifrån är ett exempel på en kostnad som kan öka markant. Om verksamheten tar på sig fullt ansvar för support kan kostnaderna öka oproportionerligt mot vinsten med BYOD vilket ses som negativt. Fler kostnader kan även uppkomma då den trådlösa infrastrukturen påverkas vid fler enheter vilket leder till att verksamheten behöver förbättra sin kapacitet. Även verksamhetens mjukvara och service måste kunna möta behovet som BYOD medför vilket leder till ytterligare ökade kostnader.(Brandel 2012)

Kostnaderna kan även öka för att skapa och uppdatera applikationer som möjliggör för den anställde att kunna arbeta ifrån sin enhet. (Kaneshige 2012)

Det som ovan nämnda författare beskriver som nackdelar med BYOD kan sammanfattas med:

- Ökade säkerhetsrisker
- Privat data och företagsdata blandas
- Högre belastning på nätverket
- Användaren tappar kontrollen över enheten
- Ökande dolda kostnader

3.2 Säkerhetsaspekter

Säkerhet är den klart största risken med BYOD och det tyngsta motargumentet mot konceptet. När privata enheter börjar cirkulera inne på ett företag och anställda börjar använda dessa till att lagra verksamhetsrelaterad information uppkommer säkerhetsproblem som tidigare inte funnits när IT-avdelningen hade full kontroll över alla enheter på nätverket. När företaget kontrollerar en enhet har de möjlighet att konfigurera den för att nå den säkerhetsnivå de vill ha på ett relativt enkelt sätt. Bland annat genom att kryptera enheten och installera programvaror för att motverka virus och skadlig kod samt tvinga användaren att ha enheten lösenordsskyddad. Med privata enheter finns inte längre den möjligheten, verksamheten kan uppmana användaren att skydda enheten men det är svårt att kontrollera och veta att det efterföljs. Följaktligen blir risken stor att information läcker ut ur enheten till obehöriga, exempelvis genom en skadlig programvara som skickar ut informationen till obehöriga. Vid en stöld eller förlust av enheten blir risken också stor att information kan utläsas om kryptering och lösenordsskydd saknas. Miller, Voas & Hurlburt (2012)

Trots att regler sätts upp för vilka applikationer som är tillåtna på en enhet så visar en undersökning gjord av Cisco (Anonymous 2012) att 69 % av BYOD användarna som var med i undersökningen använde otillåtna applikationer på sina enheter. Utan faktisk kontroll över enheten är det svårt att styra detta. Anledningen till att detta är ett problem beror på att det sker en explosionsartad ökning av skadlig kod i applikationer som är tillgängliga för nedladdning. Trend Micro rapporterade att under första kvartalet 2012 upptäcktes 5000 skadliga programvaror, under andra kvartalet 2012 hade antalet dubblerats till 10000, men då inte per kvartal utan per månad.

3.2.1 Autentisering, Verifiering och Godkännande

Kring säkerhetsfrågaor finns det några viktiga aspekter att ta hänsyn till. Ganett (2012) förespråkar att företag bör verka för att stärka upp sitt nätverk snarare än att förlita sig på tekniska lösningar. Det första som behöver göras är att försäkra sig om att användaren är vem den utger sig för att vara samt att den har rätt att komma åt det den begär.

Det första steget är autentisering, här räcker det inte med att endast ha användarnamn och lösenord, istället bör verksamheten använda minst två av följande tre identifierare:

- Information som användaren känner till, exempelvis lösenord.
- Någonting fysiskt användaren har tillgång till, exempelvis ett kreditkort, smart kort etc.
- En biometrisk egenskap såsom fingeravtryck, ansiktsigenkänning osv.

Nästa steg är verifiering, när användaren är autentiserad kan verksamheten med fördel använda sig av lokalisering för att ytterligare försäkra sig om att åtkomsten är godkänd. Det är

dock viktigt att dessa lokaliseringsdata inte går att manipulera, därför går det inte att använda GPS positions data ifrån enheten utan de behöver få tillgång till data ifrån nätverksoperatören som den anställde försöker ansluta ifrån.

Slutligen behöver företaget godkänna användaren för att se att den verkligen skall få tillgång till informationen den efterfrågar. Här kan en simpel tillgångshantering användas som bygger på åtkomstnivåer/grupperingar. Detta är den kanske vanligaste tekniken men det är inte alltid den är säker nog. Vill företagen utöver detta styra åtkomsten av data baserat på var användaren befinner sig behöver de matcha positionsdata med användarens åtkoms nivå för att på så sätt godkänna åtkomsten till informationen. (Ganett 2012)

3.3 "Hands on" och "hands off"

Beroende på hur hårt styrd en teknisk BYOD lösning är talar Caldwell, Zeltmann och Griffin (2012) om att kategorisera dem i kategorierna "hand on" och "hands off". Caldwell, Zeltmann och Griffin (2012) ser en "hands on" approach som en självklar del av att implementera BYOD i en verksamhet. Med hjälp av den tekniska lösningen Mobile Device Managment (MDM) får företaget ett kraftfullt verktyg för att tvinga användarna att följa policyn genom att låta enheter som inte styrs upp av MDM inte får åtkomst till informationen. Det är också här som nackdelen med "hands on" approach ligger, BYOD handlar i mångt och mycket om att låta användarna vara fria och att använda sina egna enheter på ett sätt de är vana vid. Som Scarfö (2012) uttrycker det, "ett företag som vill öka de anställdas produktivitet och reducera kostnader bör tänka på hur villiga användarna är till att ha sin egen enhet med deras privata data på när företaget har så hård kontroll på den som MDM ger". I en "hands on" lösning har problemet med vad som är företagets data eller den privata datan lösts genom en så kallad "remote wipes" vilket betyder att företaget kan tömma enheten på känslig information i händelse av att en användare slutar eller andra orsaker. (Caldwell, Zeltmann och Griffin 2012)

Motsatsen till en hands on approach är en hands off approach. Den kräver en del omställning vad gäller distribution av applikationer och information men ger i gengäld användaren friheten att använda sin enhet som vanligt och endast bli styrd av företaget när de begär åtkomst till applikationer och information som tillhör företaget. Det är ett effektivt sätt för att separera vad som är privat och vad som är företagsdata. En hands off approach som använder sig av virtuella skrivbord som användaren loggar in på verkar för att hålla arbetsrelaterad information inom det virtuella skrivbordet. Det uppnås genom att omöjliggöra eller försvåra för användaren att flytta eller kopiera informationen till enhetens privata lagringsutrymme. (Scarfö 2012)

3.4 Tekniska lösningar för hantering av BYOD

Olika tekniker dyker upp på marknaderna och vissa är vanligare än andra. Följande kapitel tar upp de identifierade möjliga lösningarna för hantering av BYOD. Teknikerna beskrivs med de viktigaste egenskaperna som är identifierade för att förstå hur de fungerar.

3.4.1 MDM – Mobile Device Management

Enligt Siddiqui (2012) som har jobbat många år med informationssäkerhet är MDM en lämplig lösning för verksamheter som vill få kontroll på de enheter som vill ha åtkomst till verksamhetens nätverk. Han säger att MDM är ett lätt och effektivt sätt att uppnå denna kontroll på. Det finns ett antal punkter som är typiska för en MDM lösning.

- Att användarens enhet själv utför en registrering.
- Har en certifikatbaserad autentisering för enheten.

- Enheten får en påtvingad policy som innefattar bland annat lösenord, tidsinställda enhetslås och fjärradering
- Containerisering
- Kryptering

(Siddiqui 2012)

Det är under den påtvingade policyn som MDM's kraftfulla verktyg *fjärradering* är placerad vilket de innebär att verksamheten får möjlighet att utan förvarning radera den informationen på enheten som tillhör verksamheten vilket även kan innebära att privat data raderas i de fall där verksamhetsdata och privat data blandats.

Alla ovan nämnda punkter handlar om både säkerhet, integritet och överensstämmelse. De första tre är bara fokuserade på säkerheten medan containerisering och kryptering täcker upp integriteten och överensstämmelsen genom att företagsdata lagras separat ifrån privat data samt att innehållet i enheten krypteras för att fungera skyddande ifrån brott, anmälningar och kundens krav. (Siddiqui 2012)

Stein (2012) skriver i en artikel i Network World att en MDM lösning ska täcka upp hela verksamhetens mobila säkerhet samt enheter, data och applikationslivscykler. Det finns några viktiga faser som bör ingå i en MDM lösning.

- Fas 1. handlar om etablering av enheten. Verksamheten låter enheten få ärva en persona som är en typ av profil som är bestämd av personalen som ansvarar för mobil IT och säkerhet. Här är syftet att använda sig av den befintliga infrastrukturen i företagets nätverk för att undvika dubbleringar och komplexitet i befintliga resurser.

- Fas 2. Här jobbar teamet för mobil IT aktivt för att hantera alla typer av enheter. Detta för att hålla koll så företagets personas inte förstörs. Det är i denna fas som användaren kommer åt företagets resurser så som applikationer, e-post, kataloger och fillagring. Här är det lämpligt att får reda på vilka regler som gäller så att användarna vet vad de får och inte får göra inne på nätverket. När enheten läggs till i verksamhetens MDM lösning blir verksamhetens personas påtvingade i enheterna för att användarna ska få komma åt resurserna.

- Fas 3. Nu är det dags för mobilt IT att hantera och ansvara över alla de applikationer som hör till företagsanvändarna. Det kan röra sig om ett stort antal olika applikationer, enheter, personas och operativsystem som ska skötas. MDM erbjuder en lösning där företaget kan ha ett bibliotek med företagsspecifika applikationer med den bästa säkerheten och slutanvändarens upplevelse.

En enhet ifrån Apple som är ”jailbreakad” eller motsvarande löper i sig inte en ökad risk för att infekteras av skadlig programvara såvida användaren fortsatt endast laddarn ner granskade applikationer ifrån leverantörens applikationsbutik. Problemet är att en ”jailbreakad” enhet har möjlighet att installera ogranskade applikationer ifrån tredje part. På grund av detta erbjuder MDM möjligheten att detektera ”jailbreakade” enheter för att kontrollera om de frångår verksamhetens policy. (Network World 2013)

3.4.2 MAM – Mobile Application Management

MAM har till syfte att kontrollera enskilda applikationer och dess data genom att när en enhet ansluter sig till verksamhetens MAM verktyg ges verksamheten ett par huvudsakliga

möjligheter. Dessa innefattar installation, uppdatering, borttagning, konfigurering och uppsäkring av verksamhetens applikationer med tillhörande data.(Techtarget 2012a; Rouse 2012)
Eftersom den anställdes många gånger kopplar upp sig på vanligt bredband och Wi-Fi behöver MAM undvika att dra för stora nätverksresurser. Detta görs genom att ta hänsyn till nätverks bandbredd. (Rouse 2012)

Gruman (2011) säger att företagen börjar släppa det hårda greppet om enheten och istället börjar se dem som en gemensamt ägd enhet med användaren. Det är företags applikationer som verksamheten vill kunna kontrollera. Genom att verksamheten får kontroll över deras egna applikationer kan de ta bort data ifrån enheten ifall den försvinner eller om den anställde slutar.

MAM skiljer sig ifrån MDM på huvudsakligen en punkt; IT avdelningen har ingen insyn i den privata data som är lagrad på enheten, de har endast möjlighet att styra säkerhetsaspekter relaterade till specifika verksamhetsapplikationer. Genom att kapsla in enskilda applikationer i en virtuell box kan IT avdelningen säkra upp den specifika applikationen till den nivån de vill lägga säkerheten på och användaren får åtkomst till dem genom att identifiera sig med exempelvis ett lösenord. (Scarfö 2012) De applikationer som finns i den virtuella boxen kan kontrolleras, övervakas och hanteras av företaget vilket påminner om MDM. Skillnaden är att MAM håller sig till det som finns inom den virtuella boxen. Resultatet blir en tydlig separation mellan arbete, privata applikationer och data. (Gruman 2011)
Fler skillnader mot MDM är att MAM fokuserar på mjukvara leverering, licensiering, konfigurering, underhåll, spårning av användning och påtvingande av applikations policy (Rouse 2012).

En verksamhet kan ha krav på att en enhet skall ha en uppsättning applikationer som är en blandning av egenutvecklade och publikt åtkomliga. MAM ger möjligheten att exempelvis skicka ut de privat utvecklade applikationerna trådlöst samtidigt som användaren skickas en uppmaning om att installera publikt åtkomliga applikationer snarast för att enheten skall ses som godkänd och säker på nätverket. (Techtarget 2012a) MAM hjälper även till att hålla koll på vilken användare och enhet som installerat vilken applikationspaket och version, vilket hjälper IT avdelningen att till exempel ha koll på vilka som ännu inte har installerat nödvändiga program. (Rouse 2012)

Det finns vissa MAM som kan jobba proaktivt med att applicera och påtvinga applikations policys. Detta kallas ofta svart och vitlistning av applikationer (Rouse 2012).
Svartlistning av applikationer fungerar genom att en lista med otillåtna applikationer sammanställs. När användaren försöker installera en applikation på enheten kontrolleras den först mot svartlistan innan installationen slutförs. Applikationerna på listan kan vara svartlistade på grund av att de innehåller skadlig kod men också på grund av att verksamheten anser att vissa legitima applikationer kan skada verksamheten på annat sätt. Svartlistan måste uppdateras och underhållas allt eftersom det kommer ut nya applikationer som behöver förbjudas. Den rådande meningen kring denna metod att reglera vilka applikationer som tillåts är att det är omöjligt att säkerställa att inga skadliga applikationer slinker förbi. Det kommer ständigt nya uppfinningsrika sätt att skada enheter på och listan kan uppdateras först efter att dessa har upptäckts och identifierats. (Techtarget 2012b)

Vitlistning av applikationer fungerar på motsatt sätt, istället för att sammanställa en lista på otillåtna applikationer listas samtliga applikationer som har verksamhetens godkännande. Alla

övriga program är således inte möjliga att installeras. Detta innebär givetvis att applikationsurvalet blir betydligt mer begränsat än vid användning av svartlistning men samtidigt får verksamheten en helt annan möjlighet att upprätthålla kontrollen över vilka applikationer som tillåts på enheten. (Techtarget 2012c)

3.4.3 VDI – Viritual Desktop Infrastrukturer

Viritualisering av verksamhetens tjänster, genom att låta användaren ansluta till verksamhetens tjänster och interna nätverk genom en VDI klient elimineras möjligheten för användaren att kopiera över filer ifrån arbetsytan till enheten. Den här tekniken skickar aldrig någon egentlig information till enheten, istället är det en ström av pixlar, liknande en video som användaren interagerar med vilket ur ett säkerhetsperspektiv är mycket bra då manipulering och extrahering av data till användarens privata ytor på enheten blir nära på omöjligt. Det finns möjlighet att tillåta kopiering av text och filer ifrån den virituella enheten till klienten. Denna egenskap kan också avaktiveras för att öka säkerheten(MyViritualCloud 2011). Enheten som ansluter kan ses som ett tangentbord och en skärm för att styra det användaren ansluter sig emot, den blir med andra ord en tunn klient. Anslutningen till det virituella skrivbordet skall vara krypterad för att data som skickas skall bli obrukbar i fel händer. (Marko 2011; Scarfö 2012)

På grund av att alla beräkningar som görs i den virituella miljön utförs på VDI servern möjliggörs att beräkningstunga applikationer, som inte skulle vara möjliga att köra på klientenheten, flyter på i hög hastighet då det ofta finns gott om beräkningsresurser i servern. Detta är också en baksida med VDI, det kräver stora investeringar vad gäller hårdvara för att klara av att hålla uppe hastigheten när många klienter ansluter sig för att arbeta. (Harbaugh 2012)

VDI gör att upplevelsen av exempelvis ett Windows skrivbord som viritualiseras ser exakt likadant ut oberoende av om du väljer att ansluta med exempelvis en annan Windows dator, en Mac, en iOS enhet eller en Android enhet. Detta är dock inte idealiskt då de nu vanligaste Windowsversionerna inte är avsedda att användas med ett touch gränssnitt. Det har utvecklats olika verktyg för att underlätta bristerna i gränssnittet men de är långt ifrån optimala.(Knuth 2012)

3.4.4 Containerization

”Containerization” handlar om att en del av enheten avgränsas och säkras upp för att skydda verksamhetsrelaterade applikationer och data som lagras där, en så kallad container (Mitchell 2012).

Det finns tre huvudsakliga varianter på ”Containerization”, krypterade mappar, applikationsikapsling, coh mobile hypervisors. Dessa beskrivs nedan.

Krypterade mappar

Applikationer och data placeras i ett avgränsat och krypterat utrymme. Det som befinner sig inom det krypterade utrymmet är isolerat ifrån övriga applikationer åt båda håll. Här kan verksamheten installera och tillhandahålla egna applikationer för exempelvis mailhantering eller en säker webbläsare för åtkomst till intranätet. IT-avdelningen kan på avstånd radera innehållet i det krypterade utrymmet för att på så sätt skydda data från att komma i orätta händer vid exempelvis förlust av enheten. (Mitchell 2012)

Applikationsinkapsling

Till skillnad ifrån krypterade mappar syftar den här tekniken till att kapsla in enskilda applikationer. IT-avdelningen får möjligheten att applicera olika policys anpassade till verksamhetens säkerhetsbehov för respektive applikation. Möjlighet finns även här för IT-avdelningen att på avstånd radera de inkapslade applikationerna tillsammans med dess tillhörande data. (Mitchell 2012)

Mobile hypervisors

En mobile hypervisor skapar ett separat viritualiserat operativsystem på enheten och körs samtidigt som det vanliga operativsystemet men är helt isolerat ifrån det. De båda operativsystemen har sina egna applikationer, policys och filsystem. Det viritualiserade systemet styrs av IT-avdelningen medan det andra styrs av användaren som vanligt. Flera viktiga administrationsmöjligheter finns, exempelvis “remote wipe” och låsning av den virituella enheten när IT-avdelningen ser behov av det. Mobile hypervisors ger även möjlighet påtvinga lösenordsskydd. (Mitchell 2012; VMware 2013)

Då det virituella operativsystemet stödjer vanliga applikationer erhålls en användningsupplevelse som är korrekt till operativsystemet. Applikationer kan installeras, uppdateras och avinstalleras på distans, det finns även möjlighet att konfigurera dem innan de pushas ut till användarna.(VMware 2013)

3.4.5 NAC - Network Access Control

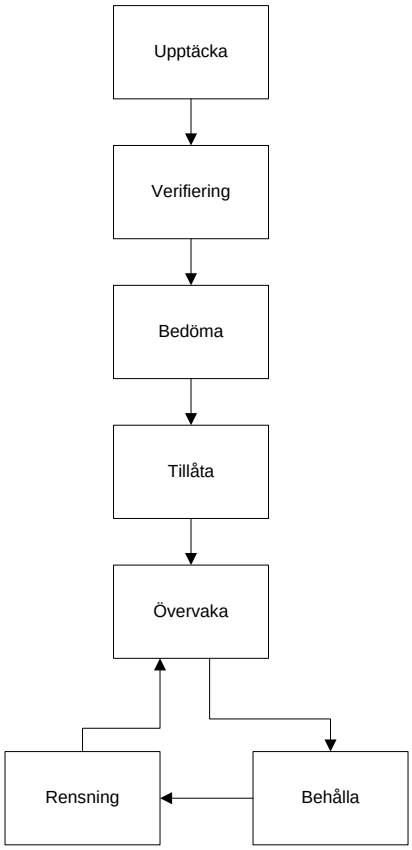
Företaget Enterasys secure networks är ett världsledande företag som levererar både trådbundet och trådlös nätverksinfrastruktur samt säkerhetslösningar. De gör en väldigt bra basbeskrivning kring vad NAC är för något samt hur den skall fungera som bäst.

En NAC lösning har till syfte att använda sig av identifiering, kontrollering och säker access för att skydda tillgången till nätverket och företagets tjänster. NAC lösningen ska jobba proaktivt för att hantera både tillitliga användare, gäster och enheter som försäker logga in på nätverket, samt hantera vad de är auktoriserade för att få lov att göra online.

NAC’s tre huvudsakliga uppgifter säger Enterasys i sin artikel Enterasys Secure Network (2008) är registrering och auktorisering av nätverksuppkopplade slutsystem samtidigt som den ska skydda nätverket mot virus och även fungera som en portvakt för kontroll av hur slutsystem och gästsystem får logga in på nätverket.

Nedan i figur 4 visas ett flöde hur en väl arkitektur med NAC borde fungera och vilka viktiga delar den skall innehålla.

- Upptäcka: Upptäcker och identifierar en ny enhet som kopplas upp emot nätverket.
- Verifiera: Verifiering av både användaren och enheten som kopplas upp.
- Bedöma: Bedömning av slutsystemet vad gäller dess efterlevnad och sårbarhet.
- Tillåta: Ger tillstånd för användaren att använda nätverket beroende på resultatet ifrån verifieringen och bedömningen från tidigare steg.
- Övervaka: Övervakning av användare och enheter när de är uppkopplade på nätverket.
- Behålla: Placera problem, slutsystem och användare i karantän för att hindra dem från att negativt påverka den totala nätverksmiljön.
- Rensning: Sanering av problem med slutsystemet eller användaren.



Figur 4. NAC olika funktioner. Egen översatt bild ifrån Enterasys Secure Network, 2008

Upptäck och verifiera
Här gäller det för systemet att identifiera vem det är som försöker koppla upp sig mot nätverket samt var den befinner sig. Det system som används för att verifiera användaren eller enheten används också för att på bästa sätt identifiera slutsystemet. Att använda sig av MAC och IP adresser ger bara en kortvarig identifiering då dessa kan bytas ut på mindre än två minuter.

Det finns flera lämpliga tekniska metoder för att hantera identifiering och verifiering av enheter och användare som vill logga in på nätverket. För att välja en lämplig lösning bör företaget ta reda på vilken form av verifiering som stöds av slutsystemet.

Bedömning av slutsystemet
Enterasys Secure Network (2008) ser bedömningen av slutsystemet som en så kallad hälsocheck där företaget kan använda sig av två olika vägar. Antingen agentlös eller agentbaserad metod.

Den agentlösa metoden fungerar genom att många manuella tester över nätverkssökningar automatiseras och utförs av en centraliserad server i nätverket. Detta blir det naturliga valet ifall företaget inte kan ha agenter, vilket resulterar i att metoden gör det möjligt att scanna många fler enheter som finns i en NAC implementation. Fler fördelar är att det går snabbt att implementera, ger täta signaturuppdateringar och omfattande tester. Resulterar även i detaljerad kundinformation och en hög slutsystemskompatibilitet. Det som dock talar emot en

agentlös metod är den begränsade skalbarheten, de tidskrävande skanningarna och den höga belastningen på nätverket.

En agentbaserad metod betyder istället att det är en form av mjukvara som körs på slutsystemet och resulterar i en hälsoinformation om slutsystemet och som även kan skydda emot hot. Den agentbaserade metodens största fördelar är att den har direkt access till kundinformation, jobbar med förebyggande åtgärder, har en god skalbarhet, bra lastbalansering och korta söktider. Det som däremot är mindre bra är slutsystemskompatibiliteten, då det oftast bara finns en leverantör och den ger en stor konfigurations ansträngning.

Tillåta
Efter att användaren tagit sig igenom de ovanstående stegen är det nu som de access-regler som bestämdes i början ska appliceras. Systemet avgör nu vad den inloggade enheten skall få tillgång till. Även här finns det olika system för att hantera vad som är tillåtet och valet av system är beroende på nätverkets prestanda och vilka förutsättningar NAC lösningen har. Det kan även spela roll om vilken nivå av önskad säkerhet som företaget har samt designen på infrastrukturen.

Övervaka
Här handlar det om att övervaka den enhet och användare som är uppkopplad på nätverket. Det sker en bedömning vid olika intervaller med hjälp av agent eller kontroll skanning av slutsystemet.

Rensning
Enterasys Secure Network (2008) talar om vikten av att ha ett rensningssystem integrerat i lösningen. Finns inte ett sådant är sannolikheten stor att NAC kommer blockera alla slutsystem som försöker komma åt nätverket och de tjänster som slutsystemen egentligen ska få tillgång till. Ett bra rensningssystem bör vara automatiserat vilket resulterar i en bättre rensningsprocess som ger mindre administrativt jobb.

3.5 Sammanfattning

Efter genomförd teoriinsamling har det blivit möjligt att besvara de tre delfrågorna som ställdes under kapitel 1.4.
Den första frågan var den mest grundläggande och hade till syfte att skapa förståelse för vad BYOD innebar.
Vad innebär begreppet Bring Your Own Device (BYOD)?

> BYOD handlar om att den anställde tar med sig sin egen enhet för att utföra arbetsrelaterade uppgifter på. Begreppet har uppkommit ifrån konsumentisering (Kapitel. 3.1).

Den andra delfrågan var teknisk inriktad med syfte att ta reda på vilka som var de mest förekommande teknikerna för att implementera BYOD i dagsläget.
Vilka tekniska lösningar finns det för implementering av BYOD?

> De som har identifierats och som nämns mest i teori är MDM, MAM, VDI, Containerisation och NAC (Kapitel 3.4).

För att kunna besvara huvudfrågan behövde vi även ta reda på vad det fanns för behov angående BYOD både utifrån verksamheten och användarnas perspektiv.

Vilka huvudsakliga behov har verksamheten och användarna vid införande av BYOD?

> De vanligaste behoven som i många fall även ses som hinder för införandet av BYOD är bibehållen säkerhet, separation mellan privat data och företagsdata, rimlig nätverksbelastning, bibehållen kontroll för användaren av sin privata enhet, och låga implementationskostnader. (Kapitel 3.1)

4 BYOD i praktiken

I detta kapitel presenteras den empiri som samlats in under en intervju med Jonas Toftefors på Mölnlycke Health Care.

4.1 Upplägg och struktur

Intervjumaterialet redovisas med huvudrubriker som sammanfattar texten för att identifiera kriterier som Mölnlycke Health Care har funnit viktiga för valet av teknisk lösning. Texten är en sammanfattning av intervjun och materialet har grupperats ihop kring områden som hörde ihop och var relevanta för kriterierna. Intervjufrågorna som användes finns att hitta under bilaga 1.

4.2 Beskrivning av företaget och respondenten

Intervjun ägde rum ute på Mölnlycke Health Care på deras kontor i Gamlestan Göteborg med Jonas Toftefors. Mölnlycke Health Care är ett företag inom sjukvården och tillverkar textilprodukter och sjukhusutrustning med avancerad teknik.
Jonas sitter med i Enterprise Architecture (EA) gruppen på företaget, med två olika roller, det ena är EA board där de godkänner alla förändringar som har med IT-plattformen att göra samt IT-leverans ur ett större perspektiv. Det handlar inte om att göra förändringar i ett system utan det handlar om att föra in nya system, ta bort system, förändra funktion för system, ändra verksamhetens tekniska plattform i form av nätverk, infrastruktur, klienter i form av mobila enheter och liknande. Där ingår representanter ifrån IT, verksamhet, och lite olika processer som ser till att koncernen får så stor nytta som möjligt av de pengar de stoppar in i IT. Eboard fattar inte alla beslut utan det finns en IT-styrgrupp som är mer ekonomisk. Den här är mer beslutande om förutsättningar att det här passar in eller inte passar in, är mer en rådgivande funktion för det mer formella beslutet. Eboard har ingen formell makt men en rekommenderande som tas på stort allvar i de beslutande forumen. Allt har ju en prislapp, om företaget har alternativ A och alternativ B, med alternativ A når företaget 80% av vägen men den kostar bara en tiondel av alternativ B då kan det fortfarande bli alternativ A även om B var rekommenderat av Eboard.
Den andra rollen som Jonas har är som arkitekt, han förbereder inför ovan nämnda mötena för att kunna presentera olika scenarier mot varandra. Funktionen heter ASI – Architecture Security and Innovation så där hamnar även säkerhetsfrågor och det är rätt bekvämt med tanke på att arkitektur och säkerhet är rätt starkt förknippade med varandra. Innovation delen är egentligen att facilitera innovation, det går ju inte att säga till tre människor att ni skall vara innovativa, det är ju inte så det fungerar, det handlar istället om att skapa en kanal där verksamheten kan ta tillvara på innovativa idéer som uppkommer på ett ställe.

4.3 BYOD på företaget

4.3.1 Drivpunkt till behovet att hantera BYOD

Jonas säger att för det första är det väldigt få som tar med sin egen enhet utan de jobbar främst för att bemöta ”olle i grind” efter mycket diskussioner och skriverier om BYOD på nätet så det var mest att möta en potentiell fara. I företaget finns det totalt 7500 anställda och de känner till att de är färre än 100 egna enheter som används i företagets nätverk. Det är en väldigt liten del, mindre än 2%. Mätningar av användningen har gjorts men utan att se en ökning av BYOD och det är alltid entusiasterna som tagit med sina egna enheter, även innan företaget var medvetna om det. De anställda har haft åtkomst till nätverket tidigare genom användande av domännamn för att logga in på nätverket. De kan mata in domänuppgifterna på sin egen telefon, det är inget företaget kan hindra, men nu har företaget fått upp ögonen för

BYOD.

Med en egen dator, så kan den anställde logga in på nätverket. Företaget har kontroll på att någon varit inne men det finns inte några krav på att specifika säkerhetsapplikationer eller inställningar skall vara installerade på datorn för att den skall få tillgång till nätverket. Däremot, för att kunna köra på vårt interna nätverk behövs ett certifikat installerat och det certifikatet har ju inte användarna, vilket gör att dessa inte kan köra en applikation, inte ens direkt mot SQL servern utan det här certifikatet, men du är inne på nätverket. Certifikatet går inte heller att kopiera över från sin jobbdator till sin privata utan det måste göras en request ifrån en dator och då knyts den dit. Den anställde kommer inte heller åt vårt produktutvecklingssystem utan det är olika svåra nivåer. Intranätet är ju inget hemligt på det sättet utan det är något alla i hela företaget kommer åt i hela världen.

När det gäller datorer ser Jonas att hybridplattorna som är både dator och platta på en gång, till exempel win8 plattor är något som tas med av de anställda. Annars tar de inte med sina privata bärbara datorer. Företaget distribuerar applikationer genom grupp policys och genom grupper i active directory (AD). Genom att din privata dator inte är registrerad i AD så får de inte applikationer de anställda behöver för sina jobb. Det är någonting företaget uttryckligen sagt, men de köper inte en Visio licens och installerar på en anställds privata dator för det innebär ju egentligen att företaget betalar en licens de egentligen inte äger, vilket inte gör det så attraktivt då den anställde skulle behöva köpa programlicenserna själv. Eller, här får du en dator som är max 2,5 år gammal med alla program installerade, det väger ju givetvis över.

4.3.2 The buisness case kring BYOD

Det som är intressant och som företaget tittat väldigt mycket på är: ”Vad är buissnes caset för BYOD?” Företaget har kommit fram till att det helt enkelt inte finns ett buissnes case ur företagets synvinkel på BYOD. Företaget köper in en iPhone för 4000-4500:- och betalar ingen moms, skall den anställda ta med sin enhet och betala den anställda för det då blir kostnaden istället 9-10.000 för något som företaget i slutändan inte äger. Det är inte lätt att motivera. Dessutom måste företaget skapa många applikationer som leder till ökade supportkostnader. Företaget ser alltså inte ett egenvärde i att betala användarna för att dessa skall ta med sina egna enheter. Det verksamheten ser är att låta de anställda som har ett brinnande intresse ta med sina privata enheter, men utan ersättning. Tar användaren med sig en enhet som inte är supportad av verksamheten genom att de själva delar ut den typen av enheter kan användaren inte förvänta sig att det finns fullt stöd för den enheten i verksamhetens applikationer. Dessutom kan användren inte förvänta sig att företaget ger någon support på enheten.
Det företaget ser som en business case i BYOD är att det är en speciell typ av mäniskor som vill gå sin egen väg och vill ha sina egna grejer. Ofta är det ganska kreativa mäniskor och att knyta dem till sig genom att underlätta för dem, det är där vi ser affärssvärdet. Tittar på det rent ekonomiskt och att det inte ger något mervärde för personen så finns det inget buissness case.

4.3.3 Tankar kring BYOD

Mölnlycke Health Care finns i många länder bland annat i Tyskland som har ett extremt kraftigt personuppgiftslagen (PUL) jämfört med Sverige. Där får företaget inte kontrollera den anställdes enhet särskilt mycket, tyskarna har en egen text när företaget registrerar enheten i MDM, med många ifrånsäganden. Jonas är osäker på om de har några privata enheter i Tyskland utan det är vanligt främst i norden, och i USA, som har en annan kultur. Det har inte alltid varit självklart att arbetsgivaren där betalat bärbara enheter som exempelvis

telefonen åt den anställde.

Skulle man slumpmässigt fråga 100 personer så skulle antagligen 97 av dem rycka på axlarna och fråga sig varför de skulle ta med sin egen enhet när de får en av företaget. Det är väldigt populärt just nu.

I arbete måste Jonas alltid sätta allting i relation, de jobbar mycket riskbaserat och lyder under massa komplicerade lagar gällande läkemedel. Det är därmed väldigt viktigt att informationen vad gäller läkemedel har rätt version och är godkänd. Det medför att det är viktigt att hålla koll på företagets information. Det är viktigt att ha en balans mellan åtgärder företaget tar och vad de försöker skydda sig mot.

4.4 Den tekniska lösningen för BYOD

Jonas anser att BYOD är väldigt tätt sammanknuten med Bring Your Own Behavour, att det inte bara har med enheter att göra utan även beteendet den anställde tar med sig. Denna fråga har diskuterats på företaget och de har löst den genom att skapa en teknisk förutsättning för att ta med sin egen enhet, de har infört ett system som heter Afaria som är den device manager som i princip går ut på att de skapar ett område på den anställdes enhet som är företagskontrollerat, för att kunna använda företagets applikationer behöver den anställde registrera sin enhet, det vill säga att den ansluter till en gateway som då talar om att nu är delar av den här enheten kontrollerad av företaget och den ytan som är kontrollerad kan då fjärr radera och fjärradministrera, men den anställde har fortfarande kvar en privat del av enheten.
Det är en MDM lösning och det som är bra med den är att företaget har skapat upp ett antal policys kring vad företaget gör och inte gör. För plattformen Afarias MDM lösning kan göra väldigt mycket, precis vad vi vill med telefonen trots policyn och där har det varit ett stort arbete för oss att få en etisk balans. De har inte gjort någon undersökning, men tror att tilliten i alla fall är hög inom Sverige.

4.4.1 Varför valet av MDM

Anledningen till att företaget valt just Afaria är att de har en stark backbone i SAP och Afaria är väldigt bra att integrera med SAP. Det de har gjort i Afaria är att lägga på en påtvingad policy globalt som omfattar ganska lite information, men sen tillåter de respektive marknad att lägga till saker vilket gör att man till exempel i Tyskland kan anpassa till lokala regler.
Möjligheten att kunna marknadsanpassa är ytterligare en anledning till valet av Afari.

Företaget använder ytterligare en plattform som heter SUP som är en modul i SAP som står för Sybus uncoppled platform. SUP är en existerande programvara som är köpt och som håller på att döpas om till SAP mobility platform. Det är ett verktyg för att ge data till applikationer i och med att de har väldigt mycket data i SAP så kan företaget alltså här bygga verktyg för att kunna ge data till devices ifrån SAP. Alla devices oavsett Android eller iOS pratar med SUP som då i sin tur har en kanal ner till SAP vilket gör att företaget slipper bygga ett interface mot SAP för varje teknik utan då kan alla enheter ansluta mot SUP.
De största kostnaderna i dagsläget är kopplingen mellan SAP och SUP. Därför är det bra att bara bygga den anslutningen en gång och sedan återanvända den till samtliga enheter.

De övervägde andra lösningar än MDM, de tittade bland annat på en moln tjänst. Anledningen till att de valde denna var dels kopplingen mot SAP och SUP och att ramverket hänger ihop i ett ekosystem vilket ledde till att det var minimalt med integrationer för företagets del. Det var i princip att installera och trycka på play så det var enkelheten som

avgjorde det.
Företaget har en princip som heter balanced security som innebär att man tittar på hur stort det verkliga hotet är jämfört med andra hot. Det är onödigt att lägga miljontals kronor på att förhindra något som folk ändå gör med papper. Då spelar det ingen roll hur väl systemen skyddas anser Jonas. Ta hänsyn till folks beteende, hjälp dem göra rätt istället för att hindra dem att göra fel. Det är essensen i företagets arbetssätt.

4.4.2 Regler kring MDM

Det företaget övervakar i enheten är i princip bara de företagsapplikationer som ligger på enheten, dvs. de kontrollerar inte kontakter, samtalslistor och epost som inte går igenom företaget. Har den anställde sitt eget Gmail konto tittar de inte på det utan det är enbart hur de arbetar med företagets information i företagets applikationer och det är framförallt för att skapa tillit hos användaren. De har satt upp ett regelverk för att om företaget ger användaren exempelvis en iPhone så måste den vara registrerad i MDM verktyget medan är det en privat så kan de inte tvinga en anställd att registrera den vilket de inte heller vill. Däremot är det enda sättet att komma åt företagets applikationer då det är först då som den anställde kommer åt shopen där applikationerna finns. Om den anställde vill använda sin egen enhet finns inget tvång att använda MDM men det är väldigt praktiskt för annars kommer de inte åt applikationerna.
Det går att få gåståtkomst till nätverket, men det hjälper inte den anställde mycket. Som en bonus så får den anställde när väl enheten är registrerad i MDM, automatisk uppkoppling till gästnätverket. Företaget vill att detta skall vara ett incitament och en fördel med att registrera sig. Det är alltså applikationsåtkomst, automatisk inloggning samt exempelvis trackning som den anställde vinner på att registrera sig.

De tittar även på om enheten är ”jailbreakad”, det är en del i registreringen, den kontrolleras dels vid installation och dels vid varje startup.
Företaget köper in iOS samt Samsung Android enheter till de anställda på grund av att de där kan kontrollera att användaren inte kan installera tredjeparts applikationer utanför applikationsbutikerna.
Viktigt gällande applikationer är att de initialt har haft tillstånd per applikation och nu går över mot tillstånd per informationstyp. De går över till informationsklassning av applikationen snarare än en applikationsklassning. Till exempel så har de sagt det att ”profit och margins”, ”det kommer du inte åt från en mobil enhet över huvud taget”. De har pratat om att reglera vad den anställde får använda var någonstans, men det lades ner,av det enkla skälet att har den anställde en telefon, då används den där de är. Det går inte att komma ihåg var applikationen får användas.

4.4.3 Säkerhetstänk

Med iOS och Windows phone kan företaget med MDM tvinga enheten att vara lösenordsskyddad, skulle användaren ta bort lösenordsskyddet känner MDM av det och spärrar då åtkomsten till företagsnätverket, på en Android enhet däremot har företaget inte möjligheten att tvinga på lösenordsskydd på alla tillexempel HTC, men det går på Samsung.

4.4.4 Hantering av lagring av företagsdata

Filmar den anställde något med sin privata kamera kan företaget inte gå igenom den enskilda anställdas enhet, de kan sätta upp en policy om att de inte är tillåtet att göra det men vad är det då för vits med att ha en egen enhet? De försöker få de anställda att använda företagets verktyg box.net, ungefär som Dropbox, fast ur företagsperspektiv. De kan från företaget stänga av och sätta på dropboxen och även då dra tillbaka filer som är felaktiga. Detta styrs

genom att säga till de anställda att har ni företagsdata skall det lagras där. Inte lagras på lokala filsystemet i telefonen utan det skall lagras i box.net, då får den anställde skyddet ifrån företaget genom att om enheten tappas bort kan den dels stänga av, men också även stänga av box.net kontot eller göra det oåtkomligt tills det rett ut sig. Om den anställde filmar kan de välja att spara det i box.net direkt vilket gör det tillgängligt på enheten men skyddat av företaget. Det kan aldrig styra rent tekniskt utan det handlar ju om en tillit till sina kollegor. Företaget har märkt att de anställda behåller sina Dropbox konton men att de flyttar över sin företagsdata till box.net eftersom de själva vill ha kontrollen över var de kan lagra vad. Det som är bra med box.net är att de erbjuder klienter till allt den anställde kan tänka dig och de är snabba med att komma med uppdateringar så fort det kommer ut ett nytt operativsystem. Det finns även ett obegränsat antal med lagringsutrymme.

Vad som sparas var är svårt att hantera när företaget ska ta hänsyn till hela enheten. Det är kameran och mikrofonen som inte går att hantera. Det är tekniskt omöjligt att skilja på privat och arbetsrelaterat material. GPS täckning är också svårt och hanteras med en policy. På telefonen finns även den del som är Afaria kontrollerad. Där ligger alla applikationer som kommer ifrån företagets appstore, de har en egen appstore för både Android och IOS. De installeras inom Afarias kontroll. Den anställde har en katalogstruktur på sin telefon och den skapa ett eget träd där allt i det trädet är kontrollerat av företaget. I iOS fall är ytan inte krypterad men det är den på android. I och med att applikationerna ligger i utrymmet kan de inte komma utanför det, i vissa fall finns det funktioner i apparna för att bifoga en bild, men den bilden sparas i den kontrollerade ytan så fort den är kopplad till appen, men den kan fortfarande ligga kvar utanför. De har dock valt att inte spärra kopiering ifrån ytan till övriga delar av enheten då många användare behöver kunna använda applikationer utanför ytan i sitt arbete. Säljarna använder applikationer som både ligger i och utanför den kontrollerade ytan eftersom det i dagsläget inte finns så många applikationer i den arenan. Enda skillnaden med MDM på en företagstelefon jämfört med MDM på en privat är att de på en företagstelefon kan radera all information på hela enheten, det kan de inte göra på en privat.

4.4.5 Marknadsföring av BYOD på företaget

Företaget har inte gått ut med att de anställda får ta med sig egna enheter utan frågar någon får de reda på det. Det beror på att det är en kostnad förknippad med BYOD som support osv. De anser att det blir för många frågor från anställda som inte kan tekniken. Anställda som är intresserade av att köra sin egen enhet har ofta så gott tekniskt kunnande att det inte blir något problem.

4.4.6 Policy hantering

Företaget har olika policys rörande BYOD, en som omfattar hanteringen enrolled enheter, och en som reglerar hur den anställde använder sin enhet, inklusive laptop och liknande. När en anställd registrerar en privat enhet får de många fördelar som de försöker trycka på som det viktiga, den anställde skall vilja enrolla enheten för att få automatisk uppkoppling till nätverket och alla dess möjligheter. Företaget eftersträvar att jobba med morot istället för piska.

4.4.7 Problemområden

Det som företaget har under uppsikt är vad som händer med device marknaden, kommer det fortsätta vara den nivån det är kommer de inte göra mer åt detta, men om det blir en ökad grej då får de diskutera vad de skall stödja. Företagets stora dilemma idag är applikationerna, de har ett tiotal idag som kostar pengar, det kostar att bygga dem och deploya dem. Den kommer IOS7, vad händer med dem? Behöver vi bygga om och redeploya dem? Skall vi verkligen

uppdatera applikationen, vem har koll på det? På större system finns det livscykelplaner osv men på mindre system fungerar det inte så, de kommer ofta fram genom att en lokal marknad går till en reklambyrå som tar fram en applikation och därefter avsäger sig ansvaret för produkten. Ägarskapet och förvaltningen, hur vet företaget när de kan ta bort en applikation, när den är inaktuell? Där jobbar Jonas ganska mycket just nu. Det finns säsongsbetonade applikationer, därför är det svårt att titta på om en applikation inte används under en period för att avgöra om den är död, det kan vara så att den endast används vid några korta tillfällen varje år. De använder även webbappar med ett applikationsskal i vissa fall, men märkt att de inte efterfrågas av marknaden. Detta på grund av att de inte får samma naturliga upplevelse som en applikation.

4.4.8 VDI på företaget

Som virtuella skrivbord används Citrix skrivbord som den anställde kan komma åt utifrån men de är inte personliga utan den anställde loggar in på sitt Citrix skrivbord får de ett standard skrivbord baserat på sin profil, så om de kommer åt 4 applikationer så kommer de till ett tomt skrivbord där de 4 applikationerna ligger, de kommer fortfarande åt mina dokument och liknande men har de installerat något lokalt på sin dator kommer de inte åt det. Den anställde kommer med andra ord inte till den sessionen de jobbat med tidigare. Så de kan ju ta med sin egen dator, ansluta till gästnätverket och sedan jobba via mitt Citrix skrivbord, det är inga problem.
Det är likt ett windows klient, men ”virtuell”. Det har man haft i flera år och därmed slipper företaget hela problematiken då licensen ligger på Citrix plattformen och inte på den privata enheten. Ingen data på datan och ingen programvara.

Jonas tror mer och mer på det virituella skrivbordet, du har ett skrivbord som du kommer åt ifrån alla dina enheter men i olika kontext beroende på vilken du ansluter med. Det finns inte för telefoner i dagsläget vad han känner till, däremot för datorer finns det massa lösningar, exempelvis Citrix VM-ware osv.
Windows 8 kan fungera att ansluta en mobil enhet mot redan i dagsläget men det blir problem så fort den anställde exempelvis skall in i Word, det gränssnittet är omöjligt att hantera på så liten skärm.

Att få en ”virituell” på sin telefon är något Jonas önskar. Det som krävs är en annan typ av UI som anpassar sig till enhetens upplösning. Skalbart och inte fixerat likt Android och iOS gör. Nackdelen är att det kräver konstant uppkoppling såvida de inte har en liten krypterad off-line area som synkroniseras när användaren går online igen. Det finns klara praktiska problem för företaget när de har säljare som sitter i en källarlokal på Sahlgrenska med dålig mobiltäckning och skall presentera något. De har krav på att företagets lösningar skall fungera off-line på grund av detta.

4.4.9 Övriga tankar BYOD

Jonas tror att den tiden är förbi när IT kunde styra och ställa vad folk kan göra, de kan erbjuda ett bättre alternativ, vill de inte att kollegorna skall diskutera på Facebook, då kanske de får införa Jammer som är en produkt där de anställda kan diskutera i ett forum internt om de saknar de så företaget måste ju se varför folk gör som de gör, folk är inte onda av naturen utan de vill väl. Företaget måste ge dem förutsättningarna att kunna vilja väl.

5 Analys

Kapitlet presenterar en analys av den insamlade teorin och empirin. Först analyseras teorin och empirin för att få fram ett antal utvärderingskriterier, därifrån väljs sedan relevanta kriterier ut. Slutligen utvärderas respektive teknik utifrån de olika utvärderingskriterierna.

5.1 Upplägg och struktur

Analysen är utförd enligt den metod som beskrevs i kapitel 2.8. I analysen har först kriterier ifrån teorin och empirin identifierats, därefter har ett urval gjorts över vilka kriterier som skall användas för utvärdering av teknikerna. Efter beskrivningen av de utvalda kriterierna utvärderas respektive teknik för att redovisa hur de uppfyller kriteriet.

5.2 Utvärderingskriterier

För att kunna värdera och jämföra de olika teknikernas lämplighet i olika aspekter är det lämpligt att ta fram och analysera ett antal utvärderingskriterier som kan användas som en grund vid utvärderingen. Under kapitel 3.1 beskrivs fördelar och nackdelar med BYOD och kapitlet ligger till grund för de kriterier som identifierats ifrån den teoretiska referensramen i kapitel 5.2.1. Genom den empiriska undersökningen identifierades även de kriterier som var viktiga för respondentens verksamhet vid införande av BYOD i kapitel 5.2.2.

5.2.1 Identifierade kriterier ifrån den teoretiska referensramen

T1. Separation av privat data och företagsdata.

- Miller, Voas & Hurlburt (2012) påpekar att företagen ska hålla koll på separationen mellan företagsdata och privat data för att veta vad som tillhör vem. I kapitel 3.1 handlar denna om privat data och företagsdata blandas. Det är en ökad säkerhetsrisk när företaget tappar kontrollen över vart deras data lagras och finns tillgängligt.

T2. Möjlighet att kontrollera åtkomst av företagsdata.

- Risken att verksamhetsdata läcker ut ifrån en privat enhet, exempelvis vid stöld ses som ett hinder för implementation av BYOD. (Miller, Voas & Hurlburt 2012). Ytterligare ett exempel på det kan ses vid en uppsägning av en anställd som tar med sig känslig data till en ny arbetsgivare. Problemet nämns under kapitel 3.1 som ökade säkerhetsrisker. Miller, Voas & Hurlburt (2012) menar på att en företagsägd enhet oftast har en hög grad av påtvingad säkerhet medan det på den privata enheten kan vara svårare att påtvinga ett sådant skydd. Fler som instämmer med säkerhetsriskerna är Mansfield-Devine (2012), Anonymous (2012), Scarfö (2012) och Ganett Co (2012).

T3. Säkra upp enheten

- Howze (2012) hävdar att de flesta enheter saknar ett inbyggt skydd mot virus och skadlig programvara vilket utgör ett hot mot verksamhetens data och dess nätverk om de oskyddade enheter tillåts komma åt dem. Under kapitel 3.1 beskrivs detta som ökade säkerhetsrisker och att möjligheten att påtvinga ett virusskydd ökar säkerheten på enheten och således skyddet av företagsdatan.

T4. Hålla en så låg belastning på nätverket som möjligt.

- Mansfield-Devine (2012) säger att när en verksamhet tillåter BYOD finns det en stor risk att antal medhavda enheter ökar vilket ökar belastningen på nätverket och de anställdas jobb påverkas negativt när nätverket går trögt.

Under kapitel 3.1 beskrivs nackdelen högre belastning på nätverket vilket naturligt formar önskan om att tekniken bör hålla en låg belastning på nätverket som möjligt för att inte hindra verksamhetens dagliga arbete eller öka investeringskostnader i nätverksinfrastruktur.

T5. Användarna bör känna sig bekväma med vad verksamheten kan göra på enheten.

- Rymon (2012) säger att användarens privata enheter är mer än bara en elektronisk enhet utan är ett personlig anpassad verktyg som används för alla privata teknologiska sysslor. Därför värdesätter användaren att sin personliga integritet inte kränks. Kapitel 3.1 beskriver hur användaren tappar kontrollen över sin egna enhet vid BYOD.

T6. Hålla ner kostnaderna (maximera vinst)

- En BYOD lösning kan innebära många kostnader som tillexempel kostander för support och underhåll av enheterna. Även mjukvara och att uppdatera infrastrukturen kostar pengar. Detta beskrivs i kapitel 3.1 som gömda kostnader. (Brandel, 2012) Caldwell, Zeltmann och Griffin (2012) talar även om att företagens intresse ligger i att minska sina kostnader för att öka vinsten. En stor kostnad för företagen är teknologin. Genom att låta de anställda köpa in och underhålla sina egna enheter kan kostnaderna minska. Beskrivs i kapitel 3.1 som minskade kostnader.

T7. Nöjdare anställda

- Caldwell, Zeltmann och Griffin (2012) och Inghe (2012) tar upp att BYOD leder till nöjdare anställda eftersom de får jobba ifrån sina egna enheter och på så sätt blir flexiblare i sitt arbete och uppmuntras till att spontant arbeta utanför normal arbetstid samtidigt som de upplever sig som mera produktiva och effektiva. Kapitel 3.1 beskriver flexiblare arbete för de anställda, nöjdare anställda och ökad produktivitet.

5.2.2 Identifierade kriterier ifrån den empiriska undersökningen

E1. Implementationskostnader och integration med befintlig systemarkitektur

- Vid valet av teknisk lösning för hantering av BYOD var integrationen med den befintliga systemarkitekturen en avgörande faktor. Det minimerar arbetet och därmed kostnaden som behöver läggas på systemintegration vilket sänker den totala implementationskostnaden.(Kapitel, 4.4.1)

E2. Applikationsutvecklings-, underhålls- och support kostnader

- Kan en BYOD-lösning förenkla och minska kostnaderna för utvecklingen av applikationer ses detta som en stor fördel. Ett problem med BYOD anses generellt vara den stora variationen i de operativsystem och operativsystemsversioner som behöver stödjas av applikationerna. Skall applikationer utvecklas och testas för varje version ökar således kostnaderna. Supportkostnaderna anses också vara en viktig fråga. På samma sätt som för utvecklingen av applikationer så gör BYOD att många olika operativsystemsversioner finns i omlopp vilket kan öka pressen på supporten. (Kapitel, 4.4.7; 4.4.1 ; 4.3.2)

E3. Användbarhet

- Den tekniska lösning som väljs måste vara användarvänlig för att vara ett alternativ. En lösning som användarna inte kan använda är onödig. Det anses även viktigt att applikationerna som utvecklas till BYOD lösningen upplevs som ”native”, det vill säga att en applikation beter sig som de andra applikationerna förväntas göra på den typen av operativsystem som den körs på. (Kapitel, 4.4.8; 4.4.7)

E4. Marknadsanpassning av BYOD implementationen

- För att kunna ha olika regler och policys beroende på vilket land eller region användaren befinner sig i, anses det viktigt att det finns möjlighet att marknadsanpassa BYOD-lösningen. (Kapitel, 4.4.1)

E5. Känna sig trygga med vad företaget kan göra på enheten

- Vi ser att verksamheten lägger ett visst focus på att hitta en balansgång mellan vad verksamheten kan och får göra för att användarna skall känna sig trygga genom att implementera en policy som reglerar det. Däremot kan vi inte se att det görs några ansträngningar i att följa upp hur användarna känner sig. (Kapitel, 4.4)

E6. Skydda och kontrollera data på enheten

- Verksamheten vill ha möjlighet att skydda den verksamhetsägda data som lagras på enheten Detta kan bland annat uppnås genom att möjliggöra fjärrlåsning och fjärradering av enheten vid en rapporterad stöld eller förlust. Verksamheten ser det också som en nödvänlighet att kunna uppdatera enstaka filer på samtliga enheten vid exempelvis feltryck av en broschyr som säljarna använder. (Kapitel, 4.4.2)

E7. Säkra upp enheten

- Möjlighet att kontrollera att enheten uppfyller de krav på säkerhetsinställningar såsom lösenordsskydd eller att det inte skall gå att installera ogranskade applikationer tolkar vi som en nödvänlighet för att minska risken för att data skall läcka ut. (Kapitel, 4.4.2; 4.4.3)

E8. Åtkomstkontroll av applikationer

- Det är vikigt att det endast går att komma åt verksamhetens applikationer genom att ansluta den privata enheten till BYOD lösningen då det säkerställer att åtkomsten sker av en behörig användare. (Kapitel, 4.4.2)

E9. Separation av privat och verksamhetsdata.

- Lösnignar för att kunna separera verksamhetens data ifrån användarens privata data anses viktiga då det ger verksamheten möjlighet att kontrollera åtkomsten av sin data. Det anses dock till stor del vara användarens ansvar att lagra data på rätt ställe. (Kapitel, 4.4.4)

5.2.3 Urval av utvärderingskriterier

Ovannämnda kriterier från kapitel 5.2.1 och 5.2.2 har grupperats ihop om så var möjligt. Under respektive kriterie förs en argumentation kring varför det blev valt alternativt bortvalt baserat på stöd för kriteriet i empirin och teorin samt om det ligger inom uppsatsens avgränsning.

Utvalda kriterier

1. Separation av företagsdata och privat data (Kriterier T1, E9)
    - Både i empirin och teorin ges stöd för att dataseparation är en viktig faktor för säker BYOD hantering. Med anledning av detta har vi valt kriteriet för vidare analys.

2. Möjlighet att kontrollera åtkomst av företagsdata (Kriterier T2, E6, E8)
    - Kriteriet handlar om hur tekniken möjliggör radering av företagsdata samt hur tekniken kan hindra åtkomst av datan vid en eventuell stöld eller förlust. Både i teorin och empirin anses möjligheten att kontrollera åtkomst av företagsdata vara en viktig del i BYOD hantering. Med anledning av detta har vi valt kriteriet för vidare analys.

3. Säkra upp enheten (Kriterier T3, E7)
    - Kriteriet tas med eftersom empirin och teorin anser det vara viktigt att tekniken möjliggör uppsäkring av enheten för att ha kontroll på att enheten är vad den utger sig att vara och inte har några virus eller annan skadlig programvara installerad.

4. Hålla låg nätverksbelastning (Kriterium T4)
    - Här fann vi stöd i teorin att det kan bli problem med en ökad nätverksbelastning vid användandet av BYOD och verksamheten och användarnas arbete påverkas negativt. Därför är denna kriterie med bland de utvalda. Vi har dock inte sett något stöd för kriteriet i empirin men väljer ändå att ta med kriteret för vidare analys eftersom vi ser att det kan påverkar många olika faktorer inom verksamheten.

5. Användarna bör känna sig bekväma med vad företaget kan göra på enheten (Kriterier T5, E5)
    - Vi har identifierat att det främst i teorin, men även i empirin, finns stöd för att användarens personliga integritet är en viktig faktor vid implementering av en BYOD lösning. Därför väljs kriteret ut för vidare analys.

Bortvalda kriterier

1. Kostnad (Kriterier T6, E1, E2)
    - Både i den teoretiska referensramen och i den empiriska undersökningen ser vi att kostnadsfrågor är en viktig del i valet av BYOD lösning. Vi väljer dock att utesluta berörda kriterier då dessa inte ligger inom vår avgränsning för uppsatsen eftersom avgränsningen ligger åt det tekniska hållet.

2. Nöjda användare (Kriterier T7, T8, E3)
    - Kriteriet är svårbedömligt och subjektivt samtidigt som begreppet är mjukt. Vi väljer att utesluta berörda kriterier på grund av att uppsatsens avgränsning inte berör de mjuka aspekterna av BYOD.

3. Marknadsanpassning (Kriterium E4)
    - Vi kan inte hitta något stöd i teorin och vi anser inte att empirin själv är tillräckligt starkt argument för att marknadsanpassning är ett krav för verksamheter när de väljer BYOD lösning, så därför väljs detta kriterium bort.

5.3 Hur teknikerna uppfyller kriterierna

De utvalda kriterierna går vi igenom en efter en där varje teknik finns beskriven tillsammans med kriteriet för att på så sätt göra det lätt att följa med i texten och se hur varje teknik förhåller sig till kriterierna.

5.3.1 Separation av företagsdata och privat data

MDM – Mobile Device Management

Vi har inte identifierat någon hantering för separation av data. (Kapitel, 3.4.1)

MAM - Mobile Application Management

MAM sköter separering av företagsdata och privat data genom att placera företagets applikationer inom en skyddad virtuell box. Här kan IT avdelningen säkra upp sina applikationer genom att de kontrolleras, övervakas och hanteras, men bara de applikationer som finns inom den virtuella boxen. Detta resulterar i att företagsdata och applikationer hålls inom denna virtuella boxen och privat data och applikationer utanför. Detta betyder att om enheten försvinner eller den anställde slutar kan företaget rensa bort data och applikationer som tillhör företaget utan att behöva ta ställning till om det är privat data som försvinner eller inte. (Kapitel, 3.4.2)

VDI - Viritual Desktop Infrastrukturer

Separationen sköts genom att åtkomsten av verksamhetens applikationer sker i en miljö helt separerad ifrån enheten. Ingen egentlig information skickas till enheten, istället skickas en bildström vilket gör datan naturligt separerad. VDI har en funktion som möjliggör kopiering av data ifrån den virituella miljön till enheten, denna går även att blockera vilket ytterligare ökar separationen av privat och verksamhetsrelaterad data. (Kapitel, 3.4.3)

Containerization

Verkar för separation av verksamhetsdata och privat data genom att på olika sätt skapa isolerade containrar där verksamhetens applikationer och data lagras separerat ifrån de privata delarna av enheten. (Kapitel, 3.4.4)

NAC - Network Access Control

Eftersom NAC jobbar med att säkra åtkomsten till nätverket kan en användare, när den väl är inloggad, spara undan företagsrelaterad data var som helst på sin egna enhet och dessutom ihop med privat data. (Kapitel, 3.4.5)

5.3.2 Möjlighet att kontrollera åtkomst av företagsdata

MDM - Mobile Device Management

Kontrollen möjliggörs genom olika tekniker inom MDM. För att komma tillrätta med problemet med att skydda företagsdata ifrån en stulen, borttappad eller uppsagd anställds enhet kan MDM tillämpa fjärradering vilket innebär att IT-avdelningen kan radera data på distans utan att enheten har möjlighet att avbryta det. För att hindra åtkomst av data ifrån

obehöriga har MDM en möjlighet att kunna påtvinga ett lösenordskydd samt ett automatiskt skärmlås. (Kapitel, 3.4.1)

MAM – Mobile Application Management

Genom att användaren loggar in i den virtuella boxen med hjälp av ett lösenord får den tillgång till företagets applikationer och data. En MAM har full möjlighet att kontrollera den data och de applikationer som finns inom den virtuella boxen och kan då radera dessa, vilket hindrar obehöriga personer att komma åt företagsdata. (Kapitel, 3.4.2)

VDI - Viritual Desktop Infrastrukturer

För att få åtkomst till applikationer och data på den virituella miljön krävs det att användaren loggar in via en applikation. Eftersom verksamhetens data endast lagras på verksamhetens servrar har de alltid möjlighet att kontrollera den. Denna kontroll kan göras först och främst genom att blockera användarens åtkomst till den virituella miljön. Utöver åtkomstkontrollen kan verksamheten även radera användarkontot och därmed den virituella enheten med all dess data. (Kapitel, 3.4.3)

Containerization

Samtliga typer av containrar möjliggör fjärradering av containerns innehåll, för att på så sätt skydda innehållet vid exempelvis förlust, stöld eller uppsägning av en anställd. ”Mobile hypervisors” möjliggör låsning av den virituella enheten när IT-avdelningen ser behov av det. (Kapitel, 3.4.4)

NAC - Network Access Control

NAC kontrollerar åtkomsten av data genom sina huvudsakliga uppgifter som är att identifiera, kontrollera och säkra accessen till nätverket. Detta görs genom tydliga steg som användaren måste ta sig igenom, ett efter ett, innan den är inne på nätverket. Först genom en tydlig verifiering av både enheten och användaren avgörs ifall användaren blir insläppt eller inte samt vad den får access till när den väl är inne på nätverket. Under inloggningstiden bevakar även systemet användaren, så att den sköter sig och om reglerna inte följs hamnar användaren i karantän och systemet städar upp efter denne. (Kapitel, 3.4.5)

5.3.3 Säkra upp enheten

MDM - Mobile Device Management

När en användare registrerar sin enhet i MDM systemet finns det möjlighet för verksamheten att installera ett antal applikationer på enheten som till exempel ett virusskydd för att på så sätt säkra upp enheten. MDM kan sedan påtvinga policys för olika säkerhetsaspekter på enheten, exempelvis för att kontrollera så att virusskyddet inte är borttaget, om så är fallet finns möjlighet att blockera enheten från fortsatt anslutning till företagets nätverk. (Kapitel, 3.4.1)

MAM - Mobile Application Management

MAM har ingen möjlighet att påtvinga ett skydd, men genom sin svart och vitlistning av applikationer håller MAM en form av uppsäkring av enheten. Genom vitlistning av applikationer har företaget i förväg bestämt vilka applikationer som är säkra för användaren att ladda ner. Via svartlistning har företaget utformat en lista med applikationer som de inte tillåter användaren att ladda ner på grund av att dessa anses osäkra och kan skada företaget. När användaren försöker laddat ner en svartlistad applikation kontrolleras den emot listan och nedladdning avbryts. (Kapitel, 3.4.2)

VDI - Viritual Desktop Infrastrukturer

Det finns ingen möjlighet att säkra upp enheten med en VDI lösning då verksamheten inte får någon kontroll av enheten. Tekniken handlar enbart om en anslutning till en virtuell miljö, i vilken verksamheten har full kontroll. (Kapitel, 3.4.3)

Containerization

Teorin talar om att en krypterad mapp är helt isolerad ifrån det övriga operativsystemet. Med anledning av detta bör det inte finnas någon möjlighet att i den krypterade mappen applicera några säkerhetsapplikationer eller policys som skall verka över hela enheten. Applikationsinkapsling möjliggör installation av säkerhetsapplikationer såsom virusskydd, genom att kontrollen av applikationerna sker med en policy som då kan anpassas till en nivå som möjliggör virusskydd på enheten. ”Mobile hypervisors” har full kontroll över den virituella enheten där alla säkerhetsapplikationer och policys installeras, däremot har den ingen möjlighet att säkra upp användarens operativsystem. (Kapitel, 3.4.4)

NAC - Network Access Control

NAC kan inte säkra upp enheten, men genom steget ”bedömning” som är en av funktionerna som NAC kontrollerar, sker en så kallad hälso check där en bedömning görs ifall enheten är okej eller inte, samt en kontroll av hälsotillståndet för själva slutsystemet för att på bästa sätt skydda verksamheten ifrån hot. (Kapitel, 3.4.5)

5.3.4 Hålla låg nätverksbelastning

MDM - Mobile Device Management

Vi har inte identifierat någon ökad nätverksbelastning förutom när IT-avdelningen skall skicka ut uppdateringar av applikationer och data. (Kapitel, 3.4.1)

MAM - Mobile Application Management

Vi har inte identifierat någon ökad nätverksbelastning förutom när IT-avdelningen skall skicka ut uppdateringar av applikationer och data. (Kapitel, 3.4.2)

VDI - Viritual Desktop Infrastrukturer

En VDI lösning kräver en konstant uppkoppling mot verksamhetens servrar då ingen data lagras och bearbetas lokalt på enheten. Alla kommandon användaren utför måste skickas till servern och alla förändringar som servern vill visa användaren måste skickas tillbaka i en bildström vilket ger en hög nätverksbelastning. (Kapitel, 3.4.3)

Containerization

Vi har inte identifierat någon ökad nätverksbelastning förutom när IT-avdelningen skall skicka ut uppdateringar av applikationer och data. (Kapitel, 3.4.4)

NAC - Network Access Control

Ett av NAC´s steg för access på nätverket handlar om bedömning av enheten och användaren. Detta kan ske med en agentlös metod som skannar enheten för att göra en hälsocheck vilket resulterar i en hög belastning på nätverket berodende på hur ofta denna utförs. (Kapitel, 3.4.5)

5.3.5 Användarna bör känna sig bekväm med vad företaget kan göra på enheten

MDM - Mobile Device Management

MDM har en hög enhetskontroll inkräktar den på användarens integritet då verksamheten har full möjlighet att komma åt all information på enheten som är ansluten till MDM. Åtkomsten kan på sätt och vis kontrolleras med skrivna policys för en överenskommelse om vad företaget tittar på, men detta fråntar dem aldrig möjligheten utan bara rättigheten att titta på all information. (Kapitel, 3.4.1)

MAM - Mobile Application Management

Eftersom MAM håller en separation av företagsdata och privat data, samt att företaget enbart hanterar data och applikationer som finns inom den virtuella boxen, kan användaren känna sig bekväm. Anledningen är att företaget inte kan titta på användarens privata data och inte heller radera privat data ifall enheten försvinner. (Kapitel, 3.4.2)

VDI - Viritual Desktop Infrastrukturer

Verksamheten får ingen möjlighet att varken kontrollera, påverka eller övervaka den privata enheten eftersom allting sker genom en applikation på enheten som ansluter till och kommunicerar med verksamhetens servrar. VDI bör således leda till att användaren känner sig bekväm då dess kontroll på den privata enheten inte blir påverkad. (Kapitel, 3.4.3)

Containerization

Verkar för att separera verksamhetens och användarens data, ingen insyn eller kontroll utanför containern ges till IT-avdelningen varpå ingen privat data kan påverkas, användarna bör således känna sig bekväma med tekniken. (Kapitel, 3.4.4)

NAC – Network Access Control

Genom att NAC bara kontrollerar nätverksåtkomsten mot verksamheten de aldrig någon kontroll över användarens hela enhet vilket bör resultera i att användaren känner sig bekväm med att ha full kontroll på sin enhet. (Kapitel, 3.4.5)

6 Resultat och diskussion

Här presenteras först resultatet ifrån analysen följt av en diskussion kring den. Vi har tagit hänsyn till studiens hermeneutiska synsätt där begreppet samt teknikernas delar har analyserats under föregående kapitel och nu hur delarna förhåller sig till helheten.

6.1 Upplägg och struktur

I detta kapitel följer en bedömning av teknikerna baserad på analysen över hur stor grad de uppfyller de olika kriterierna som togs fram under kapitel 5.2. Vi har valt att gradera teknikerna med skalan ingen, låg, mellan och hög. Detta för att på ett tydligt sätt visa på hur stor grad en teknik uppfyller kriteriet. Skalan ”ingen” betyder att tekniken inte har någon hantering alls för att uppfylla kriteriet. För ”låg” betyder det att tekniken kan ha en liten form av hantering för att uppfylla kriteriet, men att vi upplever det som väldigt tunt. För ”mellan” får de teknikerna som varken har en låg eller hög hantering för att uppfylla kriteriet, men vi anser ändå att de gör det på en rimlig nivå. ”Hög” står för att tekniken har en genomtänkt hantering som fungerar väl för att uppfylla kriteriet.

6.2 Resultat av analysen

För kriterium ett som handlar om hur tekniklösningarna hanterar separation av företags data och privat data har VDI en hög nivån av hantering, då åtkomsten till företagsdata sker i en helt separat miljö. På samma nivå identifierade vi separat container eftersom den på ett tydligt sätt separerar företagsdata och privat data genom att viritualisera ett helt separat operativsystem på enheten där ingenting i det privata operativsystemet kan påverka eller påverkas av den separata containern. MAM och lokal container har en mellan nivå på hantering av separation av data eftersom teknikerna jobbar med en form av virtuell box där data separeras men fortfarande ligger på det privata operativsystemet. Både MDM och NAC är de tekniker som inte hanterar någon separation av olika data i sina grundformer. (Kapitel, 5.3.1)

När det gäller kriteriet kontrollen av dataåtkomst håller MDM, VDI och separat container en hög nivå medan MAM och lokal container ligger på en mellan nivå, anledningen till att de tre förstnämnda rankas högre är för att verksamheten har full kontroll över operativsystemet arbetet utförs på och all dess data.
De två sistnämnda tillämpar en teknik som ger verksamheten full kontroll på en liten del av operativsystemet arbetet utförs på. Skulle data hamna utanför denna del har verksamheten ingen kontroll på den längre. NAC är rankad som låg eftersom den har en hög ingående säkerhet då användaren behöver verifiera sig för att komma åt datan men när den väl ligger på enheten tappar verksamheten kontroll över datan. (Kapitel, 5.3.2)

MDM har den bästa möjligheten att uppfylla kriteriet om att säkra upp enheten då den ger verksamheten full kontroll över operativsystemet och applikationer som tillåts och installeras där. MAM och applikationsinkapsling under lokal container är rankade som mellan, MAM för att den möjliggör vitlisning och svartlisning av applikationer vilket kan bidra till att endast säkra applikationer kan installeras, applikationsinkapsling för att den möjliggör installation av säkerhetsapplikationer såsom virusskydd som dock kan vara problematiskt att få att fungera på hela enheten. Krypterade mappar under lokal container har en låg möjlighet att påtvinga installation av säkerhetsapplikationer och policys eftersom skyddet endast gäller inom containern och inte på hela enheten. VDI, separat container och NAC har ingen möjlighet att installera säkerhetsapplikationer eller applicera policys då de inte har åtkomst till enheten, VDI kan dock installera säkerhetsapplikationer på den virituella miljön. (Kapitel, 5.3.3)

Vi har identifierat att VDI ger en hög nätverksbelastning eftersom den kräver en konstant uppkoppling mot verksamhetens servrar för att användaren skall kunna arbeta. NAC är klassificerad som mellan eftersom den gör en ”hälsocheck” av enheten med täta intervall vilket kan skapa en relativt hög nätverksbelastning. I övriga kan vi inte se någon direkt ökad nätverksbelastning på de resterande teknikerna förutom när verksamheten skickar ut nya uppdateringar av applikationer och data. (Kapitel, 5.3.4)

För det sista kriteriet som handlar om personlig integritet har vi identifierar att användaren bör känna en hög trygghet med vad verksamheten kan och inte kan göra på enheten med en VDI, separat container och NAC teknik. MAM och lokal container däremot identifieras som mellan. Orsaken till att lösningarna värderas som mellan och höga är att de inte har någon möjlighet att påverka användarens privata data. Anledningen till att VDI och separat container värderas högst är att användaren får ett helt separat operativsystem att arbeta ifrån till skillnad ifrån MAM och lokal container som låter användaren arbeta i enhetens vanliga operativsystem vilket vi anser kan bidra till en osäkerhet. NAC är värderad högt med anledning av att den inte har någon möjlighet att påverka applikationer och data som finns lagrad på enheten, oavsett vem den tillhör. MDM har vi identifierat som den lösning användaren kan känna sig minst trygg med. Tekniken möjliggör för verksamheten att få åtkomst till all information på enheten, både privat och verksamhetsrelaterat. (Kapitel, 5.3.5)

Ovan nämnda resonemang sammanfattas i tabell 1.

				Containerization*		
Kriterium	MDM	MAM	VDI	Lokal container	Separat container	NAC
1.Dataseparation	Ingen	Mellan	Hög	Mellan	Hög	Ingen
2. Dataåtkomst-kontroll	Hög	Mellan	Hög	Mellan	Hög	Låg
3. Säkra upp enheten	Hög	Mellan	Ingen	Låg/Mellan**	Ingen	Ingen
4.Nätverks-belastning***	Låg	Låg	Hög	Låg	Låg	Mellan
5.Personlig integritet	Låg	Mellan	Hög	Mellan	Hög	Hög

Tabell 1, Hur teknikerna förhåller sig till kriterierna, egen

* Separeras i två delar, lokal container gäller krypterade mappar samt applikationsinkapsling, separat container gäller Mobile hypervisor (Kapitel, 3.4.4).

** Den första syftar på krypterad mapp, den andra delen syftar på applikationsinkapsling

*** Låg anses här positivt och hög negativt eftersom målet är att ha en låg nätverksbelastning.

6.2.1 Diskussion kring resultatet

MDM har en tydlig inriktning mot enhetskontroll för att ge verksamheten full kontroll och en hög datasäkerhet. Den obefintliga separationen av data orsakar dock att den personliga integriteten blir lidande då verksamheten i praktiken har möjlighet att kontrollera all data på enheten, oberoende av om det är verksamhetsrelaterat eller privat. Väljer en verksamhet en ren MDM lösning finns det ingen dataseparation vilket leder till att verksamheten inte kan

reglera vad som kontrolleras. Exempelvis kan en fjärrradering inte göras selektivt utan att all data på enheten skulle påverkas, privat så som verksamhetsrelaterad, vilket bör ge missnöjda och otrygga användare. Däremot blir informationssäkerheten ur verksamhetens perspektiv väldigt hög på grund av den hårda kontrollen.

MAM styrka ligger i att den kan säkra upp enskilda applikationer vilket begränsar verksamhetens kontroll till de applikationer och data som de äger och anser sig behöva säkra upp. Applikationerna ligger dock på samma operativsystem som användarens övriga vardagsapplikationer vilket gör att användaren behöver agera för att inte utföra privata uppgifter i en applikation som tillhör verksamheten. Dataseparationen blir därmed inte optimal och därför blir även den personliga integriteten aningen sämre då risken finns att verksamheten får åtkomst till privat data. Vid val av en MAM lösning får verksamheten en genomgående bra lösning där både verksamheten och användarnas behov uppfylls till stor del.

VDI är en teknik som har ett tydligt fokus på dataseparation och säkerhet, genom att hålla verksamhetsrelaterad data på verksamhetens egna servrar får de full kontroll över den samtidigt som den blir helt separerad ifrån personlig data. Att verksamheten inte har någon möjlighet att påverka användarens privata data då de inte har någon åtkomst till enheten leder till en hög personlig integritet. Att verksamhetens data ligger på servrar som användaren konstant måste vara uppkopplad till är också orsaken till att nätverksbelastningen blir hög. Väljer verksamheten att implementera en VDI lösning uppfylls samtliga kriterier ifrån både användaren och verksamheten förutom att den höga nätverksbelastningen och den konstanta uppkopplingen är oundviklig, vilket är en klart negativ faktor både för verksamheten men också för användaren som inte kan arbeta på enheten utan en uppkoppling till verksamhetens servrar.

Lokal container är en teknik som, genom applikationsinkapsling eller en container på användarens vardagliga operativsystem, har bedömts ha en mellan nivå vad gäller dataseparation och säkerhet. På grund av att informationen hålls på samma operativsystem kan det krävas ett mer konsekvent agerande av användaren för att data skall lagras på rätt ställe. Detta är också orsaken till att den personliga integriteten bedömts som mellan då en blandning kan orsaka att verksamheten får tillgång till privat data. Vid val av en lokal container får verksamheten en genomgående bra lösning där både verksamheten och användarnas behov uppfylls till stor del.

Separat container är den teknik som vi identifierat flest styrkor i, den har en tydlig separation av data då användaren är tvungen att växla till ett separat operativsystem för att komma åt verksamhetsrelaterade applikationer och data. Att tekniken inte har någon möjlighet att säkra upp det privata operativsystemet ser vi inte som relevant då den har möjlighet att göra det på den verksamhetsstyrda miljön där den data som verksamheten behöver säkra upp finns. Den personliga integriteten blir också hög på grund av den tydliga separationen som det separata operativsystemet innebär. En implementation av separat container leder till att samtliga kriterier uppfylls, både för användaren och för verksamheten vilket bör tillfredställa verksamhetens behov av hög informationssäkerhet och användarens behov av hög personlig integritet.

NAC är en teknik som har en låg fokus på datasäkerhet, den ger verksamheten möjlighet att kontrollera vem som ansluter sig till nätverket och statusen på den enheten, när enheten väl är ansluten släpper den kontrollen på data som går till enheten och vad som händer med den. Den gör dock återkommande kontroller av den anslutna enheten för att försäkra att statusen på

den inte har förändrats. Detta är också orsaken till att nätverksbelastningen med tekniken ökar då alla anslutna enheter skall kontrolleras kontinuerligt. En implementation av endast NAC som en BYOD lösning kan inte anses lämpligt då den inte på något sätt eller till ringa del uppfyller många av de kriterier som använts vid bedömningen eftersom den inte har någon möjlighet att påverka data på enheten. Konsekvensen av det blir att verksamhetens behov av informationssäkerhet inte kan tillgodoses. Däremot bör användaren anse att dess personliga integritet upprätthålls.

I resultatet som helhet (se tabell 1) är ”separat container” den teknik som har högst sammanlagd grad av BYOD hantering tätt följt av ”lokal container” och MAM. Därefter ser vi att VDI och MDM placerar sig. NAC skiljer sig ifrån mängden då tekniken har en avsevärt mycket längre sammanlagd grad av hantering än övriga tekniker. Trots detta är NAC inte en teknik som blir utesluten för hantering av BYOD då den hanterar några viktiga delar på sätt som de andra teknikerna inte kan göra. Vi ser att teknikerna har olika styrkor vilket kan innebära att en kombination av tekniska lösningar för BYOD kan vara en möjlig väg att gå för att få en teknisk lösning som täcker alla behov.

7 Slutsats

I följande kapitel beskrivs slutsatsen där frågeställningen besvaras och det fungerarsom en sammanställning ifrån analysdelen. Även en utvärdering av vald metod samt de valda utvärderingskriterierna kommer att diskuteras. Slutligen ges förslag till fortsatt forskning.

7.1 Slutsatser

Uppsatsens hade till syfte att ge stöd åt verksamheter som står inför att välja en teknisk lösning för BYOD som uppfyller verksamhetens huvudsakliga behov och samtidigt gör användarna nöjda. Detta vilket leder till huvudfrågan:

Hur kan en verksamhet välja en teknisk lösning för BYOD som uppfyller verksamhetens huvudsakliga behov och dessutom göra användarna nöjda?

I kapitel 3.4 identifierades möjliga tekniska lösningarna för hantering av BYOD.

Dessa tekniska lösningar var:

- MDM – Mobile Device Management
- MAM – Mobile Application Management
- VDI – Viritual Desktop Infrastrukturer
- Containerization
- NAC - Network Access Control

Därefter tog vi, i kapitel 5.2.3, fram ett antal utvärderingskriterier som är baserade på viktiga egenskaper för en BYOD lösning, hämtade ifrån både teorin (Kapitel, 3) och empirin (Kapitel, 4).

En BYOD lösning bör:

- Separera företagsdata och privat data
- Ge möjlighet att kontrollera åtkomst av företagsdata
- Säkra upp enheten
- Hålla låg nätverksbelastning
- Få användarna att känna sig bekväma med vad företaget kan göra på enheten

Baserat på utvärderingskriterierna utfördes, i kapitel 6, en bedömning av hur väl de olika tekniska lösningarna uppfyllde kriterierna. Nedan presenteras en sammanfattning av tabellen som visar resultatet av bedömningen.

Hur stor grad teknikerna uppfyller kriterierna				
Kriterium	Ingen	Låg	Mellan	Hög
1.Dataseparation	MDM NAC		MAM Containerization* (Lokal container)	VDI Containerization* (Separat container)
2. Dataåtkomst-kontroll		NAC	MAM Containerization* (Lokal container)	MDM VDI Containerization* (Separat container)
3. Säkra upp enheten	VDI, Containerization* (Separat container) NAC	Containerization* (Lokal container**)	MAM Containerization* (Lokal container**)	MDM
4. Nätverks-belastning***		MDM MAM Containerization* (Lokal container) Containerization* (Separat container)	NAC	VDI
5.Personlig integritet		MDM	MAM Containerization* (Lokal container)	VDI Containerization* (Separat container) NAC

Tabell 2, Sammanfattning av till hur stor grad teknikerna förhåller sig till kriterierna, egen

* Separeras i två delar, lokal container gäller krypterade mappar samt applikationsinkapsling, separat container gäller Mobile hypervisor (Kapitel, 3.4.4).

** Den första syftar på krypterad mapp, den andra delen syftar på applikationsinkapsling

*** Låg anses här positivt och hög negativt eftersom målet är att ha en låg nätverksbelastning.

Baserat på ovanstående slutsatser kan vi nu besvara vår frågeställning: Verksamheter som står inför att välja en BYOD lösning måste ta ställning till hur viktiga dessa utvärderingskriterer är för dess specifika verksamhen. Utifrån det ställningstagandet kan en teknisk lösning väljas. Detta genom att studera tabellen som presenterar hur teknikerna förhåller sig till utvärderingskriterierna (Tabell 1) och resonemanget kring den(Kapitel, 6). En verksamhet kan därmed välja teknisk lösning med stöd av vårt resultat.

7.2 Utvärdering av metod

Vårt hermeneutiska synsätt gjorde att vi var öppna och engagerade i arbetet med uppsatsen. Vi strävade efter att på bästa sätt se till hur delarna förhåller sig till helheten genom att allteftersom text och material insamlades kunde vi få en förnyad förståelse och på så sätt samla in ytterligare material tills vi uppnådde en förståelse för helheten och kunde besvara

frågeställningen. Därför har de deduktiva och induktiva angreppsettet varvats för att bygga upp mera material och ökad förståelse.
Vår kvalitativa forskningsansats har varit lämplig eftersom vi har studerat och samlat in ord. Där har vi antagit ett tolkande synsätt där empirins roll var att generera kriterier. Empirin fick även hjälpa till att generera teori och berika uppsatsen. Intervjun spelades in och stödord antecknades ner. Direkt efter intervjun transkriberades den och viktiga tankar kring den noterades. Även Toftefors fick läsa igenom och godkänna transkriberingen vilket resulterade i att materialet hanterades bra och misstolkningar undveks.

Den främsta datakällan har varit digitala dokument eftersom ämnet är väldigt aktuellt och dessa dokument har av naturliga skäl en högre publiceringstakt än tryckta dokument. De digitala dokumenten har gett uppsatsen den mest aktuella informationen. Valet av bra källor har varit lätt att efterfölja med hjälp av Brymans (2011) bedömningskriterier som nämns i kapitel 2.5. Så genom att tänka på autenticitet, trovärdighet, representativitet och meningsfullhet vid källbedömning har uppsatsen fått med bra och relevanta källor. Att vara källkritisk och försöka gå till djupet med källorna skapar ett bra utbud.

7.3 Utvärderingskriterierna

Uppsatsens arbete har utformats med hänsyn till de kriterier som nämndes i kapitel 2.9.1. Nedan beskrivs hur vi gått tillväga för att tillföra tillförlitlighet i uppsatsen.

7.3.1 Tillförlitlighet

De första delkriteriet för att uppnå tillförlitlighet handlar om överförbarhet och om hur väl den externa validiteten gäller för uppsatsen. Alltså hur väl uppsatsen fungerar i andra miljöer än den som har undersökts. Detta kriterie har följts genom en utförlig dokumentation över den teori som insamlats för att på så sätt kartlägga de tekniska lösningarna, så noga som möjligt.
Genom den tydliga kartläggningen av BYOD och de tekniska lösningarna har en grund skapats som oavsett form av verksamhet kan användas för att skapa sig en tydlig överblick på BYOD och de tekniska lösningar som identifierats.

Delkriteriet pålitlighet har till syfte att fungera likt reliabilitet där uppsatsen har eftersträvat att det ska vara möjligt att uppnå ett likartat resultat vid andra tillfällen. Detta har inte gått att få eftersom intervjun och den teorin som samlats in har varit aktuell för just det tillfället så den samlades in. För att öka pålitligheten har uppsatsen framtagits med granskning av examinatorn både under arbetet samt vid slutgiltiga resultatet. Detta ger uppsatsen en hög grad av pålitlighet.

Det sista delkriteriet handlar om möjligheten att styrka och konfirmera och detta har uppnåtts genom de hermeneutiskt synsätt som uppsatsen har och som är beskrivet under kapitel 2.2. Genom eftersträvan att återge texter på det sätt som författaren menar styrks det att inga personliga värderingar eller teoretiska inriktningar medvetet har fått påverka den slutsats som redovisats. Alla påstående och argument har noga grundats i den teori som skrivits vilket resulterar i att rapporten är skriven i god tro.

7.4 Utvärdering av forskningsbidraget

BYOD är ett relativt nytt begrepp som blivit väldigt populärt de senaste två åren vilket leder till att det inte är allmänt vedertaget vilken teknik för hantering av BYOD som är att föredra. Vi tror att detta kommer mogna med tiden när den initiala popularitet lagt sig och verksamheter börjar se på det med ett mer långsiktigt perspektiv. Denna uppsats behandlar en ögonblicksbild av teknikerna och bör ses som en nulägesanalys för hantering av BYOD.

Studien hade till syfte att ta reda på hur en teknisk lösning för BYOD kan väljas så att den uppfyller verksamhetens huvudsakliga behov och samtidigt gör användarna nöjda. Vi lyckades identifiera ett antal kriterier som var viktiga för verksamheten både ifrån teorin och empirin och med hjälp av dessa utforma utvärderingskriterier. Dessa utvärderingskriterier kunde sedan användas för att utvärdera hur de olika teknikerna förhåller sig och hanterar kriterierna. På så sätt hoppas vi att den slutliga tabellen som vi kom fram till kan fungera som ett stöd till företag som ser över möjligheten att välja en BYOD lösning som uppfyller verksamheten huvudsakliga behov och även tar hänsyn till användarna.

7.5 Förslag till fortsatt forskning

BYOD är ett brett område där utvecklingen ständigt går framåt. Vi kom fram till några olika möjliga lösningar, men för att få den bästa nyttan av dem bör de kombineras. Detta kan vara intressant för fortsatt forskning att titta vidare på. Att hålla koll på vad som händer med VDI är också en intressant del. Eftersom det förhoppningsvis kommer ske stora förbättringar, kan ytterligare forskning handla om just VDI och hur den fungerar.

Förslag till forskningsfrågor:

- *Hur kan BYOD teknikerna kombineras på bästa sätt för att gynna både företag och anställda?*
- *Är VDI den optimala BYOD lösningen?*

Referenser

Analytiker dömer ut ”bring your own” (2012). *CIO Sweden,* 6 december. https://web-retriever-info-com.lib.costello.pub.hb.se/services/archive.html?method=displayPDF&documentId=05702620121206E93B333D790AA8483E02F6A60AA10425&serviceId=2 [2013-02-12]

Anonymous. (2012). BYOD security risks on the rise. *Information Management Journal.* http://search.proquest.com.lib.costello.pub.hb.se/docview/1080736937 [2013-02-12]

Brandel, M. (2012). *BYOD: where the costs are*. Network world, 19 november. http://search.proquest.com/docview/1265771040 [2013-06-15]

Bryman, A. (2011). *Samhällsvetenskapliga metoder.* Malmö: Liber AB.

Burt, J.(2011). *BYOD Trend Pressures Corporate Networks.* Tech Analysis, 5 september. http://84.201.93.40/images/2/2e/65469365.pdf [2013-05-13]

BYOD 2013 – slår bring your own igenom brett nästa år? (2012). *CIO Sweden,* 6 december. https://web-retriever-info-com.lib.costello.pub.hb.se/services/archive.html?method=displayPDF&documentId=05702620121212063FAD6AB563E54D2FAC777842B69F5719&serviceId=2 [2013-02-12]

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD(Bring your own device). *American society for competitiveness.* Indiana, United states, ss. 117-121. http://search.proquest.com.lib.costello.pub.hb.se/docview/1196914876 [2013-02-12]

Copeland, R. & Crespi, N. (2012a). Analyzing Consumerization – Should Enterprise Business Context Determine Session Policy?. I IEEEXplore, *16th International Conference on Intelligence in Next Generation Networks.* ss. 187-193. http://ieeexplore.ieee.org.lib.costello.pub.hb.se/stamp/stamp.jsp?tp=&arnumber=6376024 [2013-02-12]

Copeland, R. & Crespi, N. (2012b). Controlling Enterprise Context-Based Session Policy and Mapping It to Mobile Broadband Policy Rules. I IEEEXplore, *16th International Conference on Intelligence in Next Generation Networks.* ss. 194-201. http://ieeexplore.ieee.org.lib.costello.pub.hb.se/stamp/stamp.jsp?tp=&arnumber=6376025 [2013-02-12]

Crook, S., Jaffe, J., Boggs, R. & Drake,S.(2011). *Worldwide Mobile Worker Population 2011–2015 Forecast*. IDC, December. http://www.idc.com/getdoc.jsp?containerId=232073 [2013-05-14]

Dimentional Research. (2012). *THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS. Checkpoint,* Januari. http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf [2013-05-13]

En av tre använder mobilen utan tillåtelse (2013). *Computer Sweden,* 31 januari. https://web-retriever-info-com.lib.costello.pub.hb.se/services/archive.html?method=displayPDF&documentId=05082720130131B8554428EBD5634AF36D71DAB9BD54EA&serviceId=2 [2013-02-12]

Enterasys Secure Network. (2008). *Understanding Network Access Control.* http://www.enterasys.com/company/literature/enterasys-nac-guide.pdf [2013-05-01]

Fick, P. (2013). *Is BYOD Negatively Impacting Your Employee Productivity?* It news Africa, 15 april. http://www.itnewsafrica.com/2013/04/is-byod-negatively-impacting-your-employee-productivity/ [2013-05-13]

Forrester Consulting. (2012). Key Strategies To Capture And MeasureThe Value Of Consumerization Of IT. Forrester Research, Inc, maj. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf [2013-05-14]

French, P. (2011). Another view on the consequences of BYOD. *Readwrite.com.* 25 December. http://readwrite.com/2011/12/25/another-view-on-the-consequenc [2013-04-13]

Ganett Co. (2012). *Bring your own device.* http://search.proquest.com.lib.costello.pub.hb.se/docview/1030105019 [2013-02-12]

Gartner. (2013). *Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013*. Gartner, 4 april. http://www.gartner.com/newsroom/id/2408515 [2013-05-14]

Goldkuhl, G. (2011). *Kunskapande.* [Elektronisk] Linköpings Universitet: Institutionen för ekonomisk och industriell utveckling. http://www.vits.org/publikationer/dokument/409.pdf [2013-04-23]

Gruman, Galen. (2011). *Mobile application management without the heavy hand.* InfoWorld, 26 april. http://www.infoworld.com/d/mobile-technology/mobile-application-management-without-the-heavy-hand-770?page=0,0 [2013-06-03]

Harbaugh, L. (2012). *The Pros and Cons of Using Virtual Desktop Infrastructure*. PCWorld, 22 Mars. http://www.pcworld.com/article/252314/the_pros_and_cons_of_using_virtual_desktop_infrastructure.html [2013-06-03]

Harkins, M.(u.å.). *Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices*. http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264 [2013-05-13]

Howze, T. (2012). BYOD- Bringing your own demise to the workplace. *Examiner.com.* 21 Februari.

http://www.examiner.com/article/byod-bringing-your-own-demise-to-the-workplace [2013-03-26]

Inghe, M. (2012). Byod – så påverkar det it-avdelningen. *TechWorld.* 10 December http://www.idg.se/2.1085/1.479114/byod--sa-paverkar-det-it-avdelningen/sida/1/fler-tar-kraft-med-sig [2013-02-12]

Kaneshige, T. (2012). *BYOD*: if you think you´re saving money, think again. *CIO*, 4 April. http://www.cio.com/article/703511/BYOD_If_You_Think_You_re_Saving_Money_Think_Again?page=2&taxonomyId=600013 [2013-06-15]

Knuth, G. (2012). *Consumerization of IT: What's VDI got to do with it?* TechTarget. http://searchvirtualdesktop.techtarget.com/tip/Consumerization-of-IT-Whats-VDI-got-to-do-with-it [2013-06-03]

Mansfield-Devine, S. (2012). *Interview: BYOD and the enterprise network*. 2012(4), ss. 14-17. http://www.sciencedirect.com.lib.costello.pub.hb.se/science/article/pii/S1361372312700313 [2013-05-14]

Marko, K.(2013). *BYOD Security: Do You Really Need MDM?* NetworkComputing, 11 mars. http://www.networkcomputing.com/security/byod-security-do-you-really-need-mdm/240150487 [2013-05-13]

Marko, K. (2011). *Keeping Corporate Data Off Mobile Devices With VDI.* UBM Tech, 27 juli. http://www.networkcomputing.com/security/byod-security-do-you-really-need-mdm/240150487 [2013-05-17]

McLellan, C. (2013). Consumerization, BYOD and MDM: What you need to know. *ZDNet.* 1 Februari. http://www.zdnet.com/consumerization-byod-and-mdm-what-you-need-to-know-7000010205/ [2013-05-15]

Mitchell, R. (2012) *Best BYOD management: Containment is your friend*. Computerworld, 29 augusti. http://www.computerworld.com/s/article/9230476/Best_BYOD_management_Containment_is_your_friend [2013-05-02]

Miller, K. W., Voas, J. & Hurlburt, G. F. (2012). BYOD: Security and Privacy Considerations. *IT Professional,*14(5), ss. 53-55. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320585 [2013-02-12]

Network World. (2013). *The science of app-wrapping*. ProQuest, 7 maj. http://search.proquest.com/docview/1350186781 [2013-05-17]

Patel, R. (2011). *Forskningsmetodikens grunder – att planera, genomföra och rapportera en undersökning.* Studentlitteratur AB, Lund

Rouse, M. (2012). *Mobile application manager(MAM).* WhatIs.com, Juli.

http://whatis.techtarget.com/definition/mobile-application-manager-MAM [2013-06-03]

Rymon, R. (2012). *Why MDM is wrong solution in most BYOD use cases.* LinkedIn, 11 maj. http://www.linkedin.com/groups/Why-MDM-is-wrong-solution-3700181.S.114544787 [2013-05-13]

Scarfö, A. (2012). New secirity perspectives around BYOD. I IEEEXplore, *Seven International Conference on broadband, Wireless Computing, Communication and applications.* ss. 446-451. http://ieeexplore.ieee.org.lib.costello.pub.hb.se/stamp/stamp.jsp?tp=&arnumber=6363095 [2013-02-12]

Siddiqui, S. (2012) *BYOD, MDM, NAC, DLP, VDI and Beyond!* Secureworld post, 12 November. http://secureworldpost.secureworldexpo.com/byod-mdm-nac-dlp-vdi-and-beyond-2/ [2013-05-01]

Stein, A. (2012). How does mobile device management (MDM) work?. *Networkworld,* 13 Februari. http://www.networkworld.com/news/2012/021312-mobile-device-management-256043.html [2013-05-02]

VMware. (2013). VMware Horizon Mobile. *VMware, Inc, 22 April.* http://www.vmware.com/files/pdf/horizon-mobile/vmw-horizon-mobile-datasheet.pdf [2013-05-29]

Techtarget. (2012a). *mobile application manager (MAM)*. Techtarget, juli. http://whatis.techtarget.com/definition/mobile-application-manager-MAM [2013-05-17]

Techtarget. (2012b). *mobile application manager (MAM)*. Techtarget, juli. http://searchsecurity.techtarget.com/definition/application-blacklisting [2013-05-17]

Techtarget. (2012c). *mobile application manager (MAM)*. Techtarget, juli. http://searchsecurity.techtarget.com/definition/application-whitelisting [2013-05-17]

Bilaga 1

Intervjufrågor

1. Vad är din uppgift på företaget?
2. Vad triggade igång tanken på att ni måste hantera problemet med BYOD?
3. Vad var motivet till er valda teknik?
4. Ser ni en begränsning med den?
5. Känner ni er nöjda med den valda tekniken?
6. Övervägde ni någon annan lösning än den ni valde?
7. Hur ser policyhanteringen ut för den privata enheten och för en företags ägd enhet?
8. Vet användarna om att de får ta med sig sina egna enheter?
9. Tror ni att de anställda känner sig trygga med IT-avdelningen gör vad de har sagt?
10. Har ni tittat på separationen av företagsdata och privat data?
11. Har ni några problem just nu?

Högskolan i Borås är en modern högskola mitt i city. Vi bedriver utbildningar inom ekonomi och informatik, biblioteks- och informationsvetenskap, mode och textil, beteendevetenskap och lärarutbildning, teknik samt vårdvetenskap.

På **institutionen Handels- och IT-högskolan (HIT)** har vi tagit fasta på studenternas framtida behov. Därför har vi skapat utbildningar där anställningsbarhet är ett nyckelord. Ämnesintegration, helhet och sammanhang är andra viktiga begrepp. På institutionen råder en närhet, såväl mellan studenter och lärare som mellan företag och utbildning.

Våra **ekonomiutbildningar** ger studenterna möjlighet att lära sig mer om olika företag och förvaltningar och hur styrning och organisering av dessa verksamheter sker. De får även lära sig om samhällsutveckling och om organisationers anpassning till omvärlden. De får möjlighet att förbättra sin förmåga att analysera, utveckla och styra verksamheter, oavsett om de vill ägna sig åt revision, administration eller marknadsföring. Bland våra **IT-utbildningar** finns alltid något för dem som vill designa framtidens IT-baserade kommunikationslösningar, som vill analysera behov av och krav på organisationers information för att designa deras innehållsstrukturer, bedriva integrerad IT- och affärsutveckling, utveckla sin förmåga att analysera och designa verksamheter eller inrikta sig mot programmering och utveckling för god IT-användning i företag och organisationer.

Forskningsverksamheten vid institutionen är såväl professions- som design- och utvecklingsinriktad. Den övergripande forskningsprofilen för institutionen är handels- och tjänsteutveckling i vilken kunskaper och kompetenser inom såväl informatik som företagsekonomi utgör viktiga grundstenar. Forskningen är välrenommerad och fokuserar på inriktningarna affärsdesign och Co-design. Forskningen är också professionsorienterad, vilket bland annat tar sig uttryck i att forskningen i många fall bedrivs på aktionsforskningsbaserade grunder med företag och offentliga organisationer på lokal, nationell och internationell arena. Forskningens design och professionsinriktning manifesteras också i InnovationLab, som är institutionens och Högskolans enhet för forskningsstödjande systemutveckling.

HÖGSKOLAN I BORÅS
VETENSKAP FÖR PROFESSION

BESÖKSADRESS: JÄRNVÄGSGATAN 5 · POSTADRESS: ALLÉGATAN 1, 501 90 BORÅS
TFN: 033-435 40 00 · E-POST: INST.HIT@HB.SE · WEBB: WWW.HB.SE/HIT